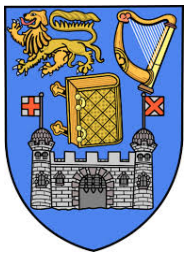
Towards an Access Control and Consent Strategy for an Electronic Healthcare Record (EHR) in Ireland: What can we learn from the experience of other nations?

Sean Lennon

A dissertation submitted to the University of Dublin, in partial fulfilment of the requirements for a degree of Masters of Science in Health Informatics



2014

Declaration

I declare that the work described in this dissertation is, except where otherwise stated, entirely my own work, and has not been submitted as an exercise for a degree at this or any other university.

Signed: Date:

I agree that Trinity College Library may lend or copy this dissertation upon request.

Signed: Date:

Acknowledgements

I wish to thank a number of people who have helped in some way towards the completion of this research.

Firstly, I would like to thank Damon Berry my research supervisor, whose in-depth knowledge, valuable advice, support and encouragement were greatly appreciated throughout the course of this research.

I would also like to thank Peter Connolly at the National Integrated Services Framework for his assistance in identifying the research area, and also for assisting with the recruitment of the case study interviewees.

I also wish to thank the interview participants for the generosity of their time and expertise, contributing greatly to the richness of the research evidence.

Also, a sincere thank you to course director, Lucy Hederman, without whose support and clear advice at an earlier time would not have allowed me to undertake this research.

And to my wife Lorraine, for her unwavering support and encouragement, and endless proofreading, I will be forever grateful.

Finally, to Rachael, Leah, Kerri, Grace and Katie, thank you for your patience.

Summary

Privacy is a fundamental right, and despite living in a world where that privacy is increasingly difficult to maintain, some aspects of our lives should necessarily remain private; this includes our personal healthcare information.

As this health information is now becoming increasingly available through integrated health information systems, and in particular the emergence of national Electronic Healthcare Records (EHRs), this has presented new challenges concerning the protection of the privacy and confidentiality of that data.

As a result, national interoperability programmes must strategically address these issues, including an approach to topics such as EHR identities, access control and consent management.

This research seeks to inform Ireland's National EHR programme on these specific areas, and this is achieved through an exploration of the experiences of, and lessons learned in three countries: England, the Netherlands and Canada.

The research methodology is qualitative in nature, and based on the multi-case case study approach. Evidence was collated from interviews with senior employees, in positions of responsibility central to the main research themes, and also from the available documentation in the literature and from national artefacts.

Analysis was conducted iteratively through cross-case comparison based on the theory building paradigm. A number of central themes emerged relating to:

- role engineering processes,
- finding a socio-technical balance to the access control strategy, and
- establishing a clear national position on consent management issues at the outset.

These themes are reflected in a series of twelve recommendations to the National Integrated Services Framework (NISF), Ireland's EHR interoperability programme.

Contents

Declaration ii

Acknowledgements iii

Summary iv

Contents vi

List of Tables ix

List of Figures x

List of Acronyms xi

1 Introduction 1

2 State of The Art 5

2.1 Introduction 5

2.2 Privacy Matters 6

2.3 The Right to Privacy 7

2.3.1 Patient Consent 9

2.3.2 Privacy Impact Assessments 11

2.4 Definitions 11

2.5 Access Control Considerations 13

2.6 Identification 16

2.7 Authentication 18

2.8 Access Control Models 19

2.8.1 Mandatory Access Control (MAC) 19
2.8.2 Discretionary Access Control (DAC) 20
2.8.3 Role-Based Access Control (RBAC) 20
2.8.4 Structural and Functional Roles 23
2.8.5 Role Engineering 24
2.9 Sensitivity 27
2.10 Policy Framework 29
2.11 Policy Domains 31
2.12 Audit 32
2.13 Conclusion 33

3 Methodology **36**
3.1 Introduction 36
3.2 Methodologies 37
3.2.1 Methodological Strategies 37
3.2.2 Methodologies in ICT Research 38
3.2.3 The methodology of Choice 38
3.3 Qualitative Method Selection 39
3.3.1 Qualitative Methods 39
3.3.2 Theory Testing versus Theory Building 41
3.4 Case Study Design 42
3.4.1 Case Study Sampling 42
3.4.2 Case Study Evidence 42
3.4.3 The Case Study Protocol 43
3.4.4 Interviews 43
3.4.5 Analysis 44
3.5 Study Execution 44
3.5.1 Setting the Study Goals 45
3.5.2 Literature Review 45
3.5.3 Methodological Selection 46
3.5.4 Designing the Case Study 46
3.5.5 Case Study Evidence 47
3.5.6 The Interviews 47

3.5.7 Documentation Gathering 50
3.5.8 Results 50
3.5.9 Analysis and Discussion 50
3.6 Conclusions 51

4 Case Study Results **54**
4.1 Introduction 54
4.2 The English Study 55
4.2.1 Context 55
4.2.2 Consent Management 56
4.2.3 Identities and Authentication 60
4.2.4 Authorisation 60
4.3 The Dutch Study 64
4.3.1 Context 64
4.3.2 Consent Management 66
4.3.3 Identities and Authentication 67
4.3.4 Authorisation 68
4.4 The Canadian Study 70
4.4.1 Context 70
4.4.2 Consent Management 72
4.4.3 Identities and Authentication 73
4.4.4 Authorisation 74
4.5 New Brunswick 75
4.5.1 Context 75
4.5.2 Consent Management 76
4.5.3 Identities and Authentication 77
4.5.4 Authorisation 78
4.6 Conclusion 80

5 Discussion **82**
5.1 Introduction 82
5.2 Analysis 83
5.2.1 Context 83

5.2.2 Consent Management 84
5.2.3 Identities and Authentication 89
5.2.4 Authorisation 91
5.3 Conclusion 98

6 Conclusions **99**

Bibliography **103**

Appendices **114**

A Case Study Protocol **115**
A.1 Information Document for Participants 116
A.2 Interview Questions 120
A.3 Informed Consent Form 122

B Interview Guide **126**

C UK Rationalised Roles **129**

D New Brunswick: EHR Access Request **131**

E Summary of Results **134**

F Table of Recommendations **140**

List of Tables

2.1 Examples of structural and functional roles 24

3.1 Mapping research themes to interview questions 47

5.1 Population variance 83

C.1 UK rationalised roles 130

E.1 Summary of results 139

F.1 Table of recommendations 143

List of Figures

2.1 Sharing healthcare information 15
2.2 Core RBAC 21
2.3 Role engineering scenario model hierarchy 25
2.4 High Level view of role engineering process 26
2.5 Default classification of healthcare information 28
2.6 Role Based Access Control policy framework 31

4.1 UK PBAC model 62
4.2 Infoway Infostructure conceptual outline. 72
4.3 Infoway consent directive process. 74
4.4 New Brunswick RBAC model 79

List of Acronyms

Acronym	Long Entry
ABAC	Attribute-Based Access Control
ANSI	American National Standards Institute
AUT	Authorisation Service (Dutch abbreviation)
BIG	Professionals In Healthcare (Dutch abbreviation)
BSN	Citizen Service Number (Dutch abbreviation)
CIBG	Central Information Point for Healthcare Professions (Dutch abbreviation)
DAC	Discretionary Access Control
DCR	Detailed Care Records
eGIF	e-Government Interoperability Framework
EHR	Electronic Health Record
EMD	Electronic Medication Record (Dutch abbreviation)
EPD	Dutch Electronic Health Record (Dutch abbreviation)
EPD-wet	Electronic Health Record Act (Dutch abbreviation)
HIPAA	Health Insurance Portability and Accountability Act
HIQA	Health Information and Quality Authority
HIT	Health Information Technology
HSCIC	Health and Social Care Information Centre
HSE	Health Service Executive
HSP	Health Service Providers
IACM	Identity, Access and Consent Management
IHI	Individual Health Identifier

Continued on next page

Acronym	Long Entry
IS	Information Systems
LR	Legitimate Relationship
LSP	Central Switch Point (Dutch abbreviation)
MAC	Mandatory Access Control
NHN	National Health Number
NHS	National Health Service
Nictiz	The National IT Institute for Healthcare (Dutch abbreviation)
NISF	National Integrated Services Framework
NIST	National Institute of Standards and Technology (American)
NPfIT	National Programme for Information Technology
OASIS	Open Architecture for Secure Inter-working Services
OPOR	One Patient One Record
PBAC	Position Based Access Control
PIA	Privacy Impact Assessment
PKI	Public Key Infrastructure
POS	Point of Service
PSIS	Personal Spine Information Service
RA	Registration Authority
RBAC	Role-Based Access Control
SCR	Summary Care Record
Sit-BAC	Situation-Based Access Control
SoD	Separation of Duty
TCD	Trinity College Dublin
UK	United Kingdom
URP	User Role Profile
UZI	Unique Healthcare Provider Identification (Dutch abbreviation)
WDH	Electronic General Practitioners Record (Dutch abbreviation)

Chapter 1

Introduction

> *"Privacy is dead - get over it" Scott McNealy, co-founder of Sun Microsystems*

The opening quotation above predates 9/11 and the consequent aggressive pursuit of intelligence information across the globe. It predates Facebook, Wikileaks, customer loyalty cards, Twitter and John Snowdons defection to Russia, each evoking a picture of private information taken without consent, or provided freely and enthusiastically en masse. The decade and a half since Scott McNealy made this controversial, yet compelling statement, has shown us that information is, now more than ever, a valuable commodity, and that while we hope privacy is not completely dead, in this digital age it is increasingly difficult to maintain.

Against this backdrop, health systems across the world strive to make better use of health information systems by promoting technology, and through the sharing of health information (Kodner & Spreeuwenberg 2002). The Electronic Health Record has become a major focus of this and is defined as:

> *"one or more repositories, physically or virtually integrated, of information in computer processable form, relevant to the wellness, health and healthcare of an individual, capable of being stored and communicated securely and of being accessible by multiple authorized users, represented according to a standardized or commonly agreed logical information model. Its primary purpose is the support of life-long, effective, high quality and safe integrated healthcare." (International Standards Organisation 2011)*

The implementation of Electronic Health Records is however, complex, and many countries across the world have seen the foundation of agencies and programmes to oversee the establishment of national EHR infrastructures. Examples include the Health and Social Care Information Centre (HSCIC) in the UK, Canada Health Infoway, and the Dutch National IT Institute for Healthcare (Nictiz).

Ireland too has embarked on this eHealth journey. As part of Ireland's Health Service Executive (HSE), the National Integrated Services Framework (NISF) represents a body of work that sets out to establish a reference model for the interoperability of healthcare systems in Ireland. This body of work:

> *"sets out a challenging but achievable work-programme which entails the development of an aligned standards based reference model which will underpin future technology developments and acquisitions within the HSE"* (Health Service Executive 2012)

One of the key outputs of this work-programme is to provide the necessary building blocks of a national Electronic Health Record (EHR). The programme is being delivered through twelve work-streams (Health Service

Executive 2012, Connolly 2013):

WS1: EHR Overview and Approach
WS2: Technical Infrastructure Work-stream
WS3: Software Applications Reference Base
WS4: Integrated Systems Management Framework
WS5: High Level Business Process Specification
WS6: Information Architecture Model
WS7: Data and Information Repository Work-stream
WS8: Transformation, Interfacing and Sourcing
WS9: Identity, Access and Consent Management
WS10: EHR Portal and Presentation
WS11: Architecture Documentation
WS12: Governance Model

Work-stream nine, listed above as Identity, Access and Consent Management (IACM) is concerned with the development of a standards based access control model, which facilitates the added complexity associated with wider access to healthcare information, namely the safeguarding of the privacy of our health information.

Access Control is concerned with a *"means of ensuring that the resources of a data processing system can be accessed only by authorised entities in authorised ways"* (International Standards Organisation 2012*a*), and patient consent, in the context of information sharing, can be described as the right of the individual to determine the extent to which personal data can be disseminated and processed beyond the original intended use (Government of Ireland 1988, Government of Ireland 2003).

This research seeks to inform work-stream nine by examining the current state of the art in relation to access control and consent management, and by looking to the experience of other nations who have attempted to meet

this challenge in what still is, at a national scale, a relatively new and emerging field.

Accordingly, the research question is defined as:

> *What can Ireland learn from the experiences of other nations towards the creation of an access control and consent strategy for a national Electronic Healthcare Record (EHR)?*

This research presents a multi-case case study of the experiences and of the lessons learned in three countries: England, the Netherlands and Canada (New Brunswick), concerning the implementation of access control and consent management in the context of a national EHR programme.

Chapter two of this dissertation represents a review of the associated literature and outlines the current state of the art on the chosen subject areas.

Chapter three describes the research methodology, how it was chosen, how it was applied, and discusses the strengths, limitations and challenges encountered as the study progressed.

Chapters four and five present the results and analysis respectively, culminating in a series of recommendations to the above mentioned work-stream nine of the NISF programme.

Finally, chapter six provides a summary and conclusion.

Chapter 2

State of The Art

2.1 Introduction

This chapter presents an understanding of the state of the art concerning access control in healthcare, based on a review of the literature.

The need for access control measures is borne out of our concerns for, and fundamental right to personal privacy. Access control in healthcare presents particular challenges, especially as healthcare moves from a centralised to the shared care model, with its associated information requirements (Kodner & Spreeuwenberg 2002). An Electronic Healthcare Record (EHR) distributed across communicating healthcare information systems must allow those connected with a patients care to access that patients information, but must also constrain that access in accordance with data protection legislation, the rules and regulations governing healthcare organisations, as well as the ethical and social norms prevailing in our society.

Access control in healthcare is surely complex, and much of the theory in this field is concerned with the derivation of models and systems concerned with simplifying the processes involved. This chapter will provide an overview of the current theory. Sections two and three will discuss aspects of privacy. Section four provides basic definitions. Section five discusses the aspects of

healthcare that make access control so difficult for this sector. Sections six and seven consider identification and authentication, while eight through eleven attends to authorisation considerations. Finally, section twelve is concerned with audit.

The design and implementation of authorisation is highly dependent on a country's legal and ethical environment. As such, international standards in this field are not specific at a computational level, but are aimed rather at providing guidance and frameworks necessary to allow individual countries meet their specific requirements. Accordingly, this discussion is weighted towards the authorisation aspects of access control.

2.2 Privacy Matters

> *"I believe there is something out there watching us. Unfortunately, it's the government". Woody Allen*

Allen's brand of paranoid and introspective humour, evident in the opening quotation, strikes a universal chord. We live in a digital age where extraordinary amounts of personal information are uploaded to, and made publicly available on the internet every day, where consumers of goods and services increasingly move to the electronic marketplace, and where health information progresses from paper-based to computer-based records.

While many sectors of society have embraced this Information Age, a drip feed of high-profile data protection breaches undermine confidence in technology, and concerns grow regarding the security and privacy of our digitally held details.

One such recent breach involved the disclosure of personal information of more than 1.5 million people at an Irish based internet company, and has been described as one of the worst data protection breaches in the history

of the state (Pope & Edwards 2013).

This, along with concerns regarding misuse and inappropriate sharing of our data serve to shape our perception of the safety of our electronic information, and consequently our attitudes towards the storage of this most sensitive of personal data.

This effect is demonstrated in a study focusing on citizens in Germany and Austria, and their understanding of, and attitudes towards electronic health records. Respondents reacted positively to the notion that their health information should be shared amongst a team of healthcare workers involved in their care, but that this positivity is offset by concerns relating to security and data protection (Hoerbst, Kohl, Knaup & Ammenwerth 2010). Similar findings were expressed in a New Zealand study. However, this study also found that providing citizens with information regarding security measures taken to protect their data, rebalanced and positively altered perceptions (Chhanabhai & Holt 2007).

Impacts arising from disclosure of our most private health information can have devastating consequences (Becker 2007, Eyers, Bacon & Moody 2006), thus health information must be protected, and be seen to be protected, from external and internal threats as the transition to the electronic healthcare record continues.

2.3 The Right to Privacy

The right to privacy is not a new notion. The Hippocratic Oath, dating back to 400BC, states that (Scott, Jennett & Yeo 2004):

> *"Whatever, in connection with my professional service, or not in connection with it, I see or hear, in the life of men, which ought not to be spoken of abroad, I will not divulge, as reckoning that all should be kept secret."*

In more recent times, the right to privacy has found wider recognition. The European Convention on Human Rights (2010), Article 8, establishes the fundamental right to privacy for its citizens, stating that:

1. *"Everyone has the right to respect for his private and family life, his home and his correspondence."*
2. *"There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."*

Also in Europe, directive 95/46/EC (1995) provides a legal basis to the protection of individuals with regard to the processing of personal data, and to the free movement of such data. Member states have enacted local legislation in compliance with the directive including Ireland's Data Protection Acts (1988, 2003) which directs that personal "sensitive" information may only be used for the purpose for which it was obtained, must be secure, and must be processed fairly. Similar legislative directives are found across the world including, for example, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) in the United States of America (Government of the United States of America 1996).

2.3.1 Patient Consent

Data Protection Legislation, such as described above, introduces the notion of consent, i.e. the right of the individual to determine the extent to which personal data can be disseminated beyond the original intended use (Government of Ireland 1988, Government of Ireland 2003).

Certain circumstances will permit an implied consent for the handling of personal information. For example, a visit to the GP may result in a patient's referral by that GP to a specialist. The GP will not normally ask for the patient's consent to disclose personal health details as part of the referral process; in these circumstances is it reasonable for the GP to assume that the consent is implied because the patient is present and the GP will have discussed the referral with the patient.

The circumstances in which consent can be implied is not always so obvious, and the extent to which consent should be implied versus explicitly obtained from the patient is the subject of much debate (van der Linden, Kalra, Hasman & Talmon 2009). Explicit consent comes at the price of adding a significant layer of complexity to the management of access control. However, proponents argue strongly for explicit consent mechanisms, describing unauthorised EHR access as *"electronic voyeurism"* and an assault on patient rights (Kluge 2004).

Internationally, differences in legislation and it's interpretation result in variations in the implementation of consent; for example, the NHS in England has proposed the implied consent model, while the Netherlands must comply with legislation which calls for explicit consent (van der Linden et al. 2009).

As described earlier, the EU Directive 95/46/EC (1995) and Ireland's Data Protection Acts (1988, 2003) provide direction in Ireland for the interpretation of consent requirements as it relates to the fair processing of personal

information. These legislative instruments are however, not specific to the area of healthcare, and to some extent are open to interpretation:

> *"Section 2A of the Acts does not specify a level of consent. This may vary from case to case and between implied and explicit. If relying upon consent, the key test will be to demonstrate that consent exists."* (Data Protection Commissioner, Ireland 2014)

In 2008, Ireland's (then) Department of Health and Children conducted a public consultation process on the establishment of specific legislation dealing with information in healthcare: the proposed Health Information Bill. Privacy and consent issues featured strongly in the resultant report and, reflecting the contentious nature of this subject, stated:

> *"individual submissions had differing views on where precisely the line might best be drawn between a 'rights' based approach, which emphasised individuals' rights to fully control their information, and a wider 'utility' based approach, which promoted a societal perspective on using the information for both the patient's individual benefit as well as society's general gain"* (Department of Health and Children, Ireland 2008*a*)

While Ireland has seen some progress in health information legislation (Health Identifiers Bill - see section 2.6 below) a Health Information Bill dealing with the issues of privacy and consent has yet to be brought forward.

In addition to legislation, Irish healthcare professionals are also expected to comply with various ethical and organisational codes of practice. Examples include the Irish Medical Council's *A Guide to Ethical Conduct and*

Behaviour (The Medical Council, Ireland 2004), the Health Service Executive's organisational guide: *Data Protection And Freedom Of Information Legislation* (Health Service Executive n.d.), and in General Practice: *A Guide to Data Protection Legislation for Irish General Practice* (Irish College of General Practitioners, GPIT Data Protection Working Group 2011).

2.3.2 Privacy Impact Assessments

The successful implementation of distributed EHRs will not only depend on strict compliance with data protection legislation, such systems must also be demonstrably secure, providing public assurance that their information is being processed safely, fairly and in accordance with their wishes. HIQA (2010) recommends and provides guidance on the adoption of Privacy Impact Assessments (PIAs) as an information governance tool for assessing, documenting and managing the risks associated with the processing of sensitive health data. The PIA document, which should evolve over the course of a project, should be publicly available, and promote awareness and consultation among project stakeholders, including the public. PIAs have been widely adopted in health IT projects across the world, including for example the Canadian Infoway project (Canada Health Infoway 2008).

2.4 Definitions

Terminology in this domain as found in the literature is often used interchangeably. For example the entire subject is referred to as *authentication and authorisation* in some discussions and *access control* in others, yet in other documents authorisation is treated as a discrete subdivision alongside privilege management and access control. That in mind, it is useful at this point to provide some definitions, and the following are taken directly from the standards: The convention used in this dissertation is to use the term *Access Control* to mean the entire subject domain, unless otherwise speci-

fied in the text.

Access Control
Means of ensuring that the resources of a data processing system can be accessed only by authorised entities in authorised ways, ISO/DIS 22600:(2012*a*).

Authentication
Provision of assurance of the claimed identity of an entity by securely associating an identifier and its authenticator, ISO/DIS 22600:(2012*a*).

Authorisation
Granting of privileges, which includes the granting of privileges to access data and functions, ISO/DIS 22600:(2012*a*).

Access Control Policy
Set of legal, political, organisational, functional and technical obligations for communication and co-operation, ISO/DIS 22600:(2012*a*).

Access Control Policy Agreement
Written agreement where all parties commit themselves to a specified set of policies, ISO/DIS 22600:(2012*a*).

Access Control Privilege
Capacity assigned to an entity by an authority, EN13606-4(2007).

Role
Set of competences and/or performances that is associated with a task, ISO/DIS 22600:(2012*a*).

Sensitivity
Measure of importance assigned to information to denote its need for protection, EN13606-4(2007).

2.5 Access Control Considerations

Healthcare is an information intensive business. Over the course of each of our lives, thousands of pieces of health related information are collected, analysed, acted upon, and stored. The increasing use of information technology in healthcare has seen a shift in the information storage medium from paper towards the electronic health record in the pursuit of greater efficiency and better patient care (Buntin, Burke, Hoaglin & Blumenthal 2011). This has presented new challenges in the preservation of our right to protected data.

As the model of healthcare delivery changes from a centralized to a distributed, shared care environment (Department of Health and Children, Ireland 2008*b*), the need for EHR interoperability increases in order to support the associated information needs. (Blobel 2007).

The EHR has many definitions, however, from an access control viewpoint, the following architectural description of a distributed EHR is useful in terms of these discussions. (ISO18308:2011 *Health informatics - Requirements for an electronic health record architecture*)

> *"The EHR for the subject of care might be scattered physically across multiple (discrete or interconnected) clinical systems and repositories, each of which will hold and manage a partial EHR for each of its subjects of care, scoped according to the service or community settings, clinical domains and time periods of use of that system in the life of each person"*

This definition highlights many of the complexities associated with access control and privilege management. Over a lifetime, each of us will interact with a diverse range of health services, geographically dispersed, and pro-

vided by a mixture of public and private healthcare organisations.

Legacy health information systems will exist in autonomous and distributed computing environments across these services, and will be provided and supported by a range of vendors who will implement access management technically and logically in different ways, and at different levels of competence and sophistication (Smith & Eloff 1999).

The shared care environment requires the sharing of our information, not just among clinicians, but also among support staff, administration, and others (Figure 2.1). This sharing of electronic information can result in multiple copies of data residing across a number of health information systems. Any update, modification or deletion of the data in one location must result in communications to maintain the integrity of the data across all copies. Furthermore, this requires a consistent version management approach across each system; overwritten information should be maintained such that the available information on a patient can be reconstructed to a particular point in time, and this is important for example when reviewing a past clinical decision based on the available information on the patient at the time (van der Linden et al. 2009). The interoperability of health information systems, including access control, is required to support this way of working.

As existing and future health information systems become increasingly interconnected, larger in scale, and generally more widely available, the complexities associated with the management of access further increase. Large national systems may have thousands of users across a range of organisational and functional roles. In addition, the flexibility of healthcare staff in a constantly evolving and adapting environment means those healthcare roles are in a constant state of change. While at the same time, each user may be required to retain several sets of credentials for a host of different systems.

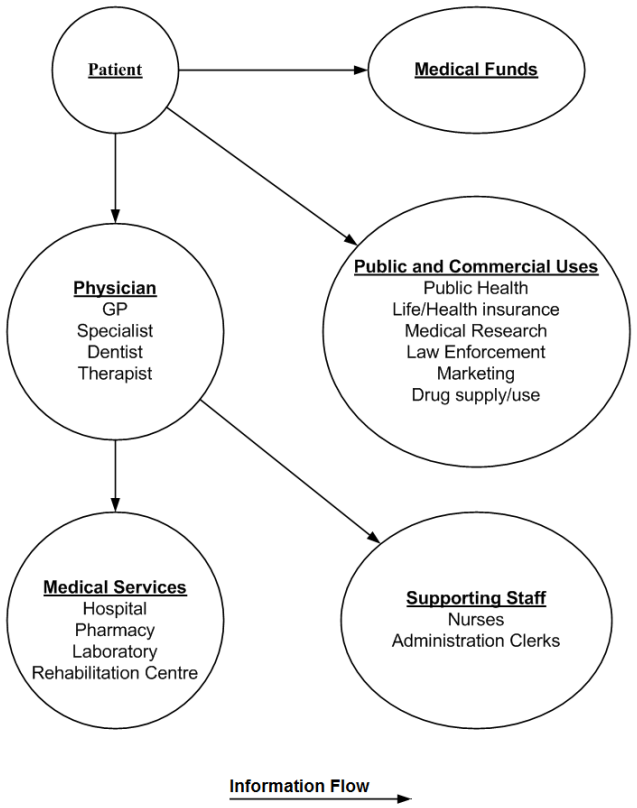


Figure 2.1: Sharing healthcare information (Ferraiolo et al. 2001)

Compliance with data protection legislation requires that access to a patient's information (paper or electronic) is governed by the relevancy of that information to the process of care, the role that the user plays, and potentially the explicit instruction of the patient (Government of Ireland 1988, Government of Ireland 2003). So access to the data must be constrained in accordance to the legislative and ethical environment as well as the sensitivity of the information, the context of care, and the wishes of the patient.

In certain circumstances, as with particularly sensitive information, unsuccessful requests for information on a patient should not even reveal its existence, as inferences can be drawn from existence alone. An access denied message, blocking the clinical details but revealing that a patient has a client identifier within a particular healthcare domain (mental health for

example) is already revealing too much information. On the other hand, care must be taken when classifying data, as these classifications may have future ramifications in the context of care. Access must be controlled, yet constraints and omissions must not mislead clinicians so as to cause harm or prevent a successful intervention.

Finally, the provision of healthcare often spans international borders, and Ruotsalainen (2004) argues that this trans-border communication is set to increase. Differences in legislation, ethics, standards, and technology present significant challenges to interoperable communications.

Clearly, the issues are complex. The research in this area focuses primarily on the reduction of this complexity, and this will be discussed in the following sections with respect to:

- Identification
- Authentication
- Authorisation
- Role-Based Access Control
- Sensitivity
- Policy Frameworks
- Policy Domains
- Audit

2.6 Identification

Uniquely identifying patients and system users across all interconnected systems is a critical requirement for the EHR (Chen, Berry & Grimson 2009). Implementing a common identifier allows the mapping of individual identifiers in healthcare systems to a single subject of care without ambiguity, and is essential for safe and efficient sharing of information among systems.

Additionally, identifying practitioners and organisations is an essential foundation to authentication services, authorisation, role management, data provenance and digital signatures, in an environment where healthcare workers commonly operate across different structural and functional roles and often across different organisations (public/private for example).

ENISO21091:(2013), *Health informatics - Directory services for healthcare providers, subjects of care and other entities* provides specifications for health informatics directory services to support interoperability and security of health information systems. The standard recognises that identifier management may by distributed, but must also support communication across organisations and national boundaries. The standard also provides for the registration of hardware devices and software, also discussed in (van der Linden et al. 2009).

Common identifiers at a national level is preferred, and HIQA's (2009) report outlines research and recommendations towards unique identifiers for individuals in Ireland, followed by (HIQA 2011) with recommendations concerning unique identifiers for practitioners and organisations. Both reports recommend identification at a national level, and both sets of recommendations require the enactment of legislation. The Health Identifiers Bill (2013) was published in Ireland in December 2013 covering the assignment of health identifiers for use in the public and private health services. This calls for the establishment of a National Register of Individual Health Identifiers (IHI) for patients and a National Register of Health Service Providers (HSP) covering health practitioners, health service organisations and their employees and agents. The bill requires the association of these identifiers with appropriate health records in any related communications. The bill is at the first stage of the legislative process and it is expected to pass into law in 2014.

2.7 Authentication

Authentication is carried out by ensuring that the person or system is who they say they are. Before the computerisation of health records, the reliable identification of those involved in a patients care was commonly based on individuals being known to each other, or by physical presence, or by the individual's status in the organisation. With the advent of electronic records, and in particular distributed EHRs, authentication from remote locations renders these traditional forms unreliable and redundant.

Authentication can be achieved through a range of methods; from username and password combinations, to token based access, and biometrics. However, the increasing use of health information technology has seen a rapid expansion in the number of credentials required in the day-to-day working environment. This is not sustainable, and the centralisation and integration of authentication services would provide a consistent and manageable approach while also enhancing security by enabling services such as single-sign-on (Neame 2000). This approach is consistent with the recommendations of ISO27799(2008) *Health Informatics - Information security management in healthcare using ISO/IEC27002.*

Strong authentication methods often rely on a combination of *something we hold* and *something we know*. This is exemplified in smart card technology where the smart card is the item we hold, and an associated pin is the item we know. Biometrics such as finger print reading or retinal scanning provide a step-up by authenticating the *someone we are* (Scarfo 2013). A systematic literature review of security and privacy in electronic health records (Fernandez-Aleman, Senor, Lozoya & Toval 2013), presents a range of solutions such as username/password combinations, digital signatures, digital certificates, smart cards and biometrics. In their review, articles based on digital signatures and Public Key Infrastructure (PKI) were in a clear majority.

Van der Linden, et al (2009) advise that authentication across different organisations can be achieved through either, a) registering individuals on systems in advance of use, or b) through registration on a centralised register common across all organisations. Given Ireland's direction with regards to the aforementioned Health Information Bill, the latter would seem most appropriate.

2.8 Access Control Models

Authorisation limits the actions that an authenticated individual may perform. Blobel (2004) describes a healthcare organisation as having thousands (potentially millions) of patients, each with thousands of pieces of health information, all being accessed by thousands of healthcare workers, constrained by an ever shifting need to know. The management of authorisation is complex, and requires the application of an access control model to assist. According to (Sandhu & Samarati 1994) three models are in widespread use: Mandatory Access Control (MAC), Discretionary Access Control (DAC) and Role-Based Access Control (RBAC).

2.8.1 Mandatory Access Control (MAC)

Mandatory Access Control (MAC) governs access to privileges based on a classification matrix of users and objects. Objects are assigned a sensitivity level, and users are assigned a clearance level. The relationship between the sensitivity level of the object and the clearance of the individual determines access. A common example cited in the literature refers to the military application of MAC, where objects are classified as Top Secret(TS), Secret(S), Confidential(C), and Unclassified(U). A user with a clearance (S) will have access to all of the objects classified as (S) and will automatically have clearance for (C) and (U) also.

2.8.2 Discretionary Access Control (DAC)

Discretionary Access Control governs access based on the privilege relationship of the user or group of users with each individual object. For example a user may have read, write or execute privileges, and access is granted or denied based on this. Users with full control over an object have the discretion to grant other users access, and so the dissemination of access control, while very flexible, is somewhat out of the control of the object owner. In addition, changes to the security attribute of one object requires the discovery of all dependent entries (Eyers et al. 2006). Microsoft Windows file-system is an example of where DAC is used.

2.8.3 Role-Based Access Control (RBAC)

MAC and DAC access control models are not well suited to the dynamic nature of healthcare. In their systematic review of security and privacy in electronic health records, (Fernandez-Aleman et al. 2013) discovered thirty-five articles relating to access control, of which twenty-seven referred to RBAC, making this model the "*access control policy of choice in EHR implementations*".

Role-based access control is a flexible model that assigns authority to a role rather than the individual. Users may then be assigned one or more roles, effectively inheriting the authority of the role(s). This separation of privilege and user allows changes in the profile of a given role to be immediately applied to all those associated with it. Equally, changes to an individual's job function could be reflected in assignment to new roles, with removal of role assignments that are not longer appropriate. This model greatly simplifies the management of privileges across an enterprise.

On behalf of the American National Institute of Standards and Technology (NIST), (Ferraiolo et al. 2001) proposed a standard for RBAC based on existing research, and grounded in an review of the deployment of RBAC in commercial systems. The article provides a reference model describing

common terms and concepts, and a functional specification for RBAC, and forms the basis for the ANSI (2004) standard ANSI 359-2004:*Role Based Access Control*. Concepts include:

Core RBAC

As described above, but including a sessional concept where roles are dynamically activated and mapped to a user in the course of a session (Figure 2.2)

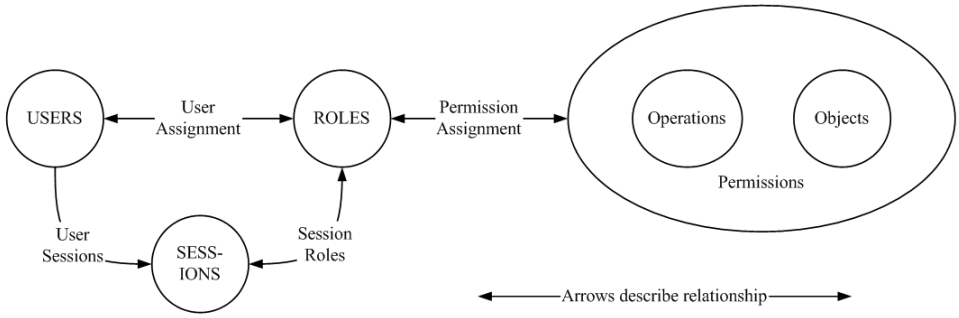


Figure 2.2: Core RBAC (Ferraiolo et al. 2001)

Hierarchical RBAC

Roles may be defined in accordance with a hierarchy (such as an organisational hierarchy) and permits the inheritance of privileges. For example, project workers on a project team may be assigned different roles depending on their function, each with different associated privileges. The project manager would ordinarily be assigned all of these privileges as part of his/her oversight responsibilities. One way to do this would be to assign the project manager each of the roles attributed to the project staff. Another, in accordance with the concept of hierarchical RBAC, would see a role defined as Project Manager which would inherit all of the privileges of the various subordinate project worker roles. For large organisations, this

has the potential to greatly simplify role assignment.

Constrained RBAC

Given the many-to-many relationships between users, roles and privileges, it is not surprising that conflict of interests arise. This is exemplified in the Separation of Duty relations (SoD); for example, in an accounting department, the person writing a cheque is usually not permitted to authorise it. Constrained RBAC is concerned with the negotiation and resolution of these conflicting and SoD policies.

Numerous extensions and variations to the basic RBAC model have been described in the literature. A Contextual-RBAC proposal builds on the NIST/ANSI model above and includes environmental factors, such as relationship to the patient at access time to determine access rights (Motta & Furuie 2003). Attribute Based Access Control (ABAC) also considers contextual factors such as relationships, location, and time in a system based on algorithms (Mohan & Blough 2010). In a different approach, (Peleg, Beimel, Dori & Denekamp 2008) propose a situation-based access control model (Sit-BAC) in which access scenarios discovered through qualitative analysis are represented in a situation schema. Access is granted based on the role of the user, and the context of access, as it relates to the situation rules defined in the schema.

Variants of RBAC in healthcare applications are mainly concerned with associating contextual dimension to the access decision. Contextual factors, as described above, might relate to the legitimate relationship of the care provider to the patient, and/or based on temporal constraints. Other factors might include the information distance model, which describes how privileges acting on patients data become more restricted as the distance between the information and the user increases. In this model, the patient is considered closest to the information (the data owner), the author of the

data, usually the primary caregiver, is next, and the distance increases with separation in the relationship to the information and the patient (users of the information).

Van der Linden et al (2009) cite another example where access to a patients data can become unrestricted in the event of an emergency. In such circumstances a patient may be incapable of providing the consent necessary to access relevant records, and so a clinician may override access control restrictions to access the necessary information, but must provide a subsequent report of the incident.

2.8.4 Structural and Functional Roles

To further simplify access management, it is useful to separately define structural and functional roles. Structural roles can be thought of as relating to the organisational structure, are usually coarse grained, and are most often associated with a competency or qualification - for example Doctor, Nurse, Clinical Director. Functional roles are more finely grained and are associated with actions - for example subject of care agent, prescribing doctor (Blobel, Nordberg, Davis & Pharow 2006). In this way, privileges are assigned to functional roles, which are in turn bound to structural roles. This subdivision allows structural roles (such as doctor) to remain reasonably static, while the functionality of the role can be highly dynamic. Further examples are provided in Table 2.1.

Separation of structural and functional roles is also important in the context of international communications. Structural roles can differ from country to country. For example, a nurse in one jurisdiction may have different responsibilities to that in another. However, action based functional roles such as 'prescribing doctor' are common across international boundaries. Blobel highlights the importance of internationally agreeing these functional roles so that differences in structural roles can be easily mapped through the functional equivalents (Blobel 2007). Standards such as the HL7 Permis-

Structural Roles Examples	Functional Roles Examples
Medical director	Caring doctor (responsible doctor)
Director of clinic	Member of diagnostic team
Head of the department	Member of therapeutic team
Senior physician	Consulting doctor
Physician	Admitting doctor
Medical Assistant	Family doctor
Trainee	Function specific nurse
Head nurse	
Medical student	

Table 2.1: Examples of structural and functional roles (Blobel et al. 2006)

sions Catalog (described below) play an important role here in terms of a common vocabulary for RBAC interoperability.

2.8.5 Role Engineering

Ferraiolo, Kuhn and Ramaswamy suggest that the *"biggest obstacle to RBAC is the initial complexity to setting it up"*, and they go on to describe the role engineering process as a *"technical , social and business process"* encompassing all of the activities associated with defining roles, permissions, constraints and assignments (Ferraiolo, Kuhn & Chandramouli 2007).

Neumann and Strembeck (2002) present a role engineering approach designed to elicit roles based on healthcare scenarios. Figure 2.3 presents their scenario model hierarchy where work profiles are made up of tasks, which are in turn made up of a combination of scenarios, described as a series of steps, each having associated permissions.

The scenario modelling process is iterative in nature, and (Neumann & Strembeck 2002) describe seven distinct steps:

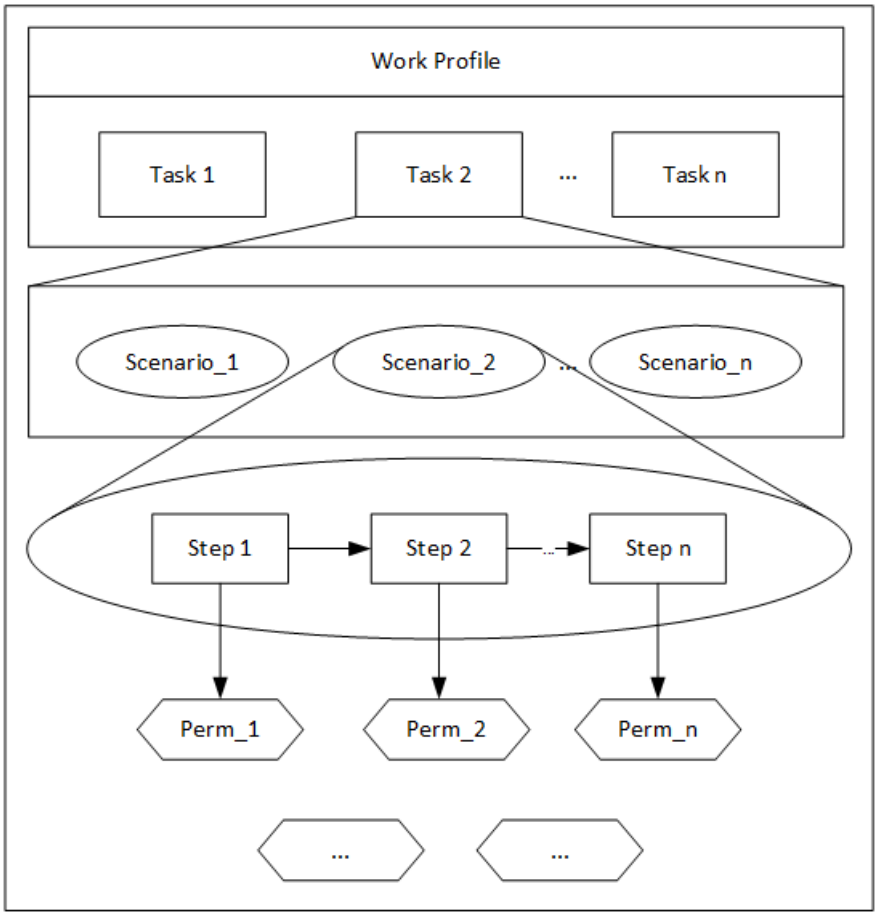


Figure 2.3: Role engineering scenario model hierarchy (Neumann & Strembeck 2002)

1. Identify and model usage scenarios: scenarios must be identified corresponding to system usage; for example "discharge a patient"

2. Derive permissions from scenarios: a list of permissions for each scenario must be compiled, associated with each of the steps that make up that scenario.

3. Identify Constraints: derive a list of any associated constraints; for example Separation of Duty (SoD)

4. Refine Scenarios: review and refine identified scenarios

5. Define tasks and work profiles: combine scenarios and associated constraints to form tasks, which are subsequently combined to form work profiles.

6. Derive preliminary role-hierarchy: analyse the resultant catalog of work profiles and permissions to identify commonality which can be represented in a hierarchy.

7. Define RBAC model: define the resultant RBAC model in terms of a role hierarchy, a permissions catalog and a constraints catalog.

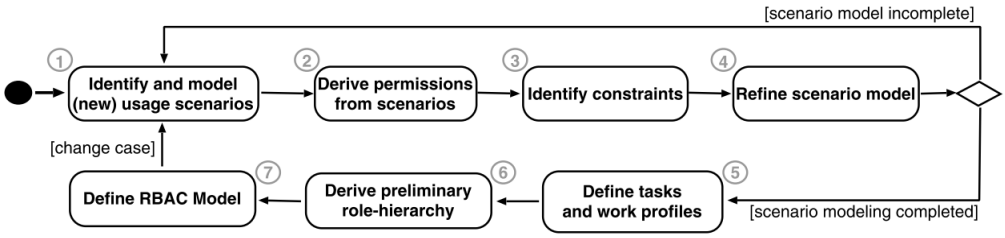


Figure 2.4: High Level view of role engineering process (Neumann & Strembeck 2002)

Neumann and Strembeck's approach has been adopted by the U.S. Department of Veteran Affairs (Ferraiolo et al. 2007), and also by the HL7 Security Technical Committee *"for the purpose of defining healthcare-specific permission standards"* (Health Level Seven International 2007).

The resultant HL7 Version 3 Standard: Role-Based Access Control Healthcare Permission Catalog (RBAC), Release 2, provides a normative permissions vocabulary, providing a comprehensive catalog of standard definitions for permission related *objects* and *operations*; see figure 2.2 earlier (Health Level Seven International 2010). *Objects* can represent any item that contains or receives information such as, for example, an immunisation list, while an *operation* executes some function for the user such as

READ or WRITE. Therefore in an example healthcare scenario which includes a review of an immunisation list, the associated permission is READ-Immunisation List (Operation-Object). Annex A to this standard provides examples of operation-object combinations based on a number of healthcare scenarios.

Additionally, the HL7 RBAC Constraint Catalog describes a process for the introduction of constraints into the role engineering process and also builds on and extends the work of Neumann and Strembeck (Health Level Seven International 2008).

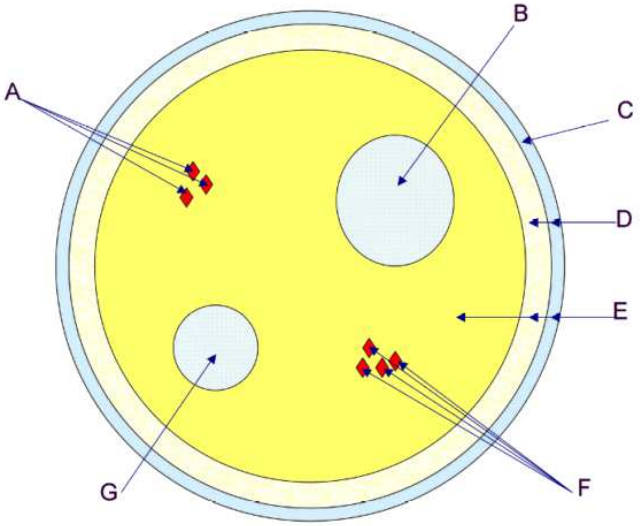
HL7 however, stops short of defining functional or structural roles (including role hierarchy), describing these as locally defined and currently out of scope (Health Level Seven International 2007).

Also in development by the international standard community is the ISO standard ISO/PDTS 21298:(2006) *Health informatics Functional and structural roles*, which provides a model for describing structural and functional roles, and additionally provides examples.

2.9 Sensitivity

The sensitivity of personal data can be classified. Basic demographic information such as name and address is generally considered less sensitive than data relating to, for example, a chronic disease, which is less sensitive again than data relating to sexual health. Sandhu and Samarati (1994) argue that classification of information can reduce complexity by allowing roles to access data based on it's classification rather than explicit assignments to each data object. This approach, recommended in EN13606-4(2007) *Health informatics - Electronic health record communication, Part 4: Security*, would see all data object assigned default classifications reflecting the norms pre-

vailing in the organisation. In situations where the default classification is inadequate or unacceptable, explicit instructions, such as consent information, can be recorded. An illustrative example is provided in the standard and reproduced in Figure 2.5



Key

A	Private entries shared with GP
B	Entries restricted to sexual health team
C	Entries accessible to administrative staff
D	Entries accessible to clinical support staff
E	Entries accessible to direct care teams
F	Private entries shared with several named parties
G	Entries restricted to prison health services

Figure 2.5: Default classification of healthcare information; reproduced from EN13606-4(2007)

In this example, the vast majority of the data is accessible to direct care teams. A subdivision is accessible by clinical support staff and a further subdivision by administrative and clerical staff. In addition to these subdivisions, islands of information exist expressing more sensitive information including the explicit wishes of the patient. The ISO18308 (2011) standard, *Health informatics - Requirements for an electronic health record architecture*, defines EHR architectural specifications which includes specific requirements for the capture of sensitivity information, including consent.

2.10 Policy Framework

As defined earlier a policy is a set of legal, political, organisational, functional and technical obligations for communication and co-operation.

Blobel (2006) suggests that formal security policies are required to negotiate access control agreements between the EHR systems and the access control infrastructure, and this is also the approach followed by the international standards community, incorporated into the draft standard ISO/DIS 22600-1,2,3:(2012*a*) *Health Informatics Privilege Management and Access Control (in three parts).*

Policies are highly dependent on the rules, regulations, and functionality of the organisation, and also the wider ethical, social and legislative constraints, and as such are not defined by the standards, but rather must be defined by the organisation or at a national level.

Policy driven access control allows the separation of the access management function from the underlying EHR(s). Providing a separate access control infrastructure makes the management of access control easier and provides for centralised and integrated access management. A request for access would invoke the access control infrastructure which would compute a decision based on the policy framework. For this to be automated, and to permit interoperability, policies can be encoded in a computer interpretable language. An example of this is provided by (Eyers et al. 2006) who describe how the policy language Casandra can be used with the Open Architecture for Secure Inter-working Services (OASIS), an established RBAC model, to interpret and negotiate complex policies including roles, hierarchies, and separation of duties.

The privilege management and access control standard ISO/DIS 22600-2 recommends that at least the following policies should be included in any framework (examples in each category provided by this author):

Patient control policy: Patient may wish to override default data classifications and explicitly exclude or include access to others.

Organisation common access rules policy: Examples include contextual policies which might express constraints relating to the ethical and social environment. Other policies in this category may relate to default sensitivity classification, the information distance model, and to emergency break-glass procedures.

Legislative and regulatory policies: Depending on legislative requirements, different levels of implicit and explicit consent may be defined.

One policy per role (structural and functional) RBAC policies concerned with role definition, the binding of privileges to functional roles, functional roles to structural roles and structural roles to individuals (known as principals in ISO/DIS22600). RBAC policies may also define sessional policies, hierarchical relationships and constraints such as Separation of Duty.

In combining these policies, access can be negotiated. And this is illustrated in Figure 2.6.

The ISO standard EN13606-4(2007) provides in it's Annex A, a series of scenario based use cases to illustrate how a simple two-dimensional policy-based access negotiation might work in practice.

Interoperable access control across organisational boundaries can be managed using Policy Domains, and this is discussed in the next section.

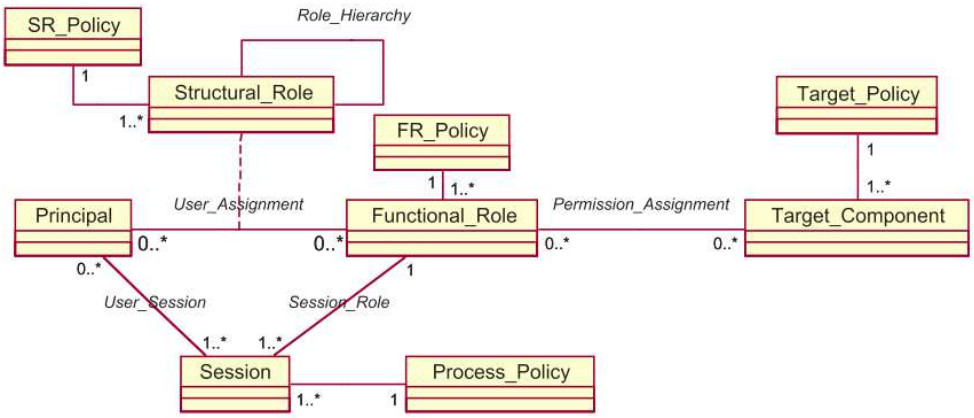


Figure 2.6: Role Based Access Control policy framework (European committee for standardization 2007)

2.11 Policy Domains

Policies may be defined at different levels known as policy domains. For example, policies may be defined at a national, organisational, departmental or service level; in fact any logical grouping may be defined as a domain. Furthermore, domains can be hierarchical so that a sub-domain may inherit the policies of the parent domain, but may also extend or specialise depending on the particular requirements of the sub-domain (Blobel et al. 2006).

This subdivision into domains has the potential to simplify the management of EHR communication. Interoperable access management within a domain is in accordance with a common set of policies. Inter-domain communication, where each domain is governed by a different set of policies, requires policy bridging. A bridging policy spanning domains can be described as a commonly agreed set of overarching policies. Domain incompatibilities may constrain the communication process in some respects and these must be noted in the agreement, along with a road-map towards resolutions and improvements in the scope of communication over time. ISO/DIS 22600-1(2012a) provides further guidance on domains, inter-domain communication and the drafting of bridging policy agreements. The standard acknowl-

edges that agreements may be in natural written language initially, but would eventually migrate to a computable format, automating the bridging process. To this end the standard suggests a common policy repository and directory services identifying all principles involved in the inter-domain communication and this is also dealt with in the standard.

Domains may also provide a mechanism for improved communications across national borders. Ruotsalainen (2004) describes the barriers to cross organisational communication as:

- legal and ethical differences,
- lack of common policies on trust, privacy and confidentiality, and
- lack of agreement on standards.

Ruotsalainen (2004) also proposes a cross-platform model for secure communication spanning security domains, and utilising policy bridging and complementary security services. The European standard EN 14484: (2003), *Health informatics - International transfer of personal health data covered by the EU data protection directive - High level security policy* provides additional support and guidance on the development of a high-level policy covering the secure transfer of health related data across borders.

2.12 Audit

Audit functionality is required to monitor security aspects of EHR access and information processing. Audit should capture all actions with respect to processing of personal information, including events and state changes (van der Linden et al. 2009). Audit logs can be used to ensure that EHR data is being accessed appropriately; the proper use of break-glass procedures being one example of this.

Distributed audit logs should be interoperable in order to trace all actions and operations in the context of an action on a distributed record, and

this also necessitates that distributed audit systems should be time synchronised. Standards are currently being worked on in this area, but no working example of interoperable audit logs currently exist (van der Linden et al. 2009).

In Fernandez-Aleman et al.'s (2013) literature review, twenty-five articles referred to the audit of health information systems. Of those, 5 articles advocate patient access to EHR audit logs to determine the who, the what, and the when their information was acted on, and in particular to review break-glass incidents.

Review of audit information can take the form of post analysis, or can happen in real-time through the integration of monitoring and intrusion alert systems which correlate patterns in access with either normal or suspicious behaviour.

In addition to access monitoring, audit can be used to support freedom of information requests, legal hearings, and can be used as a valuable input to the review of access control policy.

2.13 Conclusion

Privacy as a fundamental human right means that our information obtained for one purpose should be held securely, processed fairly, and should not be used elsewhere without consent. Public doubt in the ability of health services to meet this requirement can have negative impacts on health IT, and so measures concerning access control must be demonstrably robust.

This chapter described how the issues surrounding access control are complex, and that efforts to control this are based on simplification through the use of models, systems and frameworks. The chapter goes on to describe

how the implementation of these is influenced by many factors, including:

1. how roles are identified, structured and assigned,
2. how legislation, rules, regulations and ethics combine in policy frameworks and domains to compute access control decisions.
3. the way identifiers are defined and managed,

Emerging from this literature review, the following significant themes have been identified to provide a necessary framework, guiding the data collection and analysis processes for this study.

Authorisation

Role Based Access Control has emerged as the default access control model for healthcare information systems. Case country research should establish which access control model has been adopted in each country, and should explore the experiences of each case with regard to the establishment and ongoing management of the model.

In addition to basic RBAC, access may be further constrained and managed through, for example, contextual factors, data sensitivity and system audit. Case country research should explore theses additional authorisation factors that may impact on the overall access control strategy.

Consent Management

The requirements for consent management as it relates to the dissemination of personal health information are primarily driven by local legislative, ethical, social and cultural environments. These environments shape how, where and when patient consent is necessary and, accordingly impact on the overall access control strategy. Case country research and analysis should focus on each native environment, the resultant consent requirements, and the experiences of each case country in relation to implementation.

Identities and Authentication

Two identity types play a role in access control infrastructure:

- Patient identities ensure that the EHR record being accessed is correctly attributed to the person of interest.
- EHR user identities ensure that the user is properly authenticated, and that access to personal health information is being provided to authorised individuals only.

This research explores the role of identities, and establishes the management and methods of authentication for each case country.

Policy frameworks and policy domains are outside the scope of the case studies.

The following chapter will focus on the research methodology for this study, and will describe how the study was conducted, with reference to the themes identified above.

Chapter 3

Methodology

"Supposing is good, but finding out is better" Mark Twain

3.1 Introduction

In simple pragmatic terms, this research seeks to understand the what, how and why concerning the implementation of Health IT access control in a number of exemplar countries. It seeks to develop an understanding of the significant issues, to discover, to learn, and to develop a theoretical framework that can be reasonably applied elsewhere; in this instance, Ireland.

In order for the outcomes of this study to be viewed and accepted as valid and effective research, a methodology must be adopted that is appropriate to the question, is reliable, seeks to minimise bias, and above all is transparent. This methodology should chart the course of the journey from the initial question through to research design, data collection, analysis and reporting, and provide the reader with a clear understanding of how assertions were arrived at, the veracity of these assertions, and also the limitations.

The following sections in this chapter will describe the main research methodologies, the particular method chosen for this study, along with an outline of how the study was conducted.

3.2 Methodologies

3.2.1 Methodological Strategies

Methodological strategies can be defined in many ways, and Creswell (2003) presents three alternative strategies, broadly categorised as: quantitative, qualitative, and mixed methods.

Quantitative Approach

The quantitative research approach has its foundations in the natural sciences. It is concerned with the systematic analysis of a phenomenon involving the measurement of variables, and of numerical methods such as mathematical and statistical analysis. Typically, the analysis of data will yield a pattern or result that can be generalised to a larger population. Laboratory experimentation and surveys typify this type of research (Creswell 2003, Myers & Avison 2002).

Qualitative Approach

Qualitative research is rooted in the philosophical theory of social constructivism, where meaning is sought from the study of phenomenon and of individuals in their natural surroundings, and in the context of their social, historical, and organisational environment (Myers & Avison 2002). In other words, meaning is sought from the exploration of such phenomenon in the context in which they exist. In contrast with quantitative techniques, qualitative data is based on words rather than numbers and is combined from diverse evidentiary sources such as observations, interviews and documentation. Qualitative research is associated with the how and why questions, and the central objective is to "try to make sense of what is happening" (Kaplan & Maxwell 2005). Methods associated with the qualitative research strategy are many, and include the case study, ethnography, action research,

and grounded theory. These will be explored briefly in the later section on qualitative methods (See section 3.3.1).

Mixed Method

Though not relevant to this study, recent years have seen an increase in the use of mixing both quantitative and qualitative methods within a single study. When appropriate, this strategy combines the strengths of both approaches and can result in an outcome that provides a more subtle and richer analysis. It can also provide a mechanism through which one method can validate the findings of another, also known as triangulation (Creswell 2003).

3.2.2 Methodologies in ICT Research

Since the 1980s, Information System (IS) research has seen a shift of focus from primarily quantitative methods such as laboratory-based experiments or surveys (Galliers & Land 1987), to one which now also embraces qualitative analysis. This shift of emphasis clearly acknowledges that information systems are not implemented in a vacuum, rather they must operate in complex social and organisational environments (Kaplan & Maxwell 2005). Further to this, Benbasat, Goldstein and Mead (1987) point out that due to the pace of technological change and the associated requirement for immediate solutions, technology implementations are often somewhat ahead of theoretical research. In such cases, emergent theory is often informed through empirical studies of these innovations and actual practice, rather than theory exclusively driving innovation.

3.2.3 The methodology of Choice

In determining the correct strategic methodological approach, one must align the objectives of the study to an appropriate method of analysis. In the case of this study, we wish to understand the ways in which Health IT

access control is implemented in other countries and how this knowledge can influence a similar implementation in Ireland. It is clear from a reading of the state of the art chapter, that Health IT is complex, and highly sensitive to social and organisational dynamics, including legal and ethical aspects. These contextual influences cannot be separated from the technical requirements of an access control implementation. Instead they combine to provide solutions that are holistic and socio-technical in nature. Consequently, the qualitative approach is appropriate to this study.

3.3 Qualitative Method Selection

3.3.1 Qualitative Methods

Having chosen a qualitative strategy, the methods associated with that strategy determines the design of the study, and so requires our attention. Again, there are many variants of qualitative methods and Myers (2002) outlines four of the most popular:

Action Research

Action Research seeks to immediately solve problems or dilemmas within and during the course of the study in a collaborative and iterative way. In action research the researcher is actively involved in whatever change emerges as part of the research process.

Ethnographies

Ethnographies are concerned with cultural and behavioural aspects of a group or setting, where the researcher takes an observational approach *within* the setting being studied. These studies are usually carried out over longer time periods, are flexible, and evolve objectively over the course of the research.

Grounded Theory

Grounded Theory describes an iterative and systematic approach to data collection, analysis and theory development. With grounded theory, the emphasis is on the iterative nature of the research, continuously analysing data from a range of sources with each iteration of analysis informing the next phase of data collection, as patterns and theories emerge.

Case Studies

Case Studies are a flexible qualitative research method, primarily concerned with answering the how and why questions. Yin (2009) provides the following definition:

> *"A case study is an empirical inquiry that investigates a contemporary phenomenon within it's real-life context, especially when the boundaries between phenomenon and context are not clearly evident."*

The range of potential use of the case study in social science varies considerably. Studies can focus on a single event, or across numerous units of analysis. They can be historical, or more usually contemporary in nature. Case studies are an often used research method in political science, education, health, community planning and, according to Myers (2002) are the most common qualitative method used in information system research.
Of the four methods described above, Yin (2009) directs us towards the case study method where:

- the research questions are of a how and why nature
- we have no control over the subject events
- our study is contemporary in nature

The case study method also fits well with the chosen subject. The state of the art chapter clearly establishes access control as highly contextual to its surroundings, not just in terms of the technical architecture in which it sits, but also the legal, ethical, organisational, political and cultural aspects.

Consequently, the case study method is deemed appropriate.

3.3.2 Theory Testing versus Theory Building

This section briefly discusses two opposing philosophical approaches to the handling of theory in the context of the case study. The first approach, advanced by Yin (2009), is based on the positivist approach whereby hypothesis or propositions are proposed in advance of the study, much in the same way that we would predict the outcome of an experiment, and that the result of the experiment would test that prediction. According to Yin (2009), this method provides a focused approach to the research, and the validity of outcomes are easier to assert and are more believable.

Alternatively, Eisenhardt (2007) presents the case for an interpretive approach, whereby theory and hypothesis are built from an iterative analysis of the data, and ultimately emerge from the data. The researcher avoids hypothesising in advance of the study in order to maintain an open mind concerning emergent theory. This approach is particularly useful where there are gaps in existing theory and a sparsity of empirical study.

This is an important distinction since the choice determines the researchers frame of mind, influences the design, and thus the direction and efficacy of the research. Both theory testing and theory building approaches are valid, and the determination of the appropriate choice must be based on the research objectives and on the state of the existing theory. In this case the objective is to understand all of the factors relevant to the implementation of access control as part of the process towards developing successful solutions. Also, while the existing theory is well developed and mature in some respects, standards are sill in development in the area of roles in a healthcare environment (International Standards Organisation 2006), and there is a sparsity of empirical studies focusing on actual implementations of access control in Health IT at national levels. The circumstances around

this research more closely match the theory building approach and thus this method is adopted.

3.4 Case Study Design

3.4.1 Case Study Sampling

An important consideration when designing a study based on the case study strategy is the determination of the sample size. At a basic level, case studies can be based on a) a single case (unit of analysis) or on b) multiple cases.

Single-case case studies can yield exceptional results, and Yin (2009) provides numerous examples including a fascinating case analyzing the Cuban missile crisis. Yet he also argues that the validity of single-case research is difficult to assert. Eisenhardt (2007) agrees, claiming that the addition of *"just one or two or three more cases makes a difference"* and that, similar to the way in which a series of laboratory experiments can combine to illuminate a subject, adding cases has the potential to facilitate replication and/or contrast findings across the cases.

3.4.2 Case Study Evidence

Multiple sources of evidence is desirable since it not only widens and enhances the richness of the data, it also facilitates triangulation of finding across evidence types, and so enhances the validity and reliability of the findings. Yin (2009) discusses six potential sources of evidence, namely: documentation, archival records, interviews, direct observation, participant observation, and physical artefacts. In this research, case study evidence is sought from two primary sources: interviews and documentation, and this will be described in more detail later in sections 3.4.4, 3.5.6 and 3.5.7.

3.4.3 The Case Study Protocol

A case study protocol is required to ensure consistency and reliability across the cases, and serves to guide the data collection process in a professional and ethical way. The protocol sets out:

- Research Overview and Case Study Procedures
- Case Study Questions
- Interview Guide
- Information for Participants
- Ethical Request Form
- Consent Form

Each of these elements will be referenced later under section 3.5 (Study Execution), and an example case study protocol is included in Appendix A.

3.4.4 Interviews

Interviews are considered to be an efficient method for the collection of rich empirical data, providing a first-hand account of the phenomenon in question (Kvale 1996, Yin 2009, Eisenhardt & Graebner 2007). In the qualitative interview, and according to Kvale (1996), it is important to see the subject from the interviewee's point of view. Bryman (2004) agrees, stating that *"the emphasis must be on how the interviewee frames and understands issues and events - that is, what the interviewee views as important"*.

A semi-structured interview approach is taken, whereby the interviewer must strike a balance between providing sufficient flexibility to allow the interviewee freedom to explore topics that are considered important, but must also guide the interview across a range of themes which will, hopefully facilitate the emergence of patterns and associated theory across the cases. The interview should flow like a conversation on a topic of common interest, but should be directed by the interviewer (Bryman 2004).

3.4.5 Analysis

Analysis is a highly iterative process, and Eisenhardt (1989) recommends within-case analysis as an essential starting point. Within-case analysis involves the formation of a written narrative on each case, thus facilitating and structuring an intimate knowledge and familiarity with each case. These narratives may be subsequently scrutinised using a cross case pattern search method of analysis, involving the comparison of two cases at a time, and listing the differences and similarities of each pair. Resulting from this process, theories emerged which, in a cyclical process, are compared against the original data until valid reliable conclusions are reached.

3.5 Study Execution

This study was executed in accordance with the preceding theory, and broadly based on the stages listed below, and while these stages are presented as an ordered list, in reality their progress overlaps and interweaves in a cyclical fashion throughout the course of the project. For example, *documentation gathering* begins during the *literature review* stage and extends into the *analysis* phase as evidence is sought to corroborate an interview finding or to support a theory:

1. Setting the Study Goals
2. Literature Review
3. Methodological Selection
4. Designing the Case Study
5. Data Collection
    a) Interviews
    b) Documentation gathering
6. Results
7. Analysis and Discussion

Each of these phases are described in the following subsections.

3.5.1 Setting the Study Goals

The study goals, encapsulated in the research question below, were defined at the outset of this research as described in chapter one.

> *What can Ireland learn from the experiences of other nations towards the creation of an access control and consent strategy for a national Electronic Healthcare Record (EHR)?*

3.5.2 Literature Review

The study commenced with a thorough review of the literature to gain a clear understanding of the current state of the art relating to the theory in the chosen subject field, as presented in the preceding chapter. This literature review provided a foundation of knowledge on which to build this study, and facilitated the emergence of central themes on which to base evidence collection. These emergent research themes, identified in chapter two (section 2.13), are summarised here:

- Authorisation: An exploration of access control models, as well as additional authorisation factors that may impact on the overall access control strategy, including the context of care constraints, data sensitivity and audit.
- Consent Management: An exploration of consent issues having specific regard to the legislative, cultural and ethical environment, implementation strategies, and the resultant impact on access control infrastructure in each case country.
- Identities and Authentication: An exploration of the role of identities, and the management and methods of authentication for each case country.

3.5.3 Methodological Selection

Methodological selection (i.e a qualitative approach) has been dealt with earlier in this chapter and the associated methods are outlined in the following paragraphs.

3.5.4 Designing the Case Study

This case study design is based on the multiple case strategy. Each case, also known as a unit of study, is represented by a country or jurisdiction with an already established Electronic Health Record (EHR), and candidate countries were chosen primarily from those with an established relationship to the National Integrated Services Framework (NISF) in Ireland. A final selection would be based on the availability of suitable participants (domain experts working in an executive position of responsibility central to the themes of this research) agreeing to take part in a case country interview.

Requests for participation were sent by email. Of the eighteen individuals that received a request, ten did not respond and one declined on the basis of no longer being in a suitable role. Those that did respond either agreed to participate, or provided assistance with the identification of additional potential candidates. This process resulted in four persons across three countries offering to participate:

- England (1 participant)
- The Netherlands (2 participants - in a single shared interview)
- Canada, through participation of the New Brunswick Jurisdiction[1] (1 participant)

[1]Canada is a country consisting of a federation of provinces and territories, known as jurisdictions. Canada does have a national EHR programme overseen by Canada Health Infoway, however this programme is delivered at jurisdictional level, and so for the Canadian case, a jurisdictional EHR implementation by the province of New Brunswick is adopted as the unit of study. See Chapter 4, section 4.4.1

3.5.5 Case Study Evidence

Based on the main research themes identified in the State of the Art Chapter and summarised earlier, raw case study evidence was sought from two primary sources:

- interviews with domain experts working in an executive position of responsibility central to the themes of this research, and
- documentary artefacts such as national standards, policy documents, journal articles, etc.

3.5.6 The Interviews

Interview preparation began with the identification of questions as reflected in the research themes identified earlier. These questions are presented in Appendix A.2, and table 3.1 presents a mapping of the identified themes to the individual questions.

Research Theme	**Quest.**
Authorisation: An exploration of access control models, as well as additional authorisation factors that may impact on the overall access control strategy, including the context of care constraints, data sensitivity and audit.	1-6
Consent Management: An exploration of consent issues having specific regard to the legislative, cultural and ethical environment, implementation strategies, and the resultant impact on access control infrastructure in each case country.	7-10
Identities and Authentication: An exploration of the role of identities, and the management and methods of authentication for each case country.	11 and 12

Table 3.1: Mapping research themes to interview questions

During the recruitment process, potential candidates were provided with a

briefing pack which included:

- an outline of the nature of the study and the study procedures (Information for Participants - Appendix A.1),
- a copy of the Case Study Questions (Appendix A.2), and
- a Consent Form required to ensure the interviewees informed agreement to participate (Appendix A.3).

Additionally, an Interview Guide (Appendix B) was prepared to assist during the actual interviews. This guide was used to record circumstantial data such as interview location, the date, the time, specific notes, etc. as well as providing a listing of the interview questions (Yin 2009).

Having consideration for geographical constraints, interviews were conducted by phone, and were scheduled to last approximately 45 minutes. Also, in accordance with advice from (Bryman 2004), and with the consent of the participant, interviews were recorded to facilitate raw data analysis.

These measures were in line with the requirements of, and approved by, the Trinity College Dublin ethics committee.

Interviews were conducted in a single session, and in accordance with the above protocol. At the start of each interview a clear understanding of the purpose of the interview and the agreement to be audio recorded was reaffirmed, and noted on the associated Interview Guide. All interviewees agreed to be recorded. During the interviews, questions were not necessarily taken in order, but generally all identified themes were covered. At the end of each interview, participants were given the opportunity to ask questions or make further comments.

One additional question sought further documentation from interviewees to help validate and augment the interview findings, and this resulted in significant and valuable additional artefacts.

All interviews overran to 53 minutes (coincidentally). Recordings were transcribed within one week of each interview and transcriptions took on average five hours to complete for each interview.

Interview follow-up was necessary in one instance; a review of the English transcript revealed that critical information concerning patient relationships lacked clarity. A subsequent request to the interviewee through email resulted in a satisfactory clarification.

Subsequent to the interviews, the following observations were made:

- Although consent was identified as one of the emerging themes from the literature review, the extent of the impact of consent requirements was underestimated at the outset. Following the interviews, additional research into consent management including, for example, the societal attitudes towards consent requirements, revealed interesting and contrasting findings across New Brunswick and England in particular. Further research into Ireland's position also retrospectively strengthened section 2.3.1, page 9 of the State of The Art chapter.
- Similarly, discussions concerning the granularity of roles in each country's Role Based Access Control (RBAC) infrastructure revealed this as a critical area for consideration, and once again, an additional literature review was undertaken to more fully understand the theory and emergent standards in the associated area of role engineering. Consequently, chapter two was revised and now includes a dedicated section on role engineering (section 2.8.5, page 24).
- Patient identities, though critical for the operation of a national EHR, and for uniquely identifying the patient whose information is being accessed, does not however impact on the access control strategy. As a result, patient identifiers are not explored further in the Results or Discussion chapters.

Consequently, the central research headers were confirmed as follows[2]:

- Consent Management
- Identities and Authentication
- Authorisation

These themes provide a central structure for the research, forming the basis for evidence collection, and providing a consistent structure for analysis and reporting.

3.5.7 Documentation Gathering

Documentation augments the information found in the interviews. As stated earlier, this includes documentary artefacts such as national standards, policy documents and journal articles, which were obtained through a combination of internet searches and through documents directly provided by the case countries. All documentation is stored in a reference database (Endnote) and citations are used throughout the text, mapping to a bibliography for full traceability and transparency.

3.5.8 Results

Chapter four presents a series of within-case analyses in the form of case study narratives, and these narratives are structured in accordance with the theme headers outlined above.

3.5.9 Analysis and Discussion

The narratives presented in chapter four were scrutinised using a cross case pattern search method of analysis, involving the comparison of two cases

[2]Note that the presented order of the themes have changed, and this is to enable a more natural presentation of the narrative and analysis in the remaining chapters

at a time, and listing the difference and similarities of each pair. Themes progressively emerged from this process, and these were compared against the raw data until a clear picture emerged, along with considered assertions and recommendations.

The output of this analysis is presented in chapter five.

3.6 Conclusions

This chapter first presented a theoretical outline of research methodologies, progressively focusing towards qualitative methods and ultimately the case study method utilising the theory-building paradigm as the appropriate approach for this research. The case study method was further eiplored through discussions on case study design, protocols, interviews, documentation, analysis and reporting.

The execution of the study was also outlined, describing how the research unfolded, providing a clear and transparent account of how the final analysis and assertions were arrived at. This outline demonstrates the application of a methodological approach that stands up to the quality requirements of repeatability and dependability.

Under the heading of methodology, a number of challenges emerged that should be considered when assessing the validity of this research, and may also serve as useful considerations for any similar future work.

One of the more challenging aspects of the study related to the recruitment of candidate countries to participate in the study, primarily due to the poor response rate from prospective interviewees (section 3.5.6). One possibility that may account for the poor response rate could be attributed to the subject matter. Access Control and Consent closely relates to the processing

and security of our most precious private information, and this may have resulted in a reluctance to participate.

Another possibility could be attributed to participation fatigue. Health Informatics and associated solutions such as the interoperable EHR is a field that has yet to reach maturity. In an emerging field such as this, it is natural and appropriate for any country to look to the experience of other jurisdictions to help inform and shape their own approach on many aspects of Health IT. Often, the required knowledge and experience is found in the same pool of expertise in leading countries, and so the same group of people are frequently receiving requests to participate in similar studies. The sharing of knowledge in this field is important, yet the good will towards frequent participation in research projects such as this is perhaps tenuous.

Interviews also presented a challenge with respect to the time available to complete the interview. Such time constraints may present a challenge, particularly in a semi-structured interview where the interview is less regimented, and instead attempts to explore and tease out what the interviewee believes is important across the range of themes being discussed. One could easily spend several hours with each interviewee parsing and discussing the various aspects of the research topic, or alternatively schedule a series of interviews, each focusing on a particular theme. Yet this is not practical for a number of reasons:

- The reluctance of candidates to agree to participate would almost certainly increase as the level of commitment sought increases.
- Similarly, the good-will discussed in the previous paragraph is a valuable commodity and expending that on a single protracted study may be unwise and counter productive in the longer term.
- In studies involving geographically distributed interviewees, it is not always practical to physically meet the interviewee and so interviews are often conducted by phone - as was the case here. Telephone in-

terviews, out of courtesy to the participant, should be constrained to a reasonable length of time.

- The time to transcribe 45 minutes of recorded conversation is approximately 5 hours and produces about 12 standard pages of transcript (6000 words) per case, and so the interviews must be limited within the time constraints of completing the research.

One approach to meeting this challenge demands a thorough preparation for each case interview, involving an exploration of the available literature and country documentation to build a foundational understanding, and to familiarise oneself with the terms, acronyms, etc. in use in each case country. This permits the interview to quickly reach an appropriate depth, and also allows a rapid understanding of the issues being discussed.

Also, requesting additional information/documentation at the close of the interview, presents an opportunity to maximise this resource.

Challenges and limitations notwithstanding, the following chapter provides an outline of the results of the data gathering process, and this is presented as a series of within-case analyses, and structured in accordance with the main research themes described earlier.

Chapter 4

Case Study Results

4.1 Introduction

This chapter introduces the case studies. Each country: England, The Netherlands and Canada (New Brunswick) are presented in narrative form.

England and the Netherlands are presented first, followed by Canada in two parts; the first part provides the pan-Canadian perspective as envisioned and supported by Canada Health Infoway, and the second part outlines New Brunswick's implementation of that vision.

The structure of the narratives reflect the central research themes identified in the literature review, and which were further discussed in the previous chapter. They are:

- Consent Management,
- Identities and Authentication, and
- Authorisation.

Accordingly, evidence presented in these pages correlate directly to these themes, and information presented from the interviews can be traced to the original interview questions (see table 3.1).

Additionally, an initial section on context is provided at the beginning of each case country narrative.

Documentary evidence was compiled iteratively. Some case related material emerged during the literature review phase of this research, while additional materials were sought in advance of the interviews to provide foundational information, and to maximise the potential for each interview. Valuable artefacts were also contributed by the interviewees themselves, and interestingly, several issues emerged from the interviews that demanded further investigation, yielding additional interesting materials; for example, the impact of cultural attitudes on the different approaches to consent management.

The accumulated evidence from all documentation and interviews are presented here.

4.2 The English Study

4.2.1 Context

The National Health Service (NHS) is one of the largest publicly funded health services in the world, providing healthcare to over 63 million people throughout the United Kingdom (UK), taking in England, Northern Ireland, Scotland and Wales. England constitutes the larger part serving a population of 53 million, directly employing more than 1.35 million people, and catering for more than 1 million patients every 36 hours (NHS 2014).

In 2002, the National Programme for Information Technology (NPfIT) was commenced, representing a ten year, £11.4 billion investment in health IT, in an effort to maximise the use of information technology and so improve the quality and efficiency of healthcare (Comptroller and Auditor General 2011). Despite having a difficult and turbulent history, the NPfIT delivered

a number of significant infrastructural achievements (Department of Health, UK 2011). At the heart of this infrastructure sits the Spine; a central infrastructure that supports national services and programmes, including (among others) the:

Personal Spine Information Service (PSIS)

The PSIS is a central repository of clinical information uploaded from organisations involved in the direct care of the patient; for example GP practices.

Summary Care Record (SCR)

The SCR is an application which provides nationwide access to key clinical information found in the PSIS. In addition to demographics, the SCR provides a listing of allergies, current medications and known reactions. The service is primarily accessed by GPs, Out of Hours services and in Emergency Care settings.

In addition to these services, the Spine centrally hosts national information relating to the registration of system users and supports user authentication and authorisation. Beyond this central infrastructure, the NHS hosts more than 27,000 ICT systems across 21,000 organisations and these systems (at least the clinical ones) are collectively known as patient Detailed Care Records (DCR) (Health and Social Care Information Centre 2014*c*).

4.2.2 Consent Management

The term 'Information Governance' is used in the UK to describe the management and control of information securely, legally and effectively. Legally, the Data Protection Act (1998) enacts the EU Directive (95/46/EC), and governs the processing of data. However, the common law on confidentiality is the key legislation governing privacy and consent in the UK. This law is primarily based on individual judgments built up over time, and in

summary holds that information provided in confidence cannot be further disclosed beyond that originally understood by the provider of the information (Health and Social Care Information Centre 2013).

A report on the Review of Patient-Identifiable Information (1997) was commissioned by the UK government out of concerns being expressed by clinicians around patient consent and information governance in general. This report quickly became known as the Caldicott report (named after the author), identifying six information governance principles guiding the use of health information:

1. Justify the purpose
2. Don't use personal confidential data unless it is absolutely necessary
3. Use the minimum necessary personal confidential data
4. Access to personal confidential data should be on a strict need-to-know basis
5. Everyone with access to personal confidential data should be aware of their responsibilities
6. Understand and comply with the law

Issues around consent continued to hamper England's journey towards health information sharing (Greenhalgh, Stramer, Bratan, Byrne, Russell, Hinder & Potts 2010), and in 2013, a second report was published. The Information Governance Review (known as Caldicott2) outlined how consent had become the default basis on which information sharing decisions were being made and that healthcare professionals had become uneasy about sharing patient information due to uncertainty about when and where consent is mandated (Caldicott 2013).

This report attempted to clarify the boundaries around implicit and explicit consent and takes a more balanced view of confidentiality needs versus the

requirement to share information in the interest of the patient. The report reaffirmed the original principals along with one addition:

7. The Duty to share information can be as important as the duty to protect patient confidentiality

In the UK, consent is required at two points; firstly consent is required to capture and process data (consent to publish), and secondly consent is required to view data (permission to view). The first consent point may be implied in limited circumstances, including the default data set for the SCR:

> *"there is assumed to be a level of confidentiality when you disclose information to a clinician, so if you are holding out your arm for an injection for example, that's assumed to be you're consenting to that injection, but also the information surrounding it, and it is also assumed to be held in confidence" (UK Interviewee 2014)*

While the consent is implied for the creation of an SCR, patients are informed in advance, and are provided with opt-out options (NHS 2011). Implied consent to create an SCR is limited, and only holds for that information outlined earlier: patient demographics, allergies, current medications and known reactions. Patients do have the option to have additional information included in the SCR, but must provide explicit consent to the physician and this must be recorded in the record (Health and Social Care Information Centre 2014*a*).

When it comes to accessing information, explicit consent is required at all times under the principle "permission to view", however, while it is considered acceptable for the patient to provide this once for a given clinician or workgroup for the duration of a particular course of care, this is not always fully understood:

> *"if it's a different episode of care, then yes they should ask again, but these things are not clear in practice" (UK Interviewee 2014)*

Patients should also ideally be accommodated through additional privacy controls (consent directives), according to the NHS (Health and Social Care Information Centre 2012):

- Patients should have the facility to provide consent directives regarding who may view their record and how they may use it.
- Patients should have the facility to provide consent directives designating parts of their care record to be hidden (for example, mental health episodes, sexually transmitted disease information, etc.).
- It should be possible to override such directives in an emergency situation, or where legal or public health concerns prevail.

In practice the UK are *"struggling to make this work technically"* due to the diversity of existing Health IT, and this functionality is only implemented in one systems so far (UK Interviewee 2014). As a requirement for new Health IT, this is no longer mandatory and organisational controls are advised in its stead (Health and Social Care Information Centre 2012).

Echoing the Caldicott2 findings, the UK expert expressed the opinion that the notion of consent has to some extent overshadowed the circumstances in which information can and should be shared:

> *"I think we've got ourselves into a position where consent seems to be the de-facto ground for processing, it's assumed to be the grounds for processing personal information when other ones are probably more appropriate in a lot of circumstances and the reason I say that is that consent is difficult to pin down; it is difficult to pin it to a particular set of circumstances, it is difficult to limit it time-wise, it can be withdrawn, people don't understand what they're consenting to... it's just so complicated" (UK Interviewee 2014)*

Consent and information governance concerns have resulted in considerable debate in England, and were also identified in the Devil's in the Detail

(Greenhalgh et al. 2010) report as "wicked issues" contributing to the poor fortunes of the NPfIT .

4.2.3 Identities and Authentication

Users of Spine applications such as the Summary Care Record (SCR) are registered through a governance framework known as a Registration Authority (RA). The RA is a national service delivered locally by RA teams. In the first instance, users must be sponsored in order to apply as a user; organisations are required to nominate an RA sponsor who will approve user applications, associated job roles, activities and workgroups (Health and Social Care Information Centre 2014*b*).

Users must identify themselves to an RA using rigorous identification requirements defined in the e-Government Interoperability Framework - eGIF Level 3[1], before being issued with authentication credentials (UK Office of the e-Envoy 2002).

Access to Spine applications requires strong two-factor authentication (again eGIF level 3) and use of a smartcard and pass-codes issued by the RA (Health and Social Care Information Centre 2014*b*). In addition to authentication, smartcards contain user role information necessary for functional access (discussed next) (UK Interviewee 2014).

4.2.4 Authorisation

Role Based Access Control

National RBAC policies are guided by the national access control reference group made of a cross-section of users, clinicians, privacy and technical experts. This group also reviews applications for new roles or amendments to

[1] A now deprecated UK standard promoting information system interoperability, though still mandated for use by the NHS

roles or policies.

Structural roles were in the first instance based on the National Workforce Dataset consisting of several hundred roles. Over time, requests from local organisations for amendments or adaptations to these initial roles resulted in expansion of the list to many hundreds (UK Interviewee 2014).

> *"you might have one hospital trust that wanted their ward clerk to be able to look at prescription drugs and another hospital that their ward clerks couldn't look at drugs, and it became unwieldy" (UK Interviewee 2014)*

Recent years have seen a redesign and rationalisation of NHS job roles from many hundreds down to just twenty-five baseline structural roles (Appendix C), and a move towards an innovative and complex domain-hierarchical RBAC model, described by the UK as Position Based Access Control (PBAC). This PBAC model is depicted in Figure 4.1 and described in the following paragraphs.

In general, positions (structural roles) are mapped to activities (functional roles), and it is a users profile of associated activities that governs access (Health and Social Care Information Centre 2011).

A User Role Profile (URP) consists of (figure 4.1):

- A baseline role (BR). The baseline role will be associated with a number of baseline activities (A). For example the baseline role *R8010: Clerical Access Role* will include the activity *B0825: Amend Patient Demographics*
- The organisation (Org)
- Additional activities (A) which may be optionally added

The overall user profile determines the list of activities associated with a user and it is this that governs functional access and authorisation.

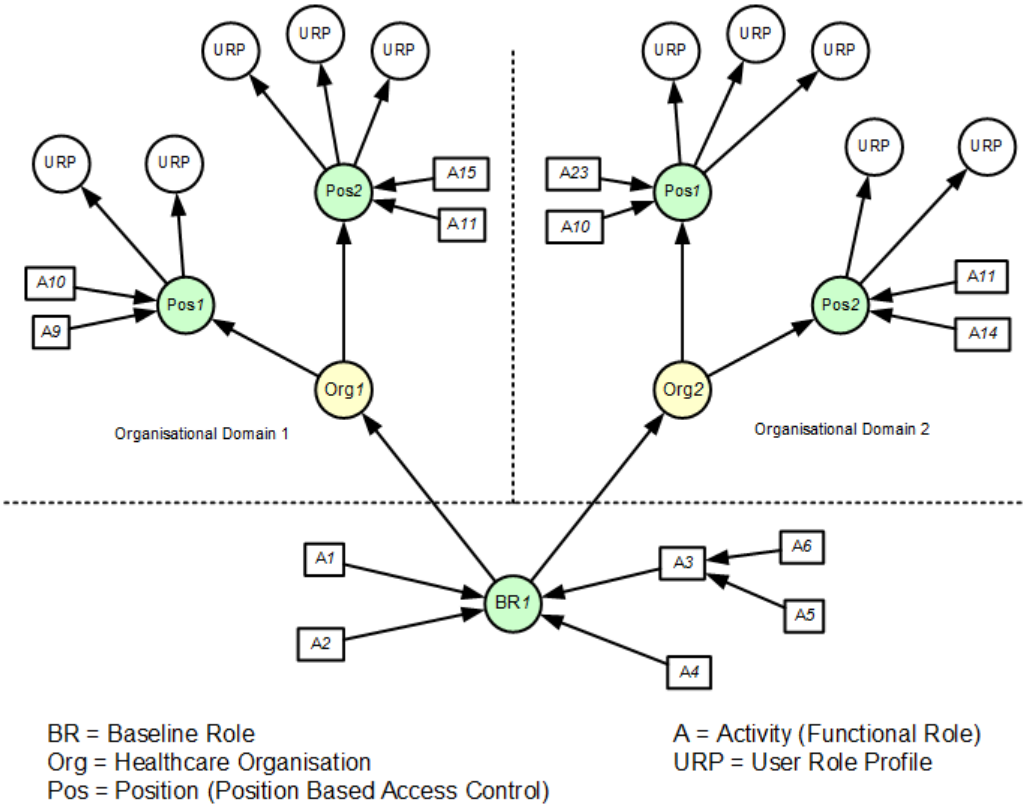


Figure 4.1: UK PBAC model - adapted from (Ferraiolo et al. 2007)

In order to simplify the administration of roles locally, user profiles may be associated with an organisational role known as a position (Pos). Users occupying the same position are assigned the same user profile, and so changes to the position propagate immediately to associated users. This is known in the UK as Position Based Access Control (PBAC). This is essentially a domain-hierarchy approach, where national baseline roles are defined centrally, while organisations have the flexibility of PBAC to meet local policy requirements (Health and Social Care Information Centre 2009).

As well as providing access control services to Spine applications, the integration of local Health IT systems to this infrastructure is also encouraged (UK Interviewee 2014)

Constrained RBAC

In addition to role based access, user access is further constrained by the context of care (contextual RBAC); a user may only access patient information if there exists a Legitimate Relationship (LR) to the patient. Legitimate relationships are established directly with a healthcare professional or through workgroup membership. Workgroups may be geographic or organisational in nature and are managed locally.

This requirement is supported by the Legitimate Relationship Service hosted on the spine. In most instances, a legitimate relationship is established in a Health IT system, for example, when a patient is registered or referred. A user may also access patient information by self-declaring a LR, though this action requires the user to provide a reason, and additionally the action raises an alert with a Privacy Officer who must verify the legitimacy of the access. A separation of duty policy avoids this alert by allowing a LR to be formed when two persons are involved; a clerical officer within a workgroup creates a LR (but without functional access to clinical information) while another in the workgroup may access the data (NHS - Connecting for Health 2013*a*).

Partially due to scale and scope of the UK's health information infrastructure, the Legitimate Relationship (LR) concept has been difficult to implement fully. The range and number of health information systems across the UK that must be modified to facilitate communication with the LR service has made this an ambitious and challenging task (UK Interviewee 2014).

Concerning data sensitivity as a potential constraint on access, the UK make a distinction between confidential and non-confidential information, however there is no sub-division or classification of confidential information.

Other Controls

Access control mechanisms such as permission to view, RBAC, legitimate relationships and privacy controls are implemented in technology. However there are other non-technical organisational controls recognised by the NHS (NHS - Connecting for Health 2013*b*), including:

- The Workplace Contract
- The NHS Codes of Practice and Legal Obligations
- The NHS Care Record Guarantee
- Professional Codes of Conduct

Audit

All NHS health information systems must maintain an audit trail of system use. Additionally, audit systems must be capable of generating alerts based on information governance policies. For example, a self-declared legitimate relationship generates an alert to the organisations Privacy Officer for investigation and verification (Health and Social Care Information Centre 2012).

4.3 The Dutch Study

4.3.1 Context

The Netherlands, though smaller in area than Ireland, has a population of over 16 million inhabitants. Health services are provided through private organisations overseen by national and regional governance, and funded primarily through a universal compulsory social health insurance scheme (Daley, Gubb, Clarke & Bidgood 2013, Flim 2010)

In 2002, the The National IT Institute for Healthcare (Nictiz) was founded as the national competence centre for health IT, charged with fostering positive conditions for health system interoperability, including (Nictiz 2014):

- the provision of knowledge and advice,
- the promotion of standardisation and interoperability,
- quality assurance, and
- stakeholder engagement.

In 2006, the Dutch government published a roadmap titled *ICT in Dutch Healthcare: An International Perspective*, and this document outlined the genesis and future development of a Dutch Electronic Health Record (EPD - Dutch abbreviation)(Ministry of Health Welfare and Sport 2006).

The EPD was developed by Nictiz in collaboration with the Ministry of Health, Welfare and Sport and the Central Information Point for Healthcare Professions (CIBG), and builds initially on two existing projects (Ministry of Health Welfare and Sport 2006):

- the Electronic Medication Record (EMD) which allows for the sharing of a patients medication history, and
- the Electronic General Practitioners Record (WDH) which provides a patient summary for the sharing of key patient information between GPs, locum GP services and out-of-hours services.

Plans to further evolve the EPD include the extension of the availability of the service to other professional groups, and the addition of modules such as diabetes as well as other chronic specialties (Ministry of Health Welfare and Sport 2006).

EHR interoperability is provided through a national infrastructure known as AORTA. Data is maintained in host systems connected to AORTA, and accessed and assembled only as required. The chosen architecture represents a federated model, whereby data remains at source and is assembled only as required. This is achieved through a central switch-point (LSP) providing reference indexing to patient data, authentication, authorisation, and audit. Systems connecting to AORTA must meet requirements as a

well managed system, and all traffic is encrypted (Ministry of Health Welfare and Sport 2006, van't Noordende 2010).

4.3.2 Consent Management

A range of legislation including the *Personal Data Protection Act* (implementing the EU Data Protection Directive 95/46/EC), the *Medical Treatment Contracts Act* and the *Use of Citizen Service Number in Healthcare Act* provide the current legal framework for information sharing in healthcare (Nictiz 2009, BakerHostetler 2014).

Further legislation was proposed in the form of the *Electronic Health Record Act* (EPD-wet), intended to make it compulsory for the related healthcare providers to participate in the national switch-point, and to establish an opt-out consent model for data sharing. In 2011 this proposed legislation was rejected by the Senate, thus reversing the consent model to one requiring explicit opt-in. In expectation that the EPD-wet act would pass, each household in the Netherlands had already received EPD information, including options for opting-out, and work had commenced regarding the population of opt-out registers: *"so we had to erase all the opt-out registered people and start all over again"* (Netherlands Interviewees 2014).

In addition to the legislative framework, a code of conduct, the *Electronic Information Exchange*, was drawn up by an umbrella group of organisations in the healthcare sector, extending the existing acts. This code of conduct provides specific direction on consent, including when consent is required and how and when to provide information to the patient.

In accordance with current legislation and the code of conduct, a patient must provide explicit opt-in consent to publish their data to the national infrastructure (consent to publish). Consent is normally obtained as patients attend their GP or pharmacy, can be provided verbally, but must be

electronically recorded by the health professional (Netherlands Interviewees 2014).

To date, approximately 1.5 million patients have provided their opt-in consent, and are already registered on the EPD (Netherlands Interviewees 2014).

While the above describes the requirement for consent to publish data, there is considerable debate in the Netherlands concerning permission to view. A new legislative proposal from the Dutch Ministry of Healthcare which is currently being considered proposes the requirement for consent at both points (consent to publish and permission to view), and additionally under the "necessity principle" provides for consent directives, affording the patient with specific control over who can see what (Netherlands Interviewees 2014).

Critics of this proposal claim that requesting consent twice is excessive and impractical, and that implementing specific consent directives is technically very challenging. The *Electronic Information Exchange* code of conduct takes an alternative approach whereby the healthcare professional does not require permission to view, however technical controls should instead verify a treatment relationship (discussed below) between the healthcare professional and the patient (Netherlands Interviewees 2014).

4.3.3 Identities and Authentication

In the Netherlands, healthcare providers are registered to the Professionals in Healthcare (BIG) registry and also to the Unique Healthcare Provider Identification (UZI) register. These registers are maintained by the Central Information Point for Healthcare Professions (CIBG), and this body also manages the provision of UZI smartcards. These smartcards enable identification and authentication to the LSP using PKI certificates, and also contain role attributes for all health professionals (Flim 2010, de Graaf,

Vlug & van Boven 2007).

4.3.4 Authorisation

Role Based Access Control

Authorisation on the national infrastructure is provided through Role Based Access Control (RBAC) and is managed by an authorisation service (AUT) located in the central switch point (van't Noordende 2010). Roles are assigned based on the BIG registry and access is determined using a two-dimensional matrix of roles on one axis and permissible actions on the other. Role to permission policies are currently decided by an Authorisation Commission, an umbrella group of healthcare organisations (Netherlands Interviewees 2014).

Considering the evolutionary nature of the Netherlands EPD, this RBAC arrangement has been mostly adequate to this point. However, some difficulties have been experienced concerning the relationship between role descriptions taken from the BIG register and a users actual care assignment:

> *"and that is because the BIG register was never created specifically for role based access control for the national infrastructure. That was never it's purpose" (Netherlands Interviewees 2014)*

Role granularity was also described as a significant issue during the interview. The broad granularity of the roles available on the BIG register have resulted in requests for more precise definitions. However, it is not possible to modify the BIG register for this purpose:

> *"if you set [granularity] too narrow it will give you a lot of problems and people wanting to override the situation and if you put it too wide, it doesn't make too much sense" (Netherlands Interviewees 2014)*

As the EPD evolves, expands and is accessed by a wider cohort of users, the limitations of the BIG register to facilitate adequate role assignments will become more difficult and in the opinion of the interviewees:

> *"we have to rethink this system. Personally, I don't think this system is sophisticated enough. They just used what they had at the time, and it worked for some time, but in the future, it won't be enough" (Netherlands Interviewees 2014)*

Constrained RBAC

As described earlier, a healthcare professional does not require permission to view consent if a treatment relationship with the patient may be verified using technical measures, thereby constraining access based on the context of care (Netherlands Interviewees 2014).

While this could be viewed as a more moderate approach to consent requirements, this technical establishment of a treatment relationship is not yet implemented. Furthermore, the Dutch interviewees point to the highly dynamic and complex nature of healthcare, and asserts that technically establishing a treatment relationship to control access to the patient record is very challenging and perhaps unnecessary:

> *"healthcare is nearly never organised so that all possible variants of treatment relations can be derived from systems, or found in databases, or administratively fixed somewhere" ... and ... "my personal opinion is, not on all points in society we make technically impossible what is forbidden... this is a thing to think about for a country such as Ireland, also for anybody; how far do you want to go"*

The Dutch participants advise that a more pragmatic approach may be appropriate. They suggest that access to a patient's record is controlled in the first instance by the role of the user, and subsequently, the logging and monitoring of all EHR actions and events, would provide the means to audit

user activity as a deterrent to inappropriate access.

Concerning data sensitivity as a constraint on RBAC - all healthcare data in the Netherlands EPD is considered to be at the highest level of confidentiality, and so does not play a role in determining access (Netherlands Interviewees 2014).

Audit

All audit activities take place at the NSP, recording at least the date and time of the access, the health professional UZI number, the patient's BSN, and the care application (de Graaf et al. 2007)

4.4 The Canadian Study

4.4.1 Context

Canada, with a population of over 35 million is a country consisting of a federation of ten provinces and three territories. Responsibility for healthcare in Canada is shared among federal, provincial and territorial governments, while operational responsibility for the delivery of healthcare is at the provincial and territorial level (also known as jurisdictions). The federal government is responsible for setting national policy, the provision of fiscal assistance and a range of specific health services including for example, public health (Health Canada 2014).

Under this arrangement, Canada Health Infoway, was founded in January 2001 by the federal government with a remit to "foster and accelerate the development and adoption of electronic health information systems with compatible standards and communications technologies on a pan Canadian basis" (Canada Health Infoway 2005). Canada Health Infoway's remit includes (Canada Health Infoway 2014):

- Promoting the adoption of health information technologies throughout the provincial territories,
- Provision of an architectural blueprint,
- Promotion of health information standards, and
- Vendor engagement, fostering a standards based approach in system development.

As such, the body have significant influence over the adoption of Health IT in Canada, yet have no executive responsibility.

Thus this case is described in two parts; the first outlines the pan Canadian position, mostly from the perspective of Canada Health Infoway, while part two presents an exemplar implementation in the province of New Brunswick.

Canada Health Infoway

Canada Health Infoway's EHRS Blueprint Version 2 (2006) presents a framework for pan-Canadian interoperable Electronic Healthcare Records. The blueprint describes architectural frameworks known as EHR Infostructures which which may be deployed at the provincial-territorial level. EHR Infostructures are built around key repositories (copies of original data) such as laboratory information, prescription records, diagnostic imaging and shared health records, and may be accessed directly via a dedicated portal known as an EHR viewer, or indirectly through existing information systems known as Point of Service (POS) systems. Figure 4.2 provides a conceptual outline.

Provinces-territories are incentivised to deploy EHRs that comply with Infoway's Blueprint, though at the same time there is significant scope within the framework for local decision. Infostructure implementation throughout the jurisdictions are advancing at different rates, and not all from the same starting point (New Brunswick Interviewee 2014).

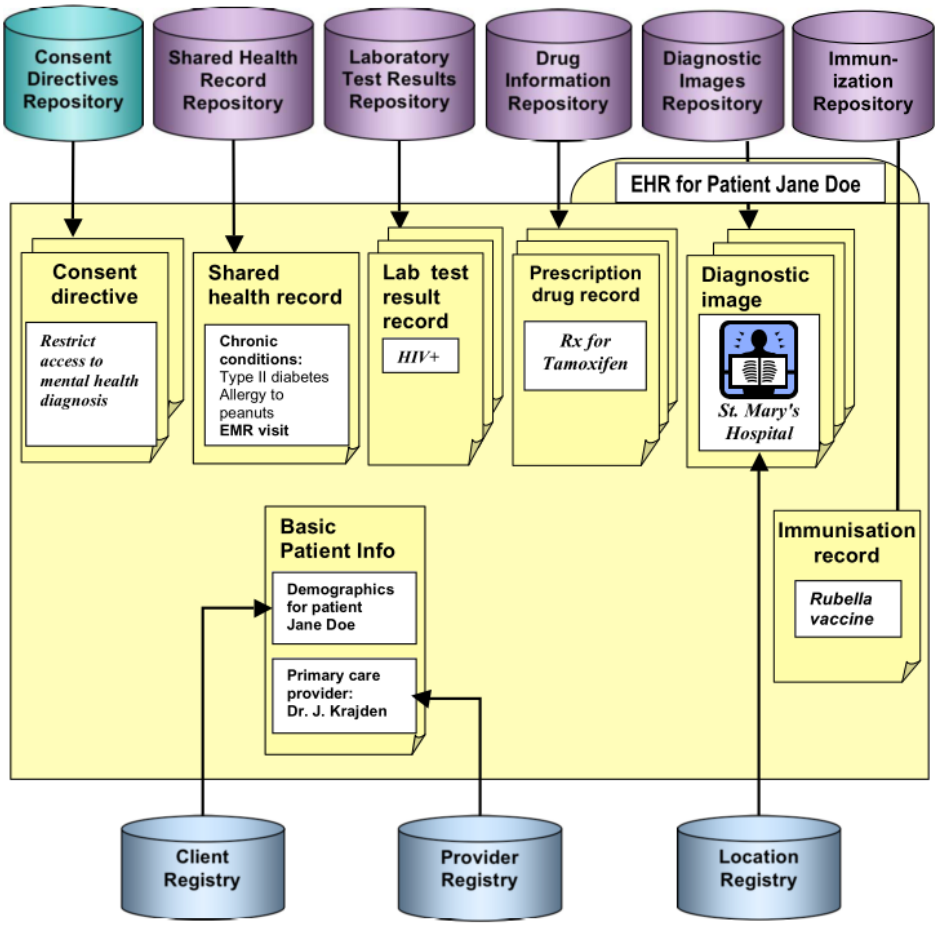


Figure 4.2: Infostructure conceptual outline. Reproduced from (Canada Health Infoway 2008).

4.4.2 Consent Management

One key area in which Canadian jurisdictions can differ is represented by the way in which privacy and related legislation differs across these jurisdictions. These differences in legislation have resulted in a range of consent models, including (Canada Health Infoway 2005):

- No consent (no consent required, however the patient may explicitly withdraw consent)
- Deemed consent (no consent required - cannot withdraw consent)

- Implied consent (functionally similar to no consent)
- Express consent (consent explicitly required for all information disclosure - Quebec)

Additionally, individual consent directives may be implemented by "masking" health information from view. Again, depending on legislation and local organisational policy, the masking of information may be overridden in circumstances such as in the context of emergency care, and reasons must be provided at the time. Masking can take place at a number of levels; for example the information domain level, the user role level or for a specific user (Canada Health Infoway 2005).

Consent directives are managed by means of a consolidated, centrally stored repository conforming to a national schema. Requests for information will check the consent directive repository, and apply any such directives before returning the data to the requester (Figure 4.3) (Canada Health Infoway 2012).

4.4.3 Identities and Authentication

Canada Health Infoway offers two methods of user identification (Canada Health Infoway 2008):

- For users indirectly accessing the Infostructure through a Point of Service (PoS), users can be uniquely identified through a combination of PoS ID + user's PoS identity.
- For users accessing the Infostructure directly, unique identities are centrally managed. Local Registration authorities validate requests for user IDs (in person) or alternatively by remote validation using a trusted information source such as a professional register.

Infoway does not advocate any specific authentication technology, describing this as a local governance issue (Canada Health Infoway 2005).

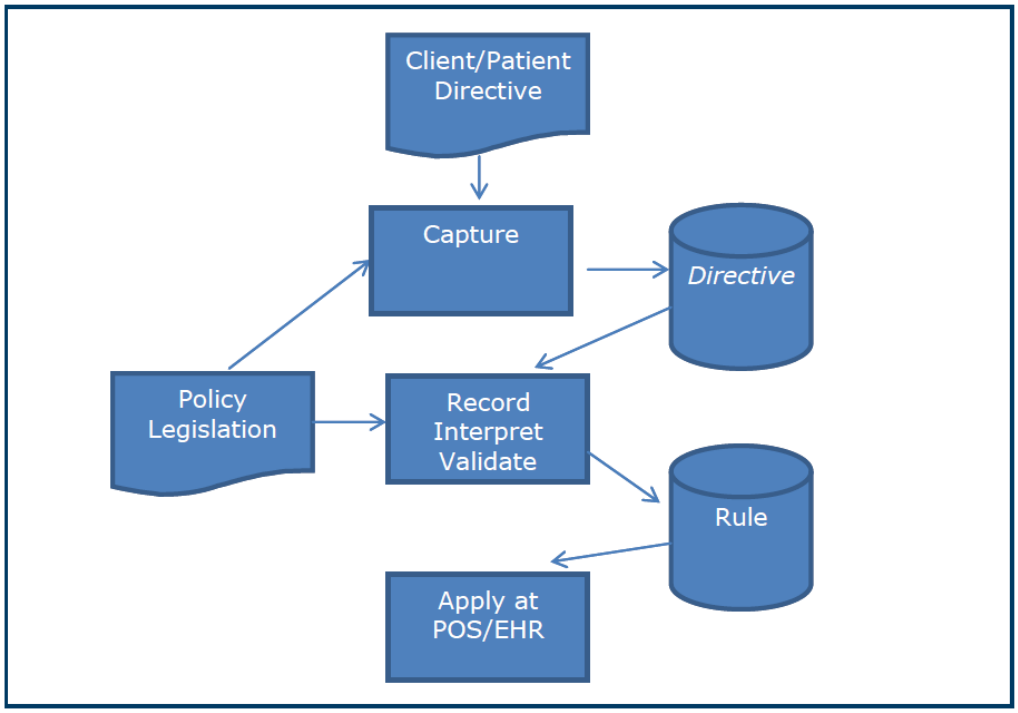


Figure 4.3: Consent directive process. Reproduced from (Canada Health Infoway 2012)

4.4.4 Authorisation

Role Based Access Control

Role Based Access Control can be based, for example, on professional roles which will determine the types and level of access appropriate to the profession. While Infoway's conceptual architecture sets out the requirement for a standardised set of roles at the EHR level, no specific advice is provided towards the use of a pan Canadian standard, or a specific role engineering process. The numbers and types of roles will be dependent on the level and range of service provided by each jurisdiction's EHR (Canada Health Infoway 2005).

Constrained RBAC

Access may be further constrained to membership of workgroups, including a Circle of Care concept; EHR systems infers membership of the Circle of Care based on those that have contributed (authored) data to the patient's record (for example a written prescription in a feeder system). Such members would have automatic access to the patients full EHR.

Concerning the classification of data, all personal data is equally classified as sensitive personal health information, and does not impact on access decisions. (Canada Health Infoway 2005).

Audit

The secure audit log service will create a secure audit record each time a user (Canada Health Infoway 2005):

- accesses, creates or updates patient information
- overrides the consent directives of a patient/person
- accesses data that is locked or masked by instruction of a patient/person; or
- accesses, creates or updates registration data on a user.

4.5 New Brunswick

4.5.1 Context

New Brunswick, on the eastern seaboard of Canada, has a population of approximately 800,000 citizens. In 2008, the government of New Brunswick published the *Provincial Health Plan: Transforming New Brunswick's Healthcare*. This plan outlined an ambitious reorganisation of healthcare delivery in the province and, amongst numerous structural reforms, described the introduction of:

> *"an electronic health record that will allow information from hospitals, doctors' offices, public health, mental health, pharmacies, laboratories and diagnostic imaging to be linked together and accessed by authorized care providers anywhere along the health-care system." (Government of New Brunswick 2008)*

Under the brand name *One-Patient-One-Record (OPOR)*, the New Brunswick EHR Infostructure has already met a number of the expectations outlined in the plan, providing provincial wide access to patient demographics, diagnostic imaging reports, laboratory results, cardiology results and, later this year, medication management. Access is provided primarily through a web-based iEHR viewer, and at this time the system can also accommodate direct access through at least one POS (New Brunswick Interviewee 2014).

4.5.2 Consent Management

In October 2010, the government of New Brunswick published the results of a provincial wide public engagement process whose purpose was to elicit New Brunswickers views on health system reform (New Brunswick Health Council 2010). The report found that citizens encouraged the greater use of technology in healthcare in order to promote operational efficiencies, health professional collaboration, reduce duplication and to make greater use of electronic health records. Caution was advised concerning confidentiality issues, though interestingly, the citizens overall attitude towards confidentiality was summarised as:

> *"ensure that privacy rules don't interfere with the ability to deliver timely service to patients"*

This attitude is in line with New Brunswick's position on consent. Health professionals may only access a patient record on a need to know basis, however, no patient consent is required to either create or view a record (New Brunswick Interviewee 2014).

A patient does however, have the option to explicitly submit a consent directive which will effectively block access to the clinical aspects on their record. The granularity of the consent directive is at the level of the entire clinical record; concerning a more granular approach to consent directives:

> *"No, we decided that we cannot do that. It would be too much work on our end. You block the record, you block the whole thing" (New Brunswick Interviewee 2014)*

Consent directives may be overridden in an emergency, however (New Brunswick Interviewee 2014):

- The user must select a valid reason,
- The action is audited,
- The patient must be informed, and
- The health professional must account for their action.

> *"they also know from their privacy training that if they break the glass, this is again monitored and they will be questioned" (New Brunswick Interviewee 2014)*

The consent position is enacted in legislation specifically brought forward in advance of the rollout of the EHR, and requires that the EHR is designated under the act as an information network. This requires the publication of designation documents detailing the use of the EHR, data sources, who the data will be released to, access control measures, etc. Changes to the EHR such as the inclusion of a new data source requires the revision of the EHR designation documents, and must be signed off at ministerial level (New Brunswick Interviewee 2014).

4.5.3 Identities and Authentication

New Brunswick does not have a common unique identifier for all health-care professionals. Users are registered using their professional registration number, license number or employee number, and numbers are all rigorously

checked before acceptance. Before users can apply for access to the EHR, they must be sponsored, and they must undergo mandatory privacy training (Appendix D). Training is delivered online, is bespoke, and a certificate of completion must be presented with an application before access can be assigned (New Brunswick Interviewee 2014):

> *"unless they do the privacy training, they are not getting access... we are very clear about the rights a patient have" (New Brunswick Interviewee 2014)*

All access requests, updates, amendments and rejections are logged, and an electronic workflow is currently being developed to manage the registration and associated logging processes (New Brunswick Interviewee 2014).

Authentication is provided through Active Directory using a username and complex password combination (New Brunswick Interviewee 2014).

4.5.4 Authorisation

Role Based Access Control

Access to the New Brunswick EHR is governed by Role Based Access Control (RBAC). The access control model is based on the principle that many users across different disciplines will require the same access profile; for example, an advanced paramedic may require the same access rights as a Registered Trauma Nurse. To facilitate this, access groups (AG) were formed and each assigned a particular set of privileges (P). These access groups are numbered rather than named to facilitate reuse, and structural roles (R) are then associated with a group (Figure 4.4)(New Brunswick Interviewee 2014).

Structural Roles, access groups and privileges are defined specifically for the purpose of the EHR by a multi-disciplinary access control committee, and strategically, these elements are only defined as required. This works well and though revision is regularly required, it is not considered excessive (New Brunswick Interviewee 2014). New Brunswick have however, found

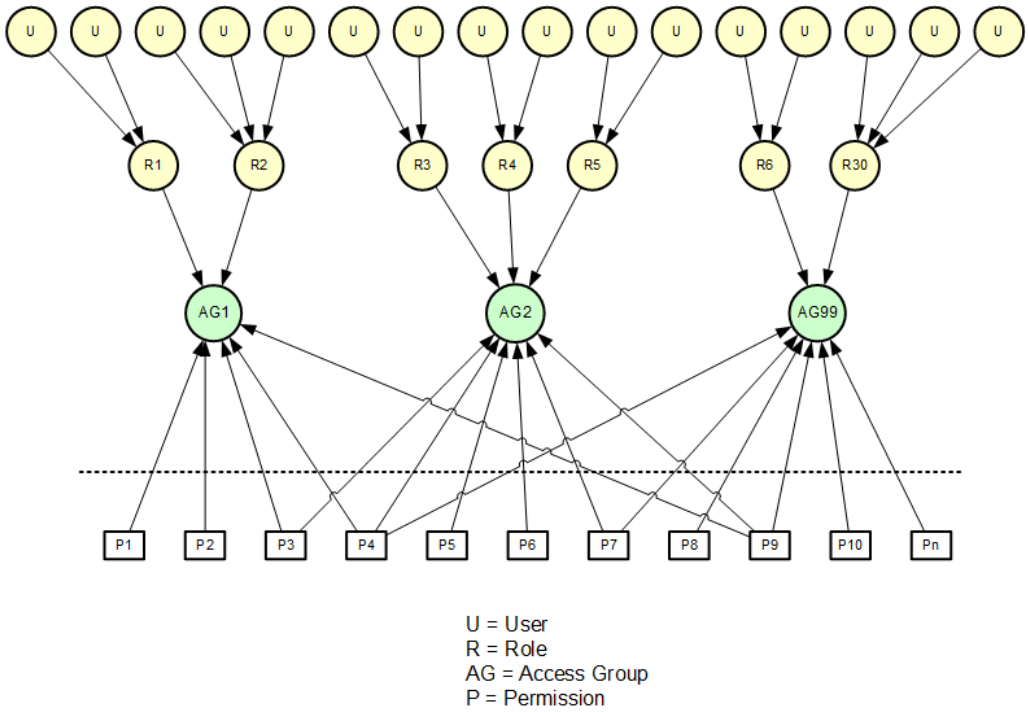


Figure 4.4: New Brunswick RBAC model - adapted from (Ferraiolo et al. 2007)

role design in the face of the need-to-know principle challenging and have cited specialisation a particular challenge, providing examples:

> *"pharmacists do work in very specialised areas; for example oncology . . . where they need to access the Diagnostic Imaging reports, whereas most of the pharmacists don't need it " (New Brunswick Interviewee 2014)*

The RBAC model must be flexible (New Brunswick Interviewee 2014). The addition of a new role requires the deliberation and evaluation of the committee, and any acceptance of a new role, or privilege, or data sources requires a consequential evaluation of existing roles and access groups:

> *"so it's a constant, whether it's the matrix or anything that has to do with privacy, its constantly being revised" (New Brunswick Interviewee 2014)*

Constrained RBAC

New Brunswick does not implement any form of legitimate relationship or circle of care concept, nor does the sensitivity of the data impact on the access decision. Access is governed in the first instance through RBAC, and thereafter the control of inappropriate access in managed through organisational controls; principally, privacy training, access logging and audit:

> *"[privacy training makes it] very clear that all access is logged and can be monitored at any time, and any user has to be ready to answer the famous question, why did you access this record? They [the users] are very much aware of that" (New Brunswick Interviewee 2014)*

Audit

As per Canada Health Infoway's recommendations, a secure audit log maintains a record of (New Brunswick Interviewee 2014):

- health information accesses
- consent directive overrides; and/or
- user registration or updates

4.6 Conclusion

This chapter described, in a structured narrative, the evidence collected against each case country. This evidence was gathered from a diverse range of documentation and from interviews with key personnel in each of the case countries.

The raw evidence was presented in these pages as it relates to the core research themes of:

- Consent Management,
- Identities and Authorisation, and
- Authentication.

Chapter five will present an overall analysis of these results including a series of twelve recommendations towards an access control and consent strategy for Ireland.

Chapter 5

Discussion

5.1 Introduction

Data analysis for this study was carried out by first developing a within-case narrative for each case country, thus developing a structural and intimate knowledge of each case, and this was presented in the preceding chapter. This was followed by an iterative process of cross-pattern matching by comparing and contrasting all cases, two cases at a time, searching for similarities and differences across both, and iterating through the cases until the emergence of new information was exhausted. Results from this analysis are presented here in four sections, along with arising recommendations to the National Integrated Services Framework (NISF), introduced in chapter one. These four sections are:

- Context
- Consent Management
- Authentication
- Identities and Authorisation

Country	Population
England	53 million
The Netherlands	16 million
Ireland	4.5 million
New Brunswick	0.8 million

Table 5.1: Population variance

5.2 Analysis

5.2.1 Context

The three case countries studied are quite different in terms of scale and, based on population alone, Ireland is closer to New Brunswick than either of the other two countries (Table 5.1).

The scope of implementation with respect to the access control infrastructure differs too. England recommends the use of their access control infrastructure in all areas of Health IT, integrating and providing single sign-on for many locally based detail care record systems. The Netherlands and New Brunswick on the other hand, deploy access control infrastructures specific to their EHR implementation only.

These differences in scale and scope can account in some part for the different approaches to each country's access control strategy. For example, the complexity of England's RBAC model must meet the requirements of their extensive enterprise wide implementation. On the other hand, issues around consent are less affected by scale, and more closely relate to the social, ethical and legal particulars of each country. Where appropriate, this will be referred to in the following discussions.

5.2.2 Consent Management

Compliance with privacy legislation is one of the principle drivers shaping the requirement for patient consent in each case country, that coupled with ethical codes of conduct and societal and cultural attitudes to privacy.

In the case of New Brunswick, specific legislation has been enacted to establish a health information network, setting aside any requirement for patient consent as it relates to the processing of personal health information (section 4.5.2).

England has no equivalent health information legislation, and consent requirements are based on non-healthcare specific instruments such as the EU Directive 95/46/EC (1995), the Data Protection Act (1998) and also on an interpretation of common law (section 4.2.2). In a similar way, the Netherlands rely on general privacy legislation, though proposals are currently being considered for a new healthcare information related bill (section 4.3.2).

Societal attitudes also appear to differ significantly across the countries. Patient consent has, and continues to be, a significant point of debate in both England and the Netherlands. Progress on EHR programmes in each country has been significantly affected by a lack of agreement on when and where explicit consent is required (sections 4.2.2 and 4.3.2). In England, this ongoing debate also feeds into a lack of clarity for healthcare workers on how existing rules should be applied, and this has resulted in a reluctance by some users to view patient information for fear of breaking consent rules.

New Brunswick however, through public consultation and the enactment of specific health information legislation, has dealt with consent in a more direct way. That this was done in advance of the One Patient One Record (OPOR) EHR Infostructure, provided a clear mandate and instruction on how sensitive information and the issues of consent should be handled. This public and legislative mandate is coupled with a clear commitment to en-

sure that all healthcare professionals clearly understand New Brunswick's position and obligations on data protection; principally applied through mandatory privacy training and continuous audit.

These various legislative, ethical and societal environments have resulted in different approaches by the case countries across a number of headings:

- Consent to Publish
- Permission to View, and
- Consent Directives

Consent to Publish

Consent to publish can be described as a patient's agreement to have their information included in an EHR, and requirements and implementations differ across the case countries.

The Netherlands require their citizens to explicitly opt in or out with respect to having an EHR record created, and this is realised progressively as Dutch citizens access their various health related services.

England assumes patient consent for the creation of their Summary Care Record (SCR); patients may opt-out, but must do so explicitly. The SCR may be extended beyond its basic dataset, though this extension requires the explicit consent of the patient.

Finally, with respect to consent to publish, New Brunswick, in accordance with its legislation, does not require its citizens to provide consent to have their health information added to their EHR Infostructure.

Permission to View

Patient consent may also be required at the point of information access, sometimes referred to as *permission to view*.

This requirement exists in the Netherlands, unless there is a technically enforced treatment relationship with the patient, at which point permission to view is not required; though this may change with the enactment of new legislation calling for explicit permission to view at all times.

England demands this explicit permission to view at all times, regardless of the presence of a legitimate relationship. For practical reasons, an explicit permission to view may be sought at the beginning of an episode of care, and this consent might hold for the course of treatment across all users involved in that treatment. England's interviewee has highlighted this as particularly complex. Episodes of care don't always progress in a straight line; illnesses can be intermittent, and are often complicated by additional related and unrelated health issues. And so it can be difficult at the outset of care to be clear about what set of circumstances the permission to view extends to, for what range of healthcare professionals, and whether some temporal constraint should apply.

In accordance with New Brunswick's legislation, consent to view an EHR record is not a requirement.

Consent Directives

Consent directives are concerned with the extent to which a patient may hide parts of their record or explicitly declare which individuals or groups may access and use their record.

England describes consent directives as *additional privacy controls*, and have had limited success in implementing technical control mechanisms (section 4.2.2). As a result, England have moved towards recommending that such directives are implemented be means of non-technical organisational controls.

In the other case countries, New Brunswick have implemented consent directives at high level only, that is, the entire clinical record, blocking all access, while the proposed legislation in the Netherlands calls for an implementation of consent directives at a more granular level.

Despite sharing a similar legislative foundation in the EU Directive 95/46/EC (1995), England and the Netherlands have clearly adopted different approaches to the three aspects of patient consent outlined above, and this is partly due to general privacy legislation in both countries and also partly resulting from the social and ethical forces prevailing in each country. Despite being some years into their respective EHR programmes, consent issues still generates considerable dialogue in both countries.

New Brunswick's approach to patient consent clearly simplifies their access control strategy, not just in the way that they have reduced their requirement to obtain consent, but also in the way in which they have clarified consent requirements in advance of their EHR programme, and also in how they have shown a clear commitment to ensure that no ambiguity exists among either the public or those working in the healthcare sector with respect to those requirements (sections 4.5.2 and 4.3.2).

Ireland's position concerning the EHR and the associated consent requirements (permission to publish, permission to view and consent directives) have yet to be defined. That position may well be nearer to its European neighbours due to closer legislative and cultural ties, and the 2008 consultation process on the proposed Health Information Bill shows us that there are already differences of opinion on what balance to strike between the personal right to control every aspect of our personal health information, and our right to receive the best healthcare through the appropriate sharing of that information (section 2.3.1).

Wherever our society chooses to strike that balance, we should learn from the experiences of the three case countries above by defining and agreeing

these consent requirements nationally in advance of an EHR deployment (ideally through the Health Information Bill), by clearly and unambiguously agreeing and communicating this consent position to the general public and healthcare workers alike, and by recognising the socio-technical limitations that make technology an inappropriate choice in enforcing every aspect of the patient consent requirement.

Recommendation 1:
In advance of Ireland's implementation of a national Electronic Health Record, following further public consultations as required, the proposed Health Information Bill should clearly set out Ireland's position on patient consent as it relates to the processing of personal health information in the context of a national Electronic Healthcare Record. The bill should clearly define consent requirement as they relate to:

1. Consent to publish: A potential requirement for consent with respect to a person's health information being included in a national EHR.
2. Permission to view: A potential requirement for consent with respect to a person allowing others to access their record.
3. Consent directives: The extent to which a person may provide instruction to hide or control access to specific aspects of their record.

Recommendation 2:
An overarching National Consent Management Policy is required, underpinned by and in accordance with the Health Information Bill. This National Policy and Code of Conduct should clearly describe:

1. Privacy and consent requirements
2. Agreed operational and procedural controls, and
3. The extent to which technology and organisational controls may combine to enforce this policy.

Recommendation 3:
A clear communication strategy is required to ensure that citizens have a clear and unambiguous understanding of their rights and how these rights are protected. A Privacy Impact Assessment, as recommended by HIQA, may form one aspect of that communication process.

Recommendation 4:
Healthcare workers must have a full understanding of the National Consent Management Policy set out in Recommendation 2. Mandatory training should form part of the EHR user registration process.

5.2.3 Identities and Authentication

Two main themes have emerged with respect to authentication:

- User Registration, and
- Authentication Mechanisms

User Registration

The user registration infrastructure and processes in England are considerably more complex than the equivalent function in either of the Netherlands or New Brunswick, involving a distributed registration service which locally confirms the identity of the applicant, maps the user to the appropriate user profile and issues the necessary authentication credentials and smartcard (section 4.2.3). In contrast, both the Netherlands and New Brunswick have centralised this function (sections 4.3.3 and 4.5.3), and this difference in implementation is most likely attributed to the differences in scale and complexity of England's implementation, as outlined earlier.

The unique identification of healthcare workers nationally is a critical requirement for a national access control infrastructure. The imminent National Register of Health Service Providers (HSP), proposed under the Health Identifiers Bill (2013) should be capable of providing this service (section 2.6).

Recommendation 5:
A centralised user registration service for access to EHR services should be established, and the imminent National Register of Health Service Providers (HSP) should provide unique identities to this registration service.

Authentication Mechanisms

While New Brunswick have opted for an Active Directory based username and complex password combination to manage authentication to their EHR, England and the Netherlands have both specified two-factor authentication,

and have implemented this through the use of smart cards. This conforms fully with ISO27799(2008) *Health Informatics - Information security management in healthcare using ISO/IEC27002* which states that authentication to health information systems *should* be controlled by means of at least two factors.

Robust authentication is a critical requirement to establish the identity of the user, to control authorisation and to ensure the integrity of, and non-repudiation of system audit.

Recommendation 6:
Authentication to an access control infrastructure should be based on two factors, in full accordance with ISO27799(2008) Health Informatics - Information security management in healthcare using ISO/IEC27002.

5.2.4 Authorisation

Areas of interest concerning authorisation arising from this case country analysis centered on the following main themes:

- RBAC-Role engineering,
- RBAC models,
- Constrained RBAC
- Data sensitivity
- Organisational controls

RBAC-Role Engineering

Role engineering was described earlier in chapter two - section 2.8.5 as encompassing all of the activities associated with defining roles, permissions,

constraints and assignments. Issues associated with the role engineering process emerged as having significant implications for at least two of the case study countries.

With respect to the definition of roles, England and the Netherlands both relied on existing registers as a basis for role assignments. England initially based their roles on the National Workforce Dataset, whilst the Netherlands relied on their Professionals in Healthcare (BIG) registry. Neither register was designed with RBAC in mind. Constant modifications to the register in England led to issues such as role sprawl, and in the Netherlands, experience has found too that roles based on the BIG register are often too broad in granularity or ill-fitting for purpose.

England has, over the past few years, significantly redesigned and rationalised their list of roles, while the Netherlands also expect that the inflexibility and broad granularity of the BIG register will require a re-evaluation of it's usefulness as their national EHR project evolves and grows.

New Brunswick in contrast, have taken a different approach, defining roles specifically for the EHR as the requirement arises, and to date, this has worked well.

Concerning the management of roles, common across all countries was the formation of a multi-disciplinary committee to manage RBAC assignments and consider amendments, and this appears to have been an appropriate approach and has worked well in all countries.

Clearly, a theme emerges here where the use of any existing professional register for the purpose of RBAC, however practical that might seem, will at best result in an inflexible and ill-fitting solution, and at worst will require a later redesign and replacement of existing roles.

Evidently, roles must be designed for purpose. A role engineering pro-

cess by Neumann and Strembeck (2002) provides an end-to-end model for defining permissions and roles (including hierarchies), and HL7 have based their role engineering standards and guidance on this model; though so far, HL7's guidance only extends as far as permission discovery, definition and catalogue. A role engineering process based on Neumann and Strembeck's scenario modelling would enable roles to be defined as required - as the EHR evolves and new scenarios emerge.

Recommendation 7:
Roles should be designed for purpose, and defined as required in accordance with the HL7-supported, scenario modelling role engineering process.

Recommendation 8:
A multi-disciplinary RBAC committee should be established to oversee the role engineering process, and to consider amendments and additions as they arise throughout the lifetime of the project.

RBAC Model

A Role Based Access Control (RBAC) model forms the basis for authorisation in all countries to varying levels of complexity. The Netherlands and New Brunswick have both implemented standard RBAC matrices closely conforming to Core-RBAC (sections 4.3.4 and 4.5.4), while England's RBAC model is considerably more complex utilising role, permissions and domain

hierarchies (section 4.2.4 and figure 4.1 for a diagrammatic representation of England RBAC model), and this reflects the scale and scope of England's access control deployment.

Role granularity, discussed in the previous section can influence the shape of the RBAC model too, and this is best illustrated in the challenges around role specialisation. England and New Brunswick's interviewees, both describe role specialisation as problematic in RBAC deployment. New Brunswick's interviewee for example indicated that:

> *"pharmacists do work in very specialised areas; for example oncology . . . where they need to access the Diagnostic Imaging reports, whereas most of the pharmacists don't need it " (New Brunswick Interviewee 2014)*

England's interviewee provided similar examples (section 4.2.4) citing this as one of the issues that ultimately led to England's move towards rationalisation and their Position Based Access Control (PBAC) model. Whilst the Netherlands did not specifically refer to specialisation as an issue, they did however highlight a lack of flexibility and granularity in their roles as an issue, and so it is reasonable to infer that they too experience problems with role specialisation.

Hierarchical-RBAC provides a flexible means to address this issue of specialisation in a way that minimises redundancy and role spread. Neumann & Strembeck's (2002) scenario modelling role engineering process, cited earlier, supports hierarchies and may be employed to define a hierarchical RBAC model.

Recommendation 9:
Authorisation control should be founded on a RBAC model. This model should be chosen with sufficient flexibility to allow role specialisation, avoid role spread and redundancy, and grow with Ireland's EHR implementation. As such, a Hierarchical-RBAC model is recommended, in accordance with the HL7-supported, scenario modelling role engineering process.

Constrained RBAC

Access control decisions may also be constrained or contextualised based on a number of factors, including the healthcare professional's treatment relationship with the patient. England implements this concept through it's Spine based Legitimate Relationship (LR) service. Relationships are established mostly in Health IT systems, and the number and variety of these systems have made this a daunting and difficult service to implement.

The Netherlands too have a patient relationship concept, though this country has not yet implemented a technical service that enforces or monitors such relationships. The Netherlands' interviewees argue strongly that establishing patient relationships in technology is difficult, and that mandating a technical barrier to data without a treatment relationship is a *"bridge too far"*, stating that:

> *"healthcare is nearly never organised so that all possible variants of treatment relations can be derived from systems, or found in databases, or administratively fixed somewhere"* and ... *"my personal opinion is, not on all points in society we make technically impossible what is forbidden"*

New Brunswick agree, and leveraging organisational controls (further discussed below) have chosen a trust based approach, backed up by robust

audit and monitoring.

Recommendation 10:
Technical enforcement of a treatment relationship between the healthcare worker and the patient should not form part of the access control decision, but should instead be subject to organisational control and audit.

Organisational Control

All three countries council the use of other non-technical controls to strengthen, and in some cases replace technical access control mechanisms. For example the UK cite the following organisational controls to augment technical authorisation mechanisms:

- Workplace contracts
- NHS Codes of practice and legal obligations
- NHS Care Record Guarantee
- Professional codes of conduct

The Netherlands too cite legislation and professional codes of conduct, and New Brunswick point to their mandatory privacy training at registration as a key component of their overall authorisation control strategy.

As with the discussion on patient consent earlier, clarity and consistency with regard to the overall access control strategy (technical and organisational control) is required to provide clear direction and enable healthcare workers to be confident in the decisions that they make with regard to accessing confidential patient information. A single overarching comprehensive policy effectively communicated is required to achieve this.

Recommendation 11:
Define an overarching National Policy on Access Control, encompassing both technical and organisational controls. This policy should be communicated as with Recommendations 3 and 4.

Audit

Given the maturity of audit functionality in health information systems in general, it is not surprising that all three countries have implemented EHR audit functionality, monitoring and logging all activity on patient information.

The UK have additionally implemented an alerting functionality that generates notifications to an Information Governance Privacy Officer, based on specified actions such as self-declaring a legitimate relationship (section 4.2.4).

All case interviewees agree that robust audit, along with high profile monitoring, can act as an effective control mechanism, providing a substantial deterrent to inappropriate access:

> *"if they break the glass, they must answer the famous question"... "[privacy training makes it] very clear that all access is logged and can be monitored at any time, and any user has to be ready to answer the famous question, why did you access this record? They [the users] are very much aware of that" (New Brunswick Interviewee 2014)*

Recommendation 12:
Implement a robust audit system which monitors at least:

- All activities on patient information
- Consent directive overrides
- Changes to user registration/role attributes.

Monitoring should be enhanced through the use of alert notifications, intelligent analysis solutions, and exceptions and alerts should be notified to an appointed information governance Privacy Officer.

5.3 Conclusion

This chapter outlined an analysis of the results presented in the previous chapter. The analysis is presented in accordance with the central research themes and, where appropriate, recommendations at a strategic level are provided to the National Integrated Services Framework, work-stream nine.

The research results and recommendations are summarised and presented in two tables, in Appendices E and F respectively.

The following chapter will provide a summation, including final conclusions and recommendations.

Chapter 6

Conclusions

Our fundamental right to privacy is of particular importance when it comes to our most personal healthcare related information. The issues and challenges surrounding the protection of that right have become all the more difficult as changes in the way healthcare is delivered demands greater levels in sharing of information, driving a need for healthcare information system integration, and ultimately the EHR.

The National Integrated Services Framework (NISF), a Health Services Executive (HSE) programme was set up to provide an interoperability framework to help meet that need. The programme is being delivered through a combination of twelve work-streams; work-stream nine relates to access control and consent issues, and the objective of this research, as outlined in chapter one, is to provide input to that work-stream through an exploration of, and learning from the experiences of other countries.

Chapter two presents a literature review, outlining the current state of the art in the associated topical areas, and provides an account of emergent standards in this relatively new field, in the context of national EHR programmes and implementations.

Chapter three describes an account of the research methodology, describing

how and why the case study method was chosen, and also presenting an outline of the progression of the study and the limitations and challenges encountered.

Some of the more significant challenges related to interviewing as a key source of raw case study evidence. Requests for participation to interview resulted in a poor response rate, and the resultant selection of case countries was thus limited to the three countries presented in this study. Chapter three, section 3.6 considers two possibilities for this poor response rate; the sensitive nature of the subject matter relating to the security of people's most sensitive healthcare information may have contributed in a reluctance to participate, and/or the possibility of participation fatigue, where a limited pool of suitably experienced staff in countries advanced in health informatics are frequently being asked to participate in similar studies.

In spite of this, interview participants were well positioned, senior staff, in roles central to the subject areas, and the selected countries proved excellent subjects, demonstrating both similarities and contrasts across the full range of research themes, yielding clear patterns from which dependable assertions could be made.

Also concerning the interviews, the wide breadth of the research topics under investigation contrasted significantly against the limited time available with interview participants. This challenge was met, insofar as possible, through thorough preparation in advance of each interview to maximise the output in the available time (again discussed in Chapter Three, section 3.6).

Chapter four presented a series of within-case analyses, structured narratives synthesising and outlining the evidence against each of the main research topics. This was followed by cross case analysis, methodically searching for emerging patterns against each of the central themes. These findings are presented in Chapter Five along with a series of recommendations to the NISF. Three themes of particular interest emerged, explored in

the following paragraphs.

All three countries expressed concern with regard to role granularity at some point during their EHR programme lifetime. This happened to such an extent in the UK that they entirely redesigned their RBAC model to one incorporating role hierarchies. The Netherlands too suggested that they may require a future re-evaluation of their user roles as their national EHR programme grows. Standards, though incomplete, exist in this area. HL7 in particular have published a standard and associated materials based on Neumann & Strembeck's (2002) scenario modelling role engineering process. The Neumann and Strembeck model as proposed, yields a hierarchical RBAC model defining permissions through to roles, yet HL7 stops short, providing a standard only for permission discovery, definition and catalogue. This research strongly suggests that in the context of a national EHR, with all of the complexity and diversity of use, successful RBAC models will demand the flexibility of role hierarchies, and that standards must extend to include the end-to-end role engineering process, including role and permission hierarchies.

The second theme which stood out relates to the extent of the impact of national debate on EHR programmes. Both England and the Netherlands, despite being a number of years into their respective programmes, continue to debate the appropriate interpretation of consent as it relates to the processing of personal health information. This continued debate clearly impacts on the EHR programme in both countries, resulting in delays and, in some instances, a lack of clarity around system use. In contrast, New Brunswick have resolved their consent issue in advance of their EHR programme and so have not experienced the same level of disruption to their ongoing EHR programme (though helped by the fact that they chose to implement a no-consent model). It should be clear that, regardless of the consent model adopted in any country, this debate should happen in advance of an EHR implementation, and the outcome should be enacted in specific healthcare legislation to reflect the national position.

Finally, a common theme expressed across all three countries was the appropriate balancing of technical versus organisational controls to effect the overall access control strategy. The mechanisms to fully enforce legitimate patient relationships, or indeed every potential aspect of consent are considered highly complex and perhaps overambitious, and a greater reliance on organisational and ethical controls are advised.

These three themes underpin the twelve recommendations to Ireland's NISF programme, and represent the central contribution of this research. The research also contributes by clearly demonstrating a real and present need for end-to-end role engineering standards.

Concerning potential future work, an in-depth study of England's Position Based Access Control model would also be, I believe, of interest to the Health Informatics standards community working in this specific area, and may also contribute to the field of RBAC control generally.

In conclusion, privacy is not entirely dead, and the issues and concerns around the maintenance of the privacy of our health information are complex and very much alive. This dissertation provides an overview of the current state of the art and, having regard for these issues and complexities, has explored and analysed the experience of three countries, which has resulted in the presentation of a series of recommendations towards an access control and consent strategy for an Electronic Healthcare Record (EHR) in Ireland.

Bibliography

American National Standards Institute (2004), 'ANSI INCITS 359-2004, Role Based Access Control'.

BakerHostetler (2014), International Compendium of Data Privacy Laws, Report.
`http://www.bakerlaw.com/files/Uploads/Documents/Data20Breach20documents/International-Compendium-of-Data-Privacy-Laws.pdf`

Becker, M. Y. (2007), 'Information governance in NHS's NPfIT: A case for policy specification', *International Journal of Medical Informatics* **76**(5), 432–437.

Benbasat, I., Goldstein, D. K. & Mead, M. (1987), 'The case research strategy in studies of information systems', *MIS quarterly* **11**(3).

Blobel, B. (2004), 'Authorisation and access control for electronic health record systems', *International Journal of Medical Informatics* **73**(3), 251–257.
`http://www.ncbi.nlm.nih.gov/pubmed/15066555`

Blobel, B. (2007), 'Comparing approaches for advanced e-health security infrastructures', *International Journal of Medical Informatics* **76**(5-6), 454–9.
`http://www.ncbi.nlm.nih.gov/pubmed/17074532`

Blobel, B., Nordberg, R., Davis, J. M. & Pharow, P. (2006), 'Modelling privilege management and access control', *Int J Med Inform* **75**(8), 597–

623.
http://www.ncbi.nlm.nih.gov/pubmed/16199198

Bryman, A. (2004), *Social Research Methods*, Oxford University Press, Oxford, UK.

Buntin, M. B., Burke, M. F., Hoaglin, M. C. & Blumenthal, D. (2011), 'The benefits of health information technology: a review of the recent literature shows predominantly positive results', *Health Affairs* **30**(3), 464–471. Health Affairs.

Caldicott, F. (2013), Information: To share or not to share: Information Governance Review, Report.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf

Canada Health Infoway (2005), 'Electronic Health Record Infostructure (EHRi): Privacy and Security Conceptual Architecture'.
https://knowledge.infoway-inforoute.ca/EHRSRA/doc/EHR-Privacy-Security.pdf

Canada Health Infoway (2006), 'EHRS Blueprint: an interoperable EHR framework - Version 2'.
https://www.infoway-inforoute.ca/index...
/284-ehrs-blueprint-v2-full

Canada Health Infoway (2008), A 'Conceptual' Privacy Impact Assessment (PIA) on Canada's Electronic Health Record Solution (EHRS) Blueprint Version 2, Report.
https://www.infoway-inforoute.ca

Canada Health Infoway (2012), 'Business and Architecture Considerations for Interoperable Consent Solutions: A discussion document'.
https://www.infoway-inforoute.ca/index.php/component/docman/doc_download

Canada Health Infoway (2014), 'What we do'.
`https://www.infoway-inforoute.ca/index.php/about-infoway/what-we-do`

Chen, X., Berry, D. & Grimson, W. (2009), Identity management to support access control in e-health systems, Springer, pp. 880–886. 4th European Conference of the International Federation for Medical and Biological Engineering.

Chhanabhai, P. & Holt, A. (2007), 'Consumers are ready to accept the transition to online and electronic records if they can be assured of the security measures', *Medscape General Medicine* **9**(1), 8. WebMD/Medscape Health Network.

Comptroller and Auditor General (2011), The National Programme for IT in the NHS: an update on the delivery of detailed care records systems, Report, National Audit Office.

Connolly, P. (2013), 'Presentation - National Integrated Services Framework'.
`http://hisi.ie/pdfs/15.15%20HISI%205%20Peter%20Connolly.pdf`

Council of Europe (2010), 'European Convention on Human Rights'.
`www.echr.coe.int/Documents/Convention_ENG.pdf`

Creswell, J. (2003), *Research design: qualitative, quantitative, and mixed methods approaches*, SAGE Publications.

Daley, C., Gubb, J., Clarke, E. & Bidgood, E. (2013), Healthcare Systems: The Netherlands, Report, Civitas: The Institute For The Study Of Civil Society.
`www.civitas.org.uk/nhs/download/netherlands.pdf`

Data Protection Commissioner, Ireland (2014), 'Data Protection Rule 1: Fair Obtaining and Processing'.
`www.dataprotection.ie/viewdoc.asp?DocID=23`

de Graaf, J., Vlug, A. & van Boven, G. (2007), 'Dutch virtual integration of healthcare information', *Methods of information in medicine* **46**(4), 458.

Department of Health and Children, Ireland (2008*a*), Proposed Health Information Bill: Synopsis Of Submissions Received Under Public Consultation Process, Report, Department of Health and Children, Ireland,.

Department of Health and Children, Ireland (2008*b*), Tackling chronic disease: A policy framework for the management of chronic diseases, Report.
`http://www.dohc.ie/publications/tackling_chronic_diease.html`

Department of Health, UK (2011), 'Dismantling the NHS National Programme for IT - Press release'.
`https://www.gov.uk/government/news/dismantling-the-nhs-national-programme-for-it`

Eisenhardt, K. M. (1989), 'Building theories from case study research', *Academy of management review* **14**(4), 532–550.

Eisenhardt, K. M. & Graebner, M. E. (2007), 'Theory building from cases: Opportunities and challenges', *Academy of Management Journal* **50**(1), 25–32.

European committee for standardization (2003), 'EN 14484:2003, Health informatics - International transfer of personal health data covered by the EU data protection directive - High level security policy'.

European committee for standardization (2007), 'EN 13606-4:2007 Health informatics - Electronic health record communication, Part 4: Security'.

European committee for standardization (2008), 'EN ISO 27799:2008, Health informatics - Information security management in health using ISO/IEC 27002 (ISO 27799:2008)'.

European committee for standardization (2013), 'EN ISO 21091:2013, Health informatics - Directory services for healthcare providers, subjects of care and other entities'.

Eyers, D. M., Bacon, J. & Moody, K. (2006), 'OASIS role-based access control for electronic health records', *IEE Proceedings-Software* **153**(1), 16–23.

Fernandez-Aleman, J. L., Senor, I. C., Lozoya, P. A. & Toval, A. (2013), 'Security and privacy in electronic health records: a systematic literature review', *Journal of biomedical informatics* **46**(3), 541–62. `http://www.ncbi.nlm.nih.gov/pubmed/23305810`

Ferraiolo, D. F., Sandhu, R., Gavrila, S., Kuhn, D. R. & Chandramouli, R. (2001), 'Proposed NIST standard for role-based access control', *ACM Transactions on Information and System Security (TISSEC)* **4**(3), 224–274.

Ferraiolo, D., Kuhn, D. R. & Chandramouli, R. (2007), *Role-based access control*, second edn, Artech House.

Flim, C. (2010), Country Brief: Netherlands, Report, European Commission.

Galliers, R. D. & Land, F. F. (1987), 'Viewpoint: choosing appropriate information systems research methodologies', *Communications of the ACM* **30**(11), 901–902.

Government of Ireland (1988), 'Data Protection Act 1988'. `http://www.irishstatutebook.ie/1988/en/act/pub/0025/index.html`

Government of Ireland (2003), 'The Data Protection (Amendment) Act 2003'.
http://www.irishstatutebook.ie/2003/en/act/pub/0006/index.html

Government of Ireland (2013), 'Health Identifiers Bill 2013'.
http://www.oireachtas.ie/viewdoc.asp?DocID=25072&&CatID=59

Government of New Brunswick (2008), Transforming New Brunswicks Health-care System: The Provincial Health Plan 2008-2012, Report.
http://www.mindbank.info/item/1751

Government of the United Kingdom (1998), 'Data Protection Act 1998'.
http://www.legislation.gov.uk/ukpga/1998/29/contents

Government of the United States of America (1996), 'The Health Insurance Portability and Accountability Act of 1996 (HIPAA) '.
http://www.gpo.gov/fdsys/pkg/PLAW-104publ191/html/PLAW-104publ191.htm

Greenhalgh, T., Stramer, K., Bratan, T., Byrne, E., Russell, J., Hinder, S. & Potts, H. (2010), The Devils in the Detail: Final Report of the Independent Evaluation of the Summary Care Record and Healthspace Programmes., Report.

Health and Social Care Information Centre (2009), 'RBAC Knowledge Structure Map (unpublished)'.

Health and Social Care Information Centre (2011), 'Overview of SCR Application RBAC Activities '.
http://systems.hscic.gov.uk/scr/documents/rbacactivities.pdf/view

Health and Social Care Information Centre (2012), 'Information Governance Requirements for IT Systems that Hold Personal Data 2012-13 (unpublished)'.

Health and Social Care Information Centre (2013), 'A guide to confidentiality in health and socila care: references'.
http://www.hscic.gov.uk/confguideorg

Health and Social Care Information Centre (2014*a*), 'Additional information and the SCR'.
http://systems.hscic.gov.uk/scr/staff/impguidpm/createscrs/additional

Health and Social Care Information Centre (2014*b*), 'RA overview'.
http://systems.hscic.gov.uk/rasmartcards/planning/raoverview/index_html

Health and Social Care Information Centre (2014*c*), 'Spine'.
http://systems.hscic.gov.uk/spine

Health Canada (2014), 'Canada's Health Care System (Medicare)'.
http://www.hc-sc.gc.ca/hcs-sss/medi-assur/index-eng.php

Health Level Seven International (2007), 'HL7 Role-Based Access Control (RBAC) Role Engineering Process, Version 1.3'.

Health Level Seven International (2008), 'HL7 Role Based Access Control (RBAC) Contraint Catalog'.

Health Level Seven International (2010), 'HL7 Version 3 Standard: Role-Based Access Control Healthcare Permission Catalog (RBAC), Release 2'.

Health Service Executive (2012), National Integrated Services Framework for the EHR.

Health Service Executive (n.d.), 'Data Protection And Freedom Of Information Legislation'.

HIQA (2009), Recommendations for a Unique Health Identifier for Individuals in Ireland, Report, Health Information and Quality Authority.
www.hiqa.ie

HIQA (2010), Guidance on privacy impact assessment in health and social care, Report, Health Information and Quality Authority.
`www.hiqa.ie`

HIQA (2011), Recommendations for Unique Health Identifiers for Healthcare Practitioners and Organisations, Report, Health Information and Quality Authority.
`www.hiqa.ie`

Hoerbst, A., Kohl, C. D., Knaup, P. & Ammenwerth, E. (2010), 'Attitudes and behaviors related to the introduction of electronic health records among Austrian and German citizens', *International journal of medical informatics* **79**(2), 81–89.

International Standards Organisation (2006), 'ISO PDTS 21298 Health informatics: Functional and structural roles'.

International Standards Organisation (2011), 'ISO 18308:2011, Health informatics - Requirements for an electronic health record architecture'.

International Standards Organisation (2012*a*), 'ISO/DIS 22600-1, Health informatics - Privilege management and access control'.

International Standards Organisation (2012*b*), 'ISO/DIS 22600-2, Health informatics: Privilege management and access control'.

International Standards Organisation (2012*c*), 'ISO/DIS 22600-3, Health informatics - Privilege management and access control'.

Irish College of General Practitioners, GPIT Data Protection Working Group (2011), 'A Guide to Data Protection Legislation for Irish General Practice'.

Kaplan, B. & Maxwell, J. A. (2005), *Qualitative research methods for evaluating computer information systems*, Springer, pp. 30–55.

Kluge, E. H. (2004), 'Informed consent and the security of the electronic health record (EHR): some policy considerations', *International Journal of Medical Informatics* **73**(3), 229–34.
http://www.ncbi.nlm.nih.gov/pubmed/15066551

Kodner, D. L. & Spreeuwenberg, C. (2002), 'Integrated care: meaning, logic, applications, and implicationsa discussion paper', *International journal of integrated care* **2**.

Kvale, S. (1996), *InterViews: An Introduction to Qualitative Research Interviewing* , SAGE, London.

Ministry of Health Welfare and Sport (2006), ICT in Dutch Health Care - An international Perspective, Report, Ministry of Health Welfare and Sport.
http://www.epractice.eu/files

Mohan, A. & Blough, D. M. (2010), An attribute-based authorization policy framework with dynamic conflict resolution, *in* 'Proceedings of the 9th Symposium on Identity and Trust on the Internet', ACM, pp. 37–50.

Motta, G. H. & Furuie, S. S. (2003), 'A contextual role-based access control authorization model for electronic patient record', *Information Technology in Biomedicine, IEEE Transactions on* **7**(3), 202–207.

Myers, M. D. & Avison, D. (2002), *Qualitative research in information systems: a reader*, Sage.

Neame, R. (2000), 'Communications and EHR: authenticating who's who is vital', *International Journal of Medical Informatics* **60**(2), 185–190.
http://www.sciencedirect.com/science/article/pii/S1386505600001192

Netherlands Interviewees (2014), 'Interview with two Experts from the Netherlands'.

Neumann, G. & Strembeck, M. (2002), A scenario-driven role engineering process for functional RBAC roles, *in* 'Proceedings of the seventh ACM symposium on Access control models and technologies', ACM, pp. 33–42.

New Brunswick Health Council (2010), Our Help. Our Perspective. Our Solutions.: Results of Our First Engagement Initiative with New Brunswick Citizens, Report.
`http://www.nbhc.ca/sites/default/files`

New Brunswick Interviewee (2014), 'Interview with a New Brunswick Expert'.

NHS (2011), 'The Care Record Guarantee'.
`http://systems.hscic.gov.uk/rasmartcards/strategy/nhscrg`

NHS (2014), 'About the National Health Service (NHS) in England - NHS Choices'.
`http://www.nhs.uk/NHSEngland/thenhs/about/Pages/overview.aspx`

NHS - Connecting for Health (2013*a*), 'Legitimate Relationships'.
`http://www.connectingforhealth.nhs.uk/systemsandservices/scr/staff/impguidpm/ig/legitrelate`

NHS - Connecting for Health (2013*b*), 'Other Controls'.
`http://www.connectingforhealth.nhs.uk/systemsandservices/scr/staff/impguidpm/ig/controls`

Nictiz (2009), eHealth in the Netherlands: Policies, developments and status of cross-enterprise information exchange in Dutch healthcare, Report.
`https://community.oecd.org/docs/DOC-34560`

Nictiz (2014), 'About Nictiz - National IT Institute for Healthcare in the Netherlands'.
`http://www.nictiz.nl/page/Over-Nictiz/About-Nictiz`

Peleg, M., Beimel, D., Dori, D. & Denekamp, Y. (2008), 'Situation-Based Access Control: Privacy management via modeling of patient data access scenarios', *Journal of Biomedical Informatics* **41**, 1028–1040.

Pope, C. & Edwards, E. (2013), 'Over 1.5 million affected by ennis data breach'.
http://www.irishtimes.com/news/consumer/over-1-5-million-affected-by-ennis-data-breach-1.1592128

Ruotsalainen, P. (2004), 'A cross-platform model for secure Electronic Health Record communication', *International Journal of Medical Informatics* **73**(3), 291–5.
http://www.ncbi.nlm.nih.gov/pubmed/15066561

Sandhu, R. S. & Samarati, P. (1994), 'Access control: principle and practice', *Communications Magazine, IEEE* **32**(9), 40–48. IEEE.

Scarfo, P. (2013), 'Achieving assured authentication in the digital age', *Biometric Technology Today* **2013**(9), 9–11.

Scott, R. E., Jennett, P. & Yeo, M. (2004), 'Access and authorisation in a glocal e-health policy context', *International Journal of Medical Informatics* **73**(3), 259–66.
http://www.ncbi.nlm.nih.gov/pubmed/15066556

Smith, E. & Eloff, J. H. P. (1999), 'Security in health-care information systems: current trends', *International Journal of Medical Informatics* **54**(1), 39–54. Elsevier.

The Caldicott Committee (1997), Report on the Review of Patient-Identifiable Information, Report.
http://webarchive.nationalarchives.gov.uk/+/www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationspolicyandGuidance/DH_4068403

The European Parliament (1995), 'Directive 95/46/EC of the European Parliament'.

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

The Medical Council, Ireland (2004), 'A Guide to Ethical Conduct and Behaviour'.

UK Interviewee (2014), 'Interview with Expert from the United Kingdom'.

UK Office of the e-Envoy (2002), Registration and Authentication: e-Government Strategy Framework Policy and Guidelines, Report.
http://systems.hscic.gov.uk/rasmartcards/documents/raegif.pdf

van der Linden, H., Kalra, D., Hasman, A. & Talmon, J. (2009), 'Inter-organizational future proof EHR systems. A review of the security and privacy related issues', *International Journal of Medical Informatics* **78**(3), 141–60.
http://www.ncbi.nlm.nih.gov/pubmed/18760661

van't Noordende, G. (2010), Security in the Dutch electronic patient record system, *in* 'Proceedings of the second annual workshop on Security and privacy in medical and home-care systems', ACM, pp. 21–32.

Yin, R. K. (2009), *Case study research: Design and methods*, Vol. 5, Sage.

Appendix A

Case Study Protocol

A.1 Information Document for Participants

Introduction

Lead Researcher: Sean Lennon
Trinity College Dublin
Student Identification Number: 12319992

This research project is being completed in partial fulfilment of an MSc Degree in Health Informatics at Trinity College Dublin. This information document for participants introduces the nature of the project and provides a procedural outline for participation.

Background

The establishment of the Integrated Services Framework (ISF) represents a landmark in the advancement of connected health in Ireland. This challenging programme of work sets out to establish a standards based reference framework for the interoperability of health information systems. Thus providing, for example, the key building blocks to a national Electronic Health Record (EHR).

The programme is being delivered through twelve work-streams:

WS1: EHR Overview and Approach
WS2: Technical Infrastructure Work-stream
WS3: Software Applications Reference Base
WS4: Integrated Systems Management Framework
WS5: High Level Business Process Specification
WS6: Information Architecture Model
WS7: Data and Information Repository Work-stream
WS8: Transformation, Interfacing and Sourcing
WS9: Identity, Access and Consent Management
WS10: EHR Portal and Presentation
WS11: Architecture Documentation
WS12: Governance Model

Ultimately, the consolidation of these work-streams will establish both a technical and strategic foundation, defining the shape of interoperable health care in Ireland into the future.

One of the above work-streams entitled *"WS9: Identity, Access and Consent Management"* (IACM) is concerned with strategy and management of these security related issues in the connected health environment.

The purpose of this research is to contribute to the ISF IACM work-stream. This research project seeks to understand the state-of-the-art in relation to IACM and hopes to gain insight into these important topics through an understanding of the experiences of other countries such as yours. This will be conducted through a series of case studies focusing on the issues and outcomes associated with areas such as national policy, deployment approaches, and implementation.

Countries have been chosen as a subject of study based on a) their current state of advancement in these areas, and b) on consideration of the most likely combination of cases to produce a valid and useful outcome. Participation is requested in the form of semi-structured interviews with key

personnel in each country having appropriate knowledge and experience in these areas.

Ultimately, it is hoped that an evaluation and analysis of these case studies will provide valuable input into the above mentioned Integrated Services Framework.

Procedures

The following subsections describe the procedures concerning your participation.

The interview

- You are requested to participate in a semi-structured interview with duration of approximately 45 minutes.
- It is expected that the interview will be conducted by telephone.
- As an interested observer, a representative of the Integrated Services Framework (ISF) may wish to be present during the interview. This however, is not a requirement, and you may request a one-to-one interview if that is your preference.
- Questions will be provided to you in advance of the interview to allow for clarifications as necessary.
- You will be contacted in advance of the interview to arrange a suitable date and time.
- Informed consent to participate will be required in advance of the interview and an informed consent document is provided for this purpose.
- Participation in the interview is on a voluntary basis. You retain the right to withdraw and to omit individual responses without penalty.
- In the extremely unlikely event that illicit activity is reported to me in during the study, I will be obliged to report it to the appropriate authorities.
- There are no anticipated risks to you, the interviewee.

Interview Recording

- It is the intention that interviews will be audio-recorded. However, you may decline to be recorded, and in this instance, notes of the interview will be taken instead.
- You may request recording to be stopped at any time during the interview, and you may also request the destruction of the recording at any time after the interview.
- No audio recordings will be made available to anyone other than the researcher, nor will any such recordings be replayed in any public forum or presentation of the research.
- All audio recordings will be deleted upon transcription.
- Recordings and transcriptions will not be identifiable without your prior written permission. Your permission will also be sought for specific reuse (in papers, talks, etc.).

Post Interview and Analysis

- I may wish to contact you again after the interview to verify understanding and/or seek clarifications, however, any such followup will be kept to a minimum.
- Preservation of your anonymity will be ensured in analysis, publication and presentation of resulting data and findings.
- You will be afforded the opportunity to verify the accuracy of direct quotations and their contextual appropriateness in advance of any publication and presentation of resulting data and findings.
- Finally, you will be provided with a copy of the completed research report.

A.2 Interview Questions

Questions relate to national or region EHR implementations involving the consolidation of data.

The questions below follow three main themes: authorisation, consent management and identities. Each theme contains a number of general questions intended to provide a broad direction to the interview.

Authorisation: Please describe how authorisation to access data and functionality is managed.

1. Is access governed by a Role Based Access Control (RBAC) model? If not, what model(s) are in use?
2. How were roles defined? What process led to the definition of roles?
3. What process led to the definition of permissions?
4. How are permissions assigned to a role?
5. How are roles managed and assigned to users? What are the significant issues, if any?
6. Aside from RBAC, is access further constrained in any way; for example in compliance with the 'need to know' principle? How is this managed and what are the significant issues, if any?

Consent Management: Please describe how privacy legislation might impact on authorisations to access health information.

7. Does privacy legislation require patient consent concerning the collection and viewing of health information?
8. If explicit consent is required at any time, how is consent information collected, stored and subsequently managed?
9. Is there a mechanism whereby consent directives can be overridden?

10. Are different sensitivity levels applied to categories of health information; for example demographic information versus clinical information?

Identities: Please describe how patient and practitioner identification is managed.

11. In what way are patients uniquely identified across EHR data?

12. In what way are EHR users uniquely authenticated?

Do you have any documentation to support the issues discussed here, and would it be possible to have a copy of these?

A.3 Informed Consent Form

Lead Researcher

Sean Lennon
Trinity College Dublin
Student Identification Number: 12319992

Background

The Integrated Services Framework (ISF) in Ireland represents a body of work that sets out to establish a reference framework for the interoperability of healthcare information systems in Ireland. Taking a standards based approach, the framework is being delivered through a structured programme of work, segmented into twelve work-streams. One such work-stream entitled *"Identity, Access and Consent Management"* (IACM) is concerned with strategy and management of these security related issues in an interoperable healthcare environment.

The purpose of this research is to contribute to the ISF IACM work-stream. This research project seeks to understand the state-of-the-art in relation to IACM and hopes to gain insight into these important topics through an understanding of the experiences of other nations. This will be conducted through a series of case studies focusing on the issues and outcomes associated with areas such as national policy, deployment approaches, and implementation. Countries have been chosen as a subject of study based a) their current state of advancement in these areas, and b) on consideration of the most likely combination of cases to produce a valid and useful outcome. Participation is requested in the form of semi-structured interviews with key personnel in each country having appropriate knowledge and experience in these areas.

Ultimately, it is hoped that an evaluation and analysis of these case studies will provide valuable input into the Integrated Services Framework in

Ireland.

Procedures of this study

You are requested to participate in a semi-structured interview with duration of approximately 45 minutes. Participation in the interview is on a voluntary basis, and you retain the right to withdraw and to omit individual responses without penalty. An interested observer from the Integrated Services Framework (ISF) programme may be present during the interview, however this is at your discretion, and you may request a one-to-one interview if that is your preference. There are no anticipated risks to you, the interviewee arising from this interview.

It is the intention that interviews will be audio-recorded. However, you may decline to be recorded, and in this instance, notes of the interview will be taken instead. Additionally, you may request recording to be stopped at any time during the interview, and you may also request the destruction of the recording at any time after the interview.

Preservation of your anonymity will be ensured in analysis, publication and presentation of resulting data and findings. Recordings and transcriptions will not be identifiable unless you have provided prior written permission. Permission will be sought for specific reuse (in papers, talks, etc.). No audio recordings will be made available to anyone other than the researchers/research team, nor will any such recordings be replayed in any public forum or presentation of the research. All audio recordings will be deleted upon transcription.

Publication

The report will be submitted as a masters dissertation in partial fulfilment of an MSc. Degree in Health Informatics at Trinity College Dublin.

Declarations

- I am 18 years or older and am competent to provide consent.
- I have read, or had read to me, a document providing information about this research and this consent form. I have had the opportunity to ask questions and all my questions have been answered to my satisfaction and understand the description of the research that is being provided to me.
- I agree that my data is used for scientific purposes and I have no objection that my data is published in scientific publications in a way that does not reveal my identity.
- I understand that if I make illicit activities known, these will be reported to appropriate authorities.
- I understand that I may stop electronic recordings at any time, and that I may at any time, even subsequent to my participation have such recordings destroyed (except in situations such as above).
- I understand that, subject to the constraints above, no recordings will be replayed in any public forum or made available to any audience other than the current researchers/research team.
- I freely and voluntarily agree to be part of this research study, though without prejudice to my legal and ethical rights.
- I understand that I may refuse to answer any question and that I may withdraw at any time without penalty.
- I understand that my participation is fully anonymous and that no personal details about me will be recorded.
- I have received a copy of this agreement.

PARTICIPANTS NAME:

PARTICIPANTS SIGNATURE:

DATE:

Statement of investigators responsibility: I have explained the nature and purpose of this research study, the procedures to be undertaken and any risks that may be involved. I have offered to answer any questions and fully answered such questions. I believe that the participant understands my explanation and has freely given informed consent.

RESEARCHERS CONTACT DETAILS:

INVESTIGATORS SIGNATURE:

DATE:

Appendix B

Interview Guide

Interview Guide

Interviewer:	Sean Lennon
Interviewee Name:	
Representing:	
Position and Responsibility:	
Date:	
Interview Location:	
Pre-interview Notes:	

Authorisation: Please describe how authorisation to access data and functionality is managed.

- Is access governed by a Role Based Access Control (RBAC) model? If not, what model(s) are in use?
- How were roles defined? What process led to the definition of roles?
- What process led to the definition of permissions?
- How are permissions assigned to a role?
- How are roles managed and assigned to users? What are the significant issues, if any?
- Aside from RBAC, is access further constrained in any way; for example in compliance with the 'need to know' principle? How is this managed and what are the significant issues, if any?

Consent Management: Please describe how privacy legislation might impact on authorisations to access health information.

- Does privacy legislation require patient consent concerning the collection and viewing of health information?
- If explicit consent is required at any time, how is consent information collected, stored and subsequently managed?
- Is there a mechanism whereby consent directives can be overridden?
- Are different sensitivity levels applied to categories of health information; for example demographic information versus clinical information?

Identities: Please describe how patient and practitioner identification is managed.

- In what way are patients uniquely identified across EHR data?
- In what way are EHR users uniquely authenticated?

Do you have any documentation to support the issues discussed here, and would it be possible to have a copy of these?

Appendix C

UK Rationalised Roles

R8000: Clinical Practitioner Access Role
R8001: Nurse Access Role
R8002: Nurse Manager Access Role
R8003: Health Professional Access Role
R8004: Healthcare Student Access Role
R8005: Biomedical Scientist Access Role
R8006: Medical Secretary Role
R8007: Clinical Coder Access Role
R8008: Admin/Clinical Support Access Role
R8009: Receptionist Access Role
R8010: Clerical Access Role
R8011: Clerical Manager Access Role
R8012: Information Officer Access Role
R8013: Health Records Manager Access Role
R8014: Social Worker Access Role
R8015: Systems Support Access Role
R8016: Midwife Access Role
R8017: Midwife Manager Access Role
R5110: Demographic Administrator
R8024: Bank Access Role
R0001: Privacy Officer
R5105: Caldicott Guardian
R5090: Registration Authority Agent
R5072: Root Registration Authority Manager
R5080: Registration Authority Manager

Table C.1: UK rationalised roles: based on (RBAC Database V25.1)

Appendix D

New Brunswick: EHR Access Request

EHR ACCESS REQUEST

Department of Health
Electronic Health Record (EHR)
Tab to go from one field to another or click on the grey box beside each item /

1. User Information – to be completed by the requester /

a. Full Name	
b. Current Job Title	
c. Work Location (site name, zone #)	
d. Employee Number (not required for physicians)	
e. Business Telephone Number	
f. Business Address	
g. Business E-mail Address	
h. Preferred E-mail Address	

i. Role (select one only)

PHYSICIANS AND NURSES

- ☐ General Practitioner (GROUP 1)
- ☐ Medical specialist (Specify the specialty)
  - Laboratory specialty (GROUP 17)
  - Other specialty (GROUP 5)
- ☐ Licensed Practical Nurse (GROUP 7)
- ☐ Nurse Practitioner (GROUP 21)
- ☐ ER Nurse (GROUP 3)
- ☐ Registered Nurse (GROUP 7)
  - Specify the service:
- ☐ Other / Specify :

DOH AND FACILICORPNB STAFF

- ☐ Cancer Registry staff (GROUP 10)
- ☐ EHR Business Team (GROUP 4)
- ☐ EHR Application Support Team (GROUP 6)
- ☐ OPOR Registry Unit (GROUP 12)
- ☐ FacilicorpNB Information Technology staff
  - ☐ Integration team (GROUP 99 or 15)
  - ☐ Application team (GROUP 99 or 15)
- ☐ Other / Specify :

OTHER PROFESSIONS: (in alphabetical order)

- ☐ Audiologist (GROUP 7)
- ☐ Chemo Room Clerk (GROUP 25)
- ☐ Coder - Trauma (GROUP 7)
- ☐ Diagnostic Imaging Technologist involved in EHR DQ activities (GROUP 11)
- ☐ Dietitian (GROUP 7)
- ☐ Health Information Management Professional involved in EHR DQ activities (GROUP 13)
- ☐ Laboratory technologist involved in EHR DQ activities (GROUP 9)
- ☐ Laboratory technologist not involved in EHR DQ activities (GROUP 23)
- ☐ Occupational Therapist (GROUP 7)
- ☐ Pharmacist (GROUP 7 or 17)
  - Do you work in a specialized sector such as oncology, nephrology or neurology?
  - Other, specify:
- ☐ Physiotherapist (GROUP 7)
- ☐ Psychologist (GROUP 17)
- ☐ Radiation Therapist (GROUP 25)
- ☐ Respiratory Therapist (GROUP 7)
- ☐ Social Worker (GROUP 29)
- ☐ Speech Language Pathologist (GROUP 7)
- ☐ Trauma Registry Manager (GROUP 29)
- ☐ Other / Specify :

j. ***Username or User-ID (Active Directory username):***

Your username is the ID that you use to log on to the network at the beginning of your work day. If you are unsure what your username is, contact your local service desk for assistance.

2. User Acknowledgment. To be completed, signed and dated by the requester and his/her supervisor.

I		**agree that:**
	User Full Name (PRINT)	

1. I understand that the personal health information (PHI) stored in the EHR is confidential and must only be used for providing or assisting in the provision of health care.
2. I must take reasonable steps to protect my EHR access information from unauthorized use.
3. I will not share my username, password or other EHR access information with anyone and I will use a complex password.
4. I am responsible for any unauthorized disclosure of personal information regarding clients/patients through the inappropriate use of my authorized access.
5. I will ensure that patient information is not made available to unauthorized individuals by way of printing, display, etc.
6. I understand that I will get a read-only access and printing is restricted to authorized users only.
7. I will not download personal health information to the hard drive on my work or personal computer(s) or any portable storage devices.
8. I will immediately notify the EHR Administrator by e-mail if my account has been, or may have been, compromised in any way. E-mail address: EHRadministrator@gnb.ca
9. I will notify the EHR Administrator by email within 5 working days when it has been determined that access to the EHR is no longer required. EHRadministrator@gnb.ca
10. The Department of Health may revoke my access if I fail to comply with my obligations outlined in this form.
11. I understand that usage of the EHR will be monitored.
12. I understand that I will not be granted access to the EHR before I complete the e-learning EHR privacy training.

By signing below, I acknowledge that I have reviewed, understand, and agree to the above. I also understand that the Department of Health may revoke my access if I fail to comply with my obligations.

Signature of requester/user	
Date	
Language of choice for training?	☐ ENGLISH ☐ FRENCH

SUPERVISOR AUTHORIZATION

I authorize the above named individual to have access to the EHR and declare that the individual has been authenticated to be the individual identified in section 1 of this form.
I verified the following:

a. All the needed information is complete and accurate;
b. The role selected is the individual's role within our organization;
c. The certificate confirming the completion of the e-learning EHR privacy training is included with this request;

and I will notify the EHR Administrator by e-mail within 5 working days when it has been determined that this user no longer requires access to the EHR. EHRadministrator@gnb.ca

Supervisor full name and title (PRINT)	
Supervisor phone number and email address	
Signature of supervisor	
Date	

If you have any questions, send an email to the EHR administrator at: EHRadministrator@gnb.ca

Appendix E

Summary of Results

Dimension	**England**	**The Netherlands**	**New Brunswick**
Population	53 million.	16 million.	Canada 35 million, New Brunswick 0.8 million.
Centralised eHealth Body	Yes - Health and Social Care Information Centre (HSCIC).	Yes - National Institute for Healthcare in the Netherlands (Nictiz).	Yes - Canada Health Infoway.
National Infrastructure	The Spine - a central infrastructure supporting national services such as the Summary Care Record, Patient Demographic Service, Legitimate Relationship Service, Authentication and Authorisation Services and others.	AORTA - a central national infrastructure supporting the Electronic Health Record (EPD), and includes authentication, authorisation and audit services.	EHR Infostructures implemented at provincial-territorial level, and based on Canada Health Infoway's EHR architectural blueprint.
EHR architecture	Information hosted centrally.	Federated with Central Switch Point (LSP).	Hosted centrally.

Dimension	**England**	**The Netherlands**	**New Brunswick**
Significant Legislation	Subject to the EU Directive 95/46/EC, Common Law on Confidentiality, Data Protection Act 1998. No specific health information legislation dealing with data protection.	Subject to the EU Directive 95/46/EC, Personal Data Protection Act, Medical Treatment Contracts Act. No specific health information legislation dealing with data protection.	Legislation is enacted at jurisdictional level - specific health information deals with patient consent and privacy requirements. Requires definition of a health information network describing information usage.
Consent Debate	Societal concerns. Uncertainty and disagreement on when and where consent is, and should be mandated. Uncertainty has and continues to affect EHR programme.	Societal concerns.. Uncertainty and disagreement on when and where consent is, and should be mandated. Continuing debate has and continues to affect EHR programme.	Public consultation reveals New Brunswickers attitude towards consent: "ensure that privacy rules don't interfere with the ability to deliver timely service to patients". Legislation enacted based on 'no consent'.
Consent to Publish	Consent required for permission to publish health information to the Spine.	Explicit consent is required to publish health information on the Central Switch Point (LSP).	No consent is required.

Dimension	**England**	**The Netherlands**	**New Brunswick**
Permission to View	Explicit consent is always required to view patient information.	No consent is required when a technically enforced patient relationship is established with the patient. Proposed legislation calls for explicit consent to view at all times.	No explicit consent is required to view health information.
EHR Opt-out	Opt-out allowed.	Opt-out allowed (opt-in model).	No opt-out.
Consent Directives	Additional controls permitting the patient to specify consent directives. Implementation challenges - now aspirational, and not mandatory.	Proposed legislation calls for consent directives.	Implemented at the clinical record only and based on all or nothing.
User Registration	Sponsored users are registered and assigned to roles via local Registration Authorities (RA). Identities are rigorously checked before acceptance.	Users must be registered on the Professionals in Healthcare (BIG) registry and also to the Unique Healthcare Provider Identification (UZI) register.	Centralised registration. Users must be sponsored, and must undergo mandatory privacy training. Identities are rigorously checked before acceptance.

Dimension	**England**	**The Netherlands**	**New Brunswick**
Authentication	Two-factor authentication via smartcard.	Two-factor authentication via UZI smartcard card.	Active Directory Username and complex password credentials.
RBAC - Roles	Initially based on the National Workforce Dataset, roles became unwieldy. RBAC model was subsequently rationalised and designed for purpose.	Roles based on BIG register. Not for purpose and issues emerging concerning role granularity.	Roles created for purpose and as required. Some challenges with specialisation and granularity.
Role Engineering	Multi-disciplinary committee.	Multi-disciplinary committee.	Multi-disciplinary committee.
RBAC model	Innovative Position Based Access Control (PBAC). A role, permission and domain hierarchical model which provides for specialisation and localisation.	Standard RBAC.	Standard RBAC.
RBAC Constraints	Legitimate Relationships (LR) to patient required.	Treatment relationship to patient required, enforced through technology (not yet achieved).	No treatment relationship concept.

Dimension	England	The Netherlands	New Brunswick
Classification of data	All clinical data is classified as sensitive.	All healthcare data is classified as sensitive.	All healthcare data is classified as sensitive.
Other Controls	Other Controls include the Workplace contract, NHS code of practice and legal obligations, NHS Care record guarantee, Professional codes of conduct.	Professional code of conduct.	Mandatory privacy training during registration.
Audit	Monitoring and logging all actions on patient information, includes alert functionality.	Monitoring and logging all actions on patient information.	Monitoring and logging all actions on patient information.

Table E.1: Summary of results

Appendix F

Table of Recommendations

Table of Recommendations

Recommendation 1:

In advance of Ireland's implementation of a national Electronic Health Record, following further public consultations as required, the proposed Health Information Bill should clearly set out Ireland's position on patient consent as it relates to the processing of personal health information in the context of a national Electronic Healthcare Record. The bill should clearly define consent requirement as they relate to:

1. Consent to publish: A potential requirement for consent with respect to a person's health information being included in a national EHR.
2. Permission to view: A potential requirement for consent with respect to a person allowing others to access their record.
3. Consent directives: The extent to which a person may provide instruction to hide or control access to specific aspects of their record.

Recommendation 2:

An overarching National Consent Management Policy is required, underpinned by and in accordance with the Health Information Bill. This National Policy and Code of Conduct should clearly describe:

1. Privacy and consent requirements
2. Agreed operational and procedural controls, and
3. The extent to which technology and organisational controls may combine to enforce this policy.

Recommendation 3:

A clear communication strategy is required to ensure that citizens have a clear and unambiguous understanding of their rights and how these rights are protected. A Privacy Impact Assessment, as recommended by HIQA, may form one aspect of that communication process.

Recommendation 4:
Healthcare workers must have a full understanding of the National Consent Management Policy set out in Recommendation 2. Mandatory training should form part of the EHR user registration process.

Recommendation 5:
A centralised user registration service for access to EHR services should be established, and the imminent National Register of Health Service Providers (HSP) should provide unique identities to this registration service.

Recommendation 6:
Authentication to an access control infrastructure should be based on two factors, in full accordance with ISO27799(2008) Health Informatics - Information security management in healthcare using ISO/IEC27002.

Recommendation 7:
Roles should be designed for purpose, and defined as required in accordance with the HL7-supported, scenario modelling role engineering process.

Recommendation 8:
A multi-disciplinary RBAC committee should be established to oversee the role engineering process, and to consider amendments and additions as they arise throughout the lifetime of the project.

Recommendation 9:

Authorisation control should be founded on a RBAC model. This model should be chosen with sufficient flexibility to allow role specialisation, avoid role spread and redundancy, and grow with Ireland's EHR implementation. As such, a Hierarchical-RBAC model is recommended, in accordance with the HL7-supported, scenario modelling role engineering process.

Recommendation 10:
Technical enforcement of a treatment relationship between the healthcare worker and the patient should not form part of the access control decision, but should instead be subject to organisational control and audit.

Recommendation 11:
Define an overarching National Policy on Access Control, encompassing both technical and organisational controls. This policy should be communicated as with Recommendations 3 and 4.

Recommendation 12:
Implement a robust audit system which monitors at least:

- All activities on patient information
- Consent directive overrides
- Changes to user registration/role attributes.

Monitoring should be enhanced through the use of alert notifications, intelligent analysis solutions, and exceptions and alerts should be notified to an appointed information governance Privacy Officer.

Table F.1: Table of recommendations