University of Newcastle upon Tyne

Faculty of Science, Agriculture and Engineering

School of Computing Science

Security Management for Services that are integrated across Enterprise Boundaries

PhD Thesis

By

Salem Sultan Aljareh

A thesis submitted in partial fulfilment
of the requirements for the degree of

Doctor of Philosophy

June 2004

ABSTRACT

This thesis addresses the problem of security management for services that are integrated across enterprise boundaries, as typically found in multi-agency environments. We consider the multi-agency environment as a collaboration network. The Electronic Health Record is a good example of an application in the multi-agency service environment, as there are different authorities claiming rights to access the personal and medical data of a patient. In this thesis we use the Electronic Health Record as the main context.

Policies are determined by security goals, goals in turn are determined by regulations and laws. In general goals can be subtle and difficult to formalise, especially across admin boundaries as with the Electronic Health Record. Security problems may result when designers attempt to apply general principles to cases that have subtleties in the full detail. It is vital to understand such subtleties if a robust solution is to be achieved

Existing solutions are limited in that they tend only to deal with pre-determined goals and fail to address situations in which the goals need to be negotiated. The task-based approach seems well suited to addressing this.

This work is structured in five parts. In the first part we review current declarations, legislation and regulations to bring together a global, European and national perspective for security in health services and we identify requirements. In the second part we investigate a proposed solution for security in the Health Service by examining the BMA (British Medical Association) model. The third part is a development of a novel task-based CTCP/CTRP model based on two linked protocols. The Collaboration Task

Creation Protocol (CTCP) establishes a framework for handling a request for information and the Collaboration Task Runtime Protocol (CTRP) runs the request under the supervision of CTCP. In the fourth part we validate the model against the Data Protection Act and the Caldicott Principles and review for technical completeness and satisfaction of software engineering principles. Finally in the fifth part we apply the model to two case studies in the multi-agency environment: a simple one (Dynamic Coalition) for illustration purposes and a more complex one (Electronic Health Record) for evaluating the model's coverage, neutrality and focus, and exception handling.

THESIS SUMMARY

It is evident that the privacy of people, the confidentiality of their information, the integrity of transactions handling, and the availability of service systems are all essential and the consequence of any breaches to any one of these aspects will be costly and could lead to disaster. Therefore security in computer services has been considered as a core subject in many new developments.

Information about an individual is absolutely secure, as long as nobody else has access to it, which is true only in the case where an individual is completely stand-alone. Information is naturally sharable among groups such as team, committee, organization, country and federation in a manner based on trust. However to achieve an accepted level of trust is quite a complicated issue because as the collaboration grows wider, more participants are involved with divergent policies and interests.

This thesis tackles the problem of security management for services that are integrated across enterprise boundaries, which are found in multi-agency environments. We consider the multi-agency environment as a collaboration network. The Electronic Health/Patient Health Record is an example for multi-agency service environment, as there are different authorities claiming rights to access the patient personal and medical data.

Existing solutions for security problems in multi-agency services are based on roles or subject-object access control; such approaches appear to lack the ability to address requirements such as need-to-know and data-use-control.

Security systems are not different from other computer systems as they are based on specific requirements and goals. Security system policies are often based on regulations and the law. The principles in the law give the overall policies but more detail is usually necessary when the implementation is being made. In particular circumstances a lawyer would look further. Security system designers make mistakes by attempting to implement general principles for cases that have subtleties in the full detail which it is vital to understand for a robust solution. It is easier to regulate a well-defined case. Security solutions are designed to enforce a security policy, which is based on a specific security goal. Security goals originate from rules and regulations, hence any security solution logically, should be validated with the regulations on the application context.

The task-based approach is a promising approach, as its rationale is suitable for addressing security problems in environments such as the multi-agency services.

While there are a number of task-based security models, a literature review found that none of them explicitly deal with the security requirements of multi-agency services.

Current declarations, legislation and regulations were reviewed to bring together a global, European and national perspective for security in health services and to identify requirements. This review highlighted the debate over security principles, emphasising the need for a framework, which should be pluralistic and flexible to accommodate many different needs.

Further investigation into a proposed solution for security in the Health Service was made by examining the BMA (British Medical Association) model. Three security languages Lasco, PONDER and ASL were used. It was found that the BMA model does not address the requirement of sharing information across boundaries of the Health Service. In particular the principle of need-to-know, which was found in the review to be a critical requirement in a multi-agency environment, was omitted.

To meet the above requirements such as need-to-know by restricting access for a specific purpose, a novel task-based CTCP/CTRP model based on two linked protocols was developed. The Collaboration Task Creation Protocol (CTCP) established a framework for handling a request for information and the Collaboration Task Runtime Protocol (CTRP) ran the request under the supervision of CTCP. The CTCP/CTRP model was represented in the Petri Net notation, validated against the Data Protection Act and the Caldicott Principles and reviewed for technical completeness and satisfaction of software engineering principles such as focus, readability and competence.

The model was applied to two case studies in the multi-agency environment: a simple one (Dynamic Coalition) for illustration purposes and a more complex one (Electronic Health Record) for evaluating the model's coverage, neutrality and focus. The model satisfied the requirements of the case studies, handling their scenarios and dealing with errors and exceptions as they arose.

To conclude the model developed met the requirements identified from an analysis of the declarations, legislation and regulations. Further work might include the development of infrastructure based on the idea of the CTCP/CTRP model for full-scale testing and development. It would also be beneficial to develop a formalisation of the model but this is not simple because of the open-ended nature of the model giving a variety of task formations.

PUBLICATION

Parts of this thesis have been published as follows:

1. Aljareh, S., Rossiter, N. and Heather, M., A Formal Security Model for Collaboration in Multi-agency Networks. *2nd Workshop on Security in Information Systems (WOSIS 2004)*, (Porto, Portugal, 2004), 157-169.

2. Aljareh, S. Dobson, J. and Rossiter N. Satisfaction of Health Record Security Principles through Collaborative Protocols, In proceedings of the 8th International Congress in Nursing Informatics. Brazil 20-25 June 2003

3. Aljareh S., Rossiter N. Modelling Security in Multi-agency environment. Technical report CS-TR-764, The University of Newcastle upon Tyne, Department of computing science 2002.

4. Aljareh, S. and Rossiter N. Toward security in Multi-agency Clinical Information Services. Health Informatics Journal, issue 8.2, June 2002.

5. Aljareh S. and Rossiter, N. A Task-based Security Model to facilitate Collaboration in Trusted Multi-agency Networks. In proceedings of SAC2002, Symposium on Applied Computing, 10–14 March 2002, Madrid pp744-749.

6. Aljareh, S. and Rossiter N. Toward security in multi-agency clinical information services. In proceedings of Workshop on Dependability in Healthcare Informatics Edinburgh, 22nd-23rd March 2001, 33-41.

7. Aljareh, S. and Rossiter, N. Toward security in multi-agency clinical information services. Technical report CS-TR-729, The University of Newcastle upon Tyne, Department of computing science 2001.

TABLE OF CONTENTS

CHAPTER 1 1

INTRODUCTION 1

1.1. Background and Motivation 1

1.2. Security Models 4

1.3. Access Control 6

1.4. Cross-organisation access control projects 11

1.5. Multi-Agency environment 16

1.6. Our approach 20

1.7. Thesis structure 27

1.8. Conclusion and Contribution summary 29

CHAPTER 2 32

SOURCES OF SECURITY REQUIREMENTS 32

SECURITY REQUIREMENTS FOR MULTI-AGENCY SERVICES IN HEALTH CARE 32

2.1. Introduction 32

2.2. Security Requirements Resources 33

2.3. General data protection 34

2.4. Medical ethics 36

2.5. Debate 44

2.6. Conclusion 49

CHAPTER 3 51

FORMAL ANALYSIS FOR EXISTING SECURITY POLICY MODEL: BMA 51

3.1. Introduction 51

3.2. The Model's Principles 53

3.3. Using security logical languages to represent Anderson's Principles: 56

3.4. A Language for Specifying Security and Management Policies for distributed Systems (Ponder): 68

3.5. Results 74

3.6. Concluding Discussion 77

CHAPTER 4 80

DEVELOPMENT OF TASK-BASED SECURITY MODEL 80

4.1. Introduction 80

4.2. General principles for our Model 83

4.3. Collaboration task characteristics 85

4.4. Diagrammatic Representation of Model 87

4.5. Notations for Protocols 90

4.6. Example of Informal Collaboration 95

4.7. Exception and error handling 100

4.8. Implementation guide lines 107

4.9. Conclusions 112

CHAPTER 5 114

REVIEW OF MODEL AGAINST REQUIREMENTS 114

5.1. Introduction 114

5.2. Security requirements for the health care information systems 115

5.3. Data Protection Act 117

5.4. Caldicott Principles and Recommendations 122

5.5. Coverage of Data Protection Act and Caldicott Principles 125

5.6. Review of Satisfaction of Principles by CTCP/CTRP Model 127

5.7. Conclusion 132

CHAPTER 6 133

CASE STUDY 133

6.1. Introduction 133

6.2. Dynamic Coalition Environment 135

6.3. DCE case study evolution 142

6.4. County Durham and Darlington EHR Project 144

6.5. Conclusion 163

CHAPTER 7 165

DISCUSSION AND CONCLUSION 165

7.1. Thesis summary and discussion 165

7.2. Related works 170

7.3. Limitation and future research 172

7.4. Conclusion 175

REFERENCES 177

APPENDIX A 1

PRINCIPLES OF THE DATA PROTECTION ACT (DPA) 1

Principles verbatim from DPA 1998 1

APPENDIX B 3

CALDICOTT PRINCIPLES AND RECOMMENDATIONS 3

Caldicott Principles 3

Caldicott Recommendations 5

LIST OF FIGURES AND TABLES

Figures

Number *Page*

Figure 1: R (97)'s conditions for controlling the provision of patients' data *40*

Figure 2: R (97)'s conditions for controlling the medical data communication *41*

Figure 3: a security policy graph to represent principle 1 of the clinical security policy. *62*

Figure 4: a security policy graph to represent principle 2 of the clinical security policy. *62*

Figure 5: a security policy graph to represent principle 3 of the clinical security policy. *63*

Figure 6: a security policy graph to represent the first part of principle 4 of the clinical security policy. *64*

Figure 7: a security policy graph to represent the second part of principle 4 of the clinical security policy. *65*

Figure 8: a security policy graph to represent principle 5 of the clinical security policy. *65*

Figure 9: a security policy graph to represent principle 6 of the clinical security policy. *66*

Figure 10: a security policy graph to represent principle 7 of the clinical security policy. *66*

Figure 11: a security policy graph to represent principle 8 of the clinical security policy. *67*

Figure 12: general architecture for secure collaboration environment *88*

Figure 13: Petri Nets Graph representing the Collaboration Task Creation Protocol (CTCP) *89*

Figure 14: Petri Net Notations *91*

Figure 15: Petri Nets Graph representing the Collaboration Task Run-time Protocol (CTRP) *93*

Figure 16: Petri Net representing the CTCP of the given example *98*

Figure 17: Petri Net representing the CTRP of the given Example *100*

Figure 18: Exception handling cycle *106*

Figure 19 Petri net graph shows the exception handling types in the CTRP protocol. ... *158*

Tables

Table 1: Comparison of how far the ASL, LaSCO and Ponder languages can represent Anderson's principles. 76
Table 2 DPA principle 1's conditions against TCP/CTRP components. 119
Table 3 Correspondence of DPA and Caldicott Principles 126
Table 4: Correspondence of DPA Principles and CTCP/CTRP Components 129
Table 5: Abbreviations for protocols components 129
Table 6: Correspondence of Caldicott Principles and CTCP/CTRP Components. 130
Table 7 summary of CTCP protocols inputs for simple coalition scenario (top level task) 138
Table 8: Summary of CTCP protocols inputs for simple coalition scenario (sub task) 140
Table 9: summary of the mapping between the DCE scenario (task one) and the components of the CTCP/CTRP protocols. 142
Table 10: summary of the mapping between the DCE scenario (task two) and the components of the CTCP/CTRP protocols. 143
Table 11: Summary of the Emergency incident Task inputs 152
Table 12: Task 2 (the GP visit) inputs summary 160
Table 13: Illustration of the mapping between the events of the emergency scenario and the components of the CTCP/CTRP. 162
Table 14: Illustration for the mapping between the events of the GP visit and the components of the CTCP/CTRP. 163

DEDICATION

I dedicate this thesis to the memory of the great man my father Sultan Aljareh, who could not wait to see me accomplish his dream. It is dedicated to him and my mother for bringing me up to the level that I accomplished this greatly desired dream of my life.

ACKNOWLEDGMENTS

I consider myself as very fortunate and privileged to benefit from the exceptional experience, insight and maturity in research of three supervisors Professor Peter Ryan, Professor John Dobson and Dr Nick Rossiter. I consider the completion of my thesis in many regards as a result of their advice, guidance, support and encouragement. Dr. Nick Rossiter although he has left Newcastle University, continued to provide me with all I need from support and guidance.

I would like to thank the Arabian Gulf Oil Co. for their funding and sincerely I would like to thank Dr John Lloyd head of School of Computing Science for his financial support and encouragement, he was always there and ready to make what look like difficult issues easy and manageable.

I would like to thank Professor Mike Martin and Dr. Nick Booth from Sowerby Centre for Health Informatics at Newcastle (SCHIN) for their co-operation regarding the case study.

I would like to thank my wife and children for their love, sacrifices and support.

Chapter 1

INTRODUCTION

1.1. Background and Motivation

The goal of security can be generally defined as protection of assets. After defining the assets and their values and being aware of any risk (*risk assessment*), security becomes a matter of preventing assets from being damaged or stolen, detecting in any case of damage who did the damage, when and how [39]. In addition security goals include disaster recovery plan. A breakdown to this definition will lead to more than one focused definition.

A general definition for computer security can be derived from four aspects/properties of security:

Confidentiality (Secrecy and Privacy): there is a longstanding thought of computer security that it is all about confidentiality. Unauthorised users must not be able to access sensitive information. Privacy is about protecting personal information, while secrecy is about protecting information belonging to an organisation [70]. Confidentiality is a well defined security aspect and compared with the other aspects it is very well researched.

Military systems are an example in which the confidentiality is given higher priority over the other security aspects.

Integrity (Accuracy and Authenticity): to prevent unauthorised data modification. In network communication integrity known as *authenticity*, provides a way to verify the origin of sent data and ensure that it has not been altered since it was sent.

In financial systems and databases integrity means accuracy.

Availability: to ensure that the system continues efficiently providing the expected service to its users. Availability also includes the idea that the system should be able to recover quickly in case of disaster.

The above are the main security aspects/properties where we try to prevent any unwelcome events. However we need to examine these properties and in case of any security violation we need to know where we have gone wrong in order to correct any security flaw. That is where *accountability* (another security property) can help.

Accountability: to ensure a user action can be traced uniquely to that specific user. However accountability is not an objective in its right. Indeed it is a sort of policy/mechanism that exists as a help to ensure the other aspects are covered. Correspondingly authenticity is generally considered to be the complement of confidentiality.

In addition there is an overlap in terminology. Depending on a preferred point of view security is an aspect of reliability. IFIP WG 10.4 introduced

dependability to group aspects such as security, reliability, integrity and availability [39].

Security systems like any other systems are based on specific requirements, which differ from one application to another. In fact a security system is a subsystem in integrated system/systems, in which the security subsystem acts as an integrated part to help other system's functions to meet their requirements without any harm/abuse to all the entities involved. System entities include people, their properties (including their personal data), hardware, software and any external entity that could interfere with the system such as public communities.

1.1.1 Goals, policies, models and mechanisms

We have so far talked only about security goals, which are just the first part of the security picture jigsaw (Goals, policies, models and mechanisms). The general security goal as stated above is to protect system assets by ensuring security properties confidentiality, integrity, availability and accountability (sometimes used as mechanism/policy to ensure one of the other three properties) and/or to protect a system from predicted *threats* or to cover defined *vulnerabilities*. There could be more specific goal(s) depending on requirements. We deploy a security system to ensure a predefined assurance. The second part of the picture is the security policy.

A security policy definition depends on security goals of an application. Security policies originate from rules and regulations that aim to achieve

security goals. Security policies can take different forms (e.g. constraints). In Chapter 2 there is a discussion on a number of rules and regulations related to heath informatics. The third piece of the security picture is the *security models* or *security policy models* which is a more formal phase of the security policies [9]. Section 1.2 covers a number of security models.

The security picture jigsaw is completed by its last piece the *security mechanisms*. Cryptography and its applications is the most used security mechanisms to ensure confidentiality; the other well researched and widely used security mechanism is the access control mechanisms (Section 1.3); auditing is another example. It is a mechanism to implement accountability. For instance, our security goal could be authorisation, our security policy to achieve this goal could be a set of constraints, the Bell-Lapadula model could be the model to use, and then we can use the Mandatory Access Control (MAC) as a mechanism to implement our policy.

1.2. Security Models

Several security models have been developed to cover different requirements. In military systems, security means confidentiality and information classified according to clearance levels (top secret, secret, confidential and unclassified). Security models that target these kinds of applications are called Multilevel Security Models (MLS). An example of these models is the Bell-Lapadula Model (BLP) [15]. BLP was introduced by David Bell and Len LaPadula in 1973 for the U.S. Air Force. It is a state

machine capturing the confidentiality aspect of the access control. It has been considered as a base or a benchmark for most security models and is used to design most of the available operating systems to support access control. However BLP deals only with confidentiality, not with the other computer security aspects such as integrity and does not address the management of access control. It has been also proven that BLP could contain a convert channel. To conclude, the BLP model is suitable for an environment where policies are static.

Subsequent models attempted to fill the gaps left open in BLP. For instance the Harrison-Ruzzon-Ullman Model (HRU) [43] defines an authorisation system to address the problem of changing access rights, which was not addressed in BLP. In business organisations, security requirements are different as the threat and vulnerabilities different from those in military. Business is based on competition where threats occur such as conflict of interest. In contrast to BLP, where access rights are usually assumed to be static, in the Chinese Wall Model [17] the access rights have to be re-examined at every state transition, to avoid conflict of interest. The Biba Model [16] is another example of MLS but it deals with the integrity aspect, not with confidentiality. In fact Biba policy is the opposite of BLP policy. The Clark-Wilson Model [24] considers security requirements for commercial applications. It has two mechanisms to enforce integrity: the well-formed transaction; and the separation of duties. The Information-Flow Model deals [57] with the problem of convert channels that has not been addressed by BLP and considers a system as a secure system if there is

no illegal information flows. It should be noted that the above models are not similar structurally. More challenging security requirements are found in the sharing of information and services across security boundaries where in contrast to the MLS models the information follows horizontally (Multilateral Security Policies) [9] rather than vertically. An application example of this kind of security requirements is found in health care information systems (Electronic Patient Record). The British Medical Association (BMA) has developed a conceptual model to cover confidentiality requirements in health care information systems [10, 11]. The BMA model is discussed in detail in Chapter 3.

1.3. Access Control

Although there is no single security definition, there is agreement in the computer security literatures that computer security is required to cover three aspects:

- Confidentiality: a system resource can only be accessed by an authorised entity.
- Integrity: data has not been altered or deleted by unauthorised entity.
- Availability: services are efficiently accessible when needed by authorised entities.

Having a further deep look at the above aspects we can figure out a common factor. It seems to be the security problems comparatively speaking, which occur as a result of unauthorised access. Access control is

the security backbone. In the absence of good access control a computer system could experience a confidentiality threat for example confidential information becomes accessible by an unauthorised entity, an integrity problem as data could be modified as result of unauthorised access, and a denial of service as an example of how poor access control could affect the system availability. In computer systems security is often reduced to access control. An item of information should only be accessible by authorised users. Basically the access control is a relationship between *subject* and *object.* A subject could be user, computer program or process and an object could be file, database record/table/view, or a piece of computer hardware. A computer program could be a subject or an object. However it is not an easy job to determine a system's subjects, objects and access methods [56]. The first formal access control model was developed by Lampson [53]. Lampson's model is structured in the form of a state machine where each state is a triple (S, O, M). S is a set of subjects, O is a set of objects and M[s,o] is an access matrix containing the access rights that subject s has for object o. This model was later refined by Denning [40]. These models used the traditional access rights (read, write, execute, append) but not the more recent access rights such as those required in a collaboration environment (viewing, coupling) [78].There are two techniques to implement the access control matrix. The first one is called *capability* where the access rights are kept with the subjects and the second is the Access Control List (ACL) where access rights are kept with the objects. ACL is easy to implement and works well in simple systems or mixed ones where it is easy for users to

define their own permissions but not in systems where access permissions are defined by the system management. For instance it will be difficult to turn off access for a particular subject. In ACL there is no way to delegate access authority for a specific period of time and it is difficult to perform security checks at runtime. Microsoft Windows NT 4.0 implements ACL. The advantage and disadvantage of the *capability* is plus or minus the opposite of the ACL. *Capability* is likely to be more popular in the internet based system taking advantage from new technology such as digital certificates. However there are operating systems such as Microsoft Windows 2000 where both ACL and *capability* are used. There are two well know types of access control: Discretionary Access Control (DAC) and Mandatory Access Control (MAC). With DAC users decide how to protect their own objects while in MAC the system takes the decision by comparing the object's label against the subject's label. MAC implements multi-level security policy – a policy considered by the BLP model. Military systems are an example of MAC implementation. The Discretionary Access Control is widely used in the commercial operating systems (e.g. UNIX and Windows). Grouping Users in DAC was not enough to deal with access control administration as it is one-side grouping (subject grouping). Managing large systems in the form of subject-object pairs is difficult if not impossible especially in dynamic authorisation environments. This security administration problem was tackled with the concept of Role Based Access Control (RBAC). In RBAC users gain their access to system resources via roles. Users are assigned to roles (e.g. based on their duties) and permissions

associated with roles. RBAC can be configured to enforce both DAC and MAC [23, 63]. OASIS (An Open Architecture for Secure Interworking Services) [45, 93] is a solution for a flexible cooperate or interoperate application or service. It is a more relaxed Role Based Access Control model and it is one step forward to the task based approach. OASIS is managing roles in a different way from the other RBAC Model. It claims to support decentralised, parameterised roles and instead of delegation OASIS introduce the appointment notation. However making the hierarchies implicit, OASIS will not capture relations that might exists among roles [7]. RBAC is implemented in most of the modern database management systems (in ORACLE since release 7.3) and operating systems such as Microsoft Windows 2000. RBAC is well documented on the Role Based Access Control web page at National Institute for Standard and Technology (NIST) [60]. For further reading about the access control models and mechanisms refer to [72].

1.3.1 Need for a holistic approach

Although, more or less, there is at least one security model for each security aspect and a strong enough security mechanism and tools (e.g. cryptography) to implement these models, security systems repeatedly fail [12, 77].

Bruce Schneier in his book *Applied Cryptography* [75] described how mathematically safe and secure digital systems can be built. Two years later in the second edition of this book [74] he went as far as to write "it is

insufficient to protect ourselves with laws, we need to protect ourselves with mathematics". This book is widely cited and used. After seven years Schneier wrote another book *Secrets and lies, Digital Security in a Networked world* [77] in which he more or less rewrites the idea of the first book as he states that it was naïve to consider the cryptography as alone providing absolute protection. However that was not due to a weakness in cryptography but because there were more important aspects that need to be considered. The following concludes Schneier's general arguments:

- Systems are vulnerable and hacking knowledge is easily available.
- Causing harm does not need that much skill or special techniques.
- Technology alone cannot prevent a number of attack classes.
- Successful attacks should be published when feedback appears as an important factor in improving system functionality.
- Security problems are not about technology; they are rather about how to use the technology.
- Detection and response is the right way to improve security not by using preventive countermeasures to avoid different attacks.

These arguments were supported by a good collection of real examples and as a result of comprehensive analysis.

System developers learn from their mistakes and learn more from public feedback. The public feedback is considered as an important input to build more improved and dependable systems. To attract valuable feedback systems' failures should be published. This, however, would not always be

possible as it conflicts with basic nature of the cryptosystems. Systems other than cryptosystems are more dependable as they react to the public feedback.

Anderson in [12] emphasises this point and gives a number of examples of failures of cryptosystems deployed in bank systems. Some of these frauds are simply caused by simple errors of implementation and operation. These kinds of attacks do not require sophisticated techniques.

1.4. Cross-organisation access control projects

The following are some examples for projects using models discussed in section 1.2 and the available mechanisms to develop application for collaboration networks requirements:

The TIHI (*Trusted Interoperation of Healthcare Information*) project [90] designed as a mediator in the form of a gateway, is owned by the enterprise security officer to mediate enquiries and responses. This mediator attempts to allow protected selective sharing of information between collaborators in an environment where the available mechanisms (firewalls and passwords, private and public keys, and encrypted transmission) provide adequate protection from adversaries.

The collaboration environment (WebOnCOLL) [21] was designed on the context of the regional healthcare of Crete [84]. The security service of this

project is based on digital certificates and a combination of digital signature, public key cryptography and secure socket layer.

Coalition for Networked Information (CNI) in a discussion draft [54] exemplifies the Cross-Organisational Access Management Problem in licensing agreements and collaboration sharing by assuming that the resource operator has reached some satisfactory resolution on this question, whereas the issue is one of testing or verifying that individuals are really a member of this community according to pre-agreed criteria. CNI in this work has defined sets of analyses and evaluation criteria as follows: feasibility and employability; authentication strength; granularity and extensibility; cross-protocol flexibility; privacy considerations; accountability; ability to collect management data. These criteria were used to analyse and evaluate the requirements for the users and the resource operators against three access managements approaches: proxies, IP source filtering and credential-based (Password-based credential and certificate-based credential). The study shows the advantages and disadvantages of each approach.

The Digital Library Authentication and Authorisation Architecture (DLA3) [58] attempts to enable cross-organisational access management of web-based resources, using the digital certificates (X.509 standard) and secure directory services (LDAP directory standard). It aims to implement authentication and authorisation functions in the context of licensed

information resources in university libraries. However the author of this paper argues that DLA3 might help in a situation where there is a need to restrict access to particular individuals across the organisation boundary. DLA3 is based on three principles: 1) privacy by ensuring that the service provider knows only that the individual is an authorised member of the consumer institutional community as a default case; 2) information partitioning; 3) separation of authentication. The future plan was a pilot project, sponsored by the Digital Library Federation DFL, to cover the following issues:

- Formal specifications and procedures.
- Further test for the Statistical Role, Persistent Identifier and Access Denied Message, and working out to be part of the service provider licensing negotiation process.
- Certificate revocation.
- Caching guidelines.
- HTTPS (secure HTTP) transaction with attributes and values to be encoded in XML.

For future work, in addition to the above issues, the team which has developed DLA3 aims to consider the Cross-Organisational Access Management approaches proposed by Lynch [54].

Work by Neil Ching and Vicki Jones [22] attempts to argue that the identity of the client will often not be enough by itself for a service provider to determine whether the client is permitted to access the service (e.g. whether

the client is over 21 years of age). The general idea of this work to tackle the problem of the identity is that a service provider generates a permission (credential) regarding a specific client's request, rather than giving fixed permission.

The Defence Advanced Research Projects Agency (DARPA) [29] has sketched a security architecture to control the flow of the information, codes, and access to services across boundaries at two levels: enclaves and domains. An enclave is the lowest level network unit (LAN, Workstation) and a domain is a set of enclaves sharing some characteristic. In this work the classification boundary, which is a set of enclaves that operate at the same security classification level, was particularly discussed. Within or across classification domains, there may be several types of interrelationships reflecting different trust and collaboration. A boundary controller provides functionality for the security requirements, such as authentication, encryption, filtering, labelling and auditing. A common public key infrastructure (PKI) is one possible mechanism to allow interoperability among enclaves. Security labels are used to preserve the source sensitivity level of shared information.

Several architectural models for such cross-organisational access management services have been developed at Columbia University by introducing a broker service to consolidate and generalise access

management. This service includes an Access Management Broker server and a plug-in module for web servers [58].

As a part of the Stanford Digital Library Project and in the context of FIRM (Framework for Interoperable Rights Management), a new architecture for security and access control in heterogeneous network environment has been prototyped. This architecture considers the security issues as relationship management rather than information access control and as network-centric rather than client-based or server-based. To support the idea of network-centric they have introduced what they call *commpact* or a first class relationship object. A *commpact* provides an encapsulated information control and establishes a many to many relationship between itself and the objects and the service that they control. The framework that was designed in this work encapsulates the agreements, contract and other factors between the participants in the form of *commpacts* which control the communication services between them. Furthermore this work aims to support the trusted shareability issue along with the privacy issue [67, 68].

All the works above are based on models discussed in 1.2 and 1.3. Subsequently none of the above projects provide a complete framework to fulfil important requirements of collaboration networks and multi-agency applications, such as: need-to-know; limiting the use of information for a specific purpose; responsibility tracing; authorisation management and relationship.

1.5. Multi-Agency environment

So far we have discussed models for applications that only deal with a single security policy. Matters start getting harder as networks grow, applications become more complex and society's reliance upon information technology grows. This is reflected in the increase in collaborations between different organisations that wish to share information for mutual benefit. These organizations take advantage of the progress in information technology in the last ten years (e.g. internet and WWW) that facilitate information sharing. The demand for collaborative networks and the nature of some applications that require multiple agencies to be involved in an integrated network create a real security challenge. In such environment: ownership is no longer static; responsibilities are difficult to trace; it is difficult to determine who has right to access what, for how long and who is authorised to decide about all these aspects.

1.5.1 Ownership and access right

In sections 1.2 and 1.3 respectively, we have discussed security models and access control. We note that all the above models assume the ownership is definite and the authorisation is conventional (assuming that it is clear who is authorised to have access to each object in the system). If you own something, it means that it legally belong to you [Cambridge dictionary]. The right to own, right to access and to control are more or less political issues. It is important to distinguish between the right to own and the ability to own and the right to have access and the ability to have access. The right

to own is what can be legally claimed. For instance a patient has a right to own his/her medical record. The ability to own is about being able to take the responsibility. For example the unborn child has the right to own his/her personal data but will not be able to act as an owner for this data. Moreover you are not always able to own what you have a right to own. For instance you cannot destroy your medical record. The right to access is what the regulation and rules support. For example you have the right to access the information that is related to your safety at your workplace. Right to access can be also claimed based on need-to-know as discussed further below. The ability to access depends on the situation, so the access might be granted or rejected. For example you have the right to gain access to your medical record but your doctor may prefer not to allow that as it may affect your treatment. Traditional access control such as DAC and MAC deals with the capability to own and the capability to access. MAC enables the system to own all the system's objects, while DAC enables the system users to own part of the system's objects (e.g. those created by them) and allows them to delegate this ownership. There is no framework to link the right and the ability to own with that of access. This framework is crucial to deal with security requirements for a multi-agency application, where ownership is a dynamic property.

1.5.2 Need to Know

Need-to-know is an important security aspect in a multi-agency environment. This section attempts to introduce this term. In fact the need-to-know term has been used to refer to two different aspects: the need-to-know as a claim or requirement and the need-to-know as a basis for authorising an access to confidential information.

Need-to-know as a claim/requirement:
Need-to-know can be briefly defined as a claim by individuals or an organisation to know a set of information in order to carry out an assigned job.

Need-to-know as a requirement/claim is defined in the American National Standard [1] for Telecommunications as follows:
"Need-to-know is the legitimate requirement of a person or organization to know, access, or possess sensitive or classified information that is critical to the performance of an authorized, assigned mission, or the necessity for access to, or knowledge or possession of, specific information required to carry out official duties".

In health informatics the term need-to-know is used in the Department of Health's draft Guidelines [31] as the basis on which disclosure of personal health information to those authorised to receive it should be allowed [42].

Need-to-know as authorisation base:
Need-to-know as an authorisation rule, is to permit access to specific information required to carry out official duties. The "least privilege" is a principle to implement this rule [73].

Although the need-to-know as an authorisation basis is common in military systems, it is also considered in systems such as health care information systems, for example principle 4 of Caldicott's principles and recommendation. Chapter 5 discuss these principles and recommendation in more details.

1.5.3 Multi-agency applications

A motivating example of an application that involves multi-agency services is the Electronic Patient Record (EPR) or more general Electronic Health Record (EHR). We could summarize our scope of health care security requirements in two general, equally respected, goals:

1) Good quality of health provision (not only for a certain patient but for all the society e.g. medical research requirements) and

2) Full respect for the patient rights. Actually, the main security requirements are implicitly included in these two goals. For instance availability and integrity are included in the first goal while confidentiality is included in the second goal. It is understood that the first goal (good quality of health provision) is relatively easier to achieve than the second one (the patient's right). In other words the main concern is now given to the patient's rights (fair and lawful use for patients' personal and medical information).

---

[1] American National Standard for Telecommunications Telecom Glossary 2000, http://www.atis.org/tg2k/t1g2k.html).

Ross Anderson in 1996 had developed a security policy model [11] to address the security problem in the health information systems. Anderson's model is known as the BMA model and particularly focuses on patient confidentiality requirements. It is comprised of nine principles based on the idea that access to a patient record will only be authorised in the presence of a patient consent. This model is investigated in more details in Chapter 3 including verification of whether this model is sufficient for the multi-agency security requirements in health care. The results of this investigation are also published in [5].

The Dynamic Coalition is another multi-agency environment, where different parties are engaged in a network to communicate and share information. However a great challenge is facing these allies as they have different interests, perform different functions using different approaches and methods, and more importantly they operate under different policies and often commanded by their own administration. Chapter 6 introduce the DCE with a brief discussion for the active research in this area. We also have used a DCE case study to demonstrate the functionality of our model (see Section 6.2).

1.6. Our approach

In our work we investigate a number of problems. Why is security policy implementation difficult, especially in the multi-agency service environment where security policies come from multi-resources? Why is there almost

complete agreement about policies but much more debate on the implementations? Why is it difficult to resolve the conflicts that rise as a result of different interests? Why are these regulations, principles and rules implementable in real-life law systems and not in information systems?

An answer for the above questions could alleviate most of the security difficulties and lead to a better understanding of the multi-agency environment security problem.

In law, the principles give the overall policies. In particular circumstances a lawyer would look further.

We make mistakes whenever we attempt to implement a general principle for cases that are not necessarily the same when the full detail is considered. It is easier to regulate a well-defined case. In our model, the twin protocols allow collaborators/task's participants to use general principles to regulate and control a specific task. In addition, collaboration, by definition, is based on the needs of the collaborators from each other.

We have developed a task-based model, which we argue will alleviate security difficulties in the multi-agency services and in the collaboration networks.

Our model covers multi-agency difficult requirements such as:

- Relationship, responsibilities, authorisation, need-to-know, and access control restriction (by time and purpose).

1.6.1 Task-based approach literature review

We consider two aspects of our work. Firstly the extent to which task-based approaches have been used before in security systems; secondly the usability and computability of task-based approaches in the security area.

The task-based approach has been introduced before in a number of models [34, 80, 81]. All were at the basic level of this approach. The focus in [80, 81] was on whether a task-based security model could be an alternative authorisation and access control model to the subject-object traditional authorisation models. While in [34] Fischer-Hubner and Ott tried to address the privacy problem using the task-based approach. We intend in our model to use all of the power of this idea (task-based approach) to address the security problem of the collaboration networks and the multi-agency services environment. In more detail:

The Group Security model (GSM) [80] by Steinke was described as a security model, which provides access to information on the basis of a user's task. However some features of GSM are already rather obvious in existing information systems infrastructure. For instance in any relational database, it is always possible to grant users/roles to functions, procedures, and packages rather than grant them to the information objects (e.g. tables, views). These functions, procedures and packages are in fact tasks and group of tasks and also can be functionally minimized. GSM considers the discretionary security approach to deal with ownership. Overall GSM is more suitable for hierarchical systems, where the responsibilities are visible.

Thomas and Sandhu [81] introduced the task-based approach initially in 1994 as an approach to address integrity issues in computerized information systems from an enterprise perspective. Subsequently in 1997 they [82] developed their approach to produce a paradigm for access control and authorisation management. The developed model is called Task-Based Authorisation Control TBAC.

Fischer-Hubner and Ott [34] in their model attempted to address the privacy aspect using the task-based approach. The nature of the task-based approach eases the handling of the main privacy requirements such as:

- Purpose binding: personal data obtained for one purpose should not be used for another purpose without informed consent.
- Necessity of data collection and processing: the collection and processing of personal data shall only be allowed, if it is necessary for tasks falling within the responsibility of the data processing agency.

In contrast to the models of Steinke and of Thomas and Sandhu, this model takes a forward step to de-centralise the authorisation using a 4-eyes principle. 4-eyes principle consists in performing an operation by one user and confirming it by another one, both users should have sufficient rights of access to perform this operation. However there were no end-user requirements supporting this model and the 4-eyes principle is not enough to ensure de-centralisation. The set theory which was used to represent this model is not proven, nor is it in a framework (Petri nets, Category theory, LaSCO, Ponder, VDM, Z, ...) where proof is done by following constructive

principles or through following rules guaranteeing a particular outcome. Finally the Fischer-Hübner and Ott model does not include collaboration requirements.

In 1990, Mahling, Coury and Croft [55] tried to build a task-based collaboration model. However this work starts from a relatively late stage in the negotiation where the plan, agreement and tasks are relatively clear. In addition their work does not consider the case of the multi-agency environments where the policies of the collaborators are different.

The state of the art is fragmented due to lack of cohesive and collaborative research in this area. Researchers, by and large, are working independently. Apart from Steinke's [80] citing of Mahling [55], no other cross-citation to others in the field have been made.

We argue that the real challenge for the task-based approach is the multi-agency services environment, where responsibilities are distributed and the ownership is dynamic. None of the existing approaches have considered the multi-agency aspects in detail. Furthermore the other issue of any computer system design including security system is the *usability* [52]. This issue was ignored in most of the above security models.

1.6.2 Other uses for the Task-based approach

Task Analysis:

Task Analysis (TA) is a method in Human-Computer Interaction and Software engineering. It is an analysis of tasks in terms of human behaviour.

Historically TA was founded at the end of the sixties and was used to meet training needs. There were a number of TA methods developed for this purpose both in the UK and in the USA. The Hierarchical Task Analysis (HTA) was the most successful method. HTA was developed by Annett and his colleagues in 1971 [48].

The task analysis method (in HCI or training) was used to analyse an existing task to figure out important points particularly in the human behaviour to design a convenient computer interface or training courses to people [33, 49, 50].

Task analysis has been mainly used for what is so called Task Analysis for Knowledge Description (TAKD). As it stands, it is the opposite direction of our approach, while we create a task this approach (TAKD) analyses an existing tasks. However there could be a use of some methods of this approach in our model where there is a need to create a task based on another existing one.

1.6.3 Usability and computability

Usability and computability are almost equally important issues. It is not sufficient for a computer system to be robust, dependable, and cover all the expected functions (computability). It also has to be accepted by its users, in other words it has to be user-friendly (usability). Social specialists and some groups of information and computer specialists argue that the issue of

"usability" has more to do with developments and implementations of computer systems than their computability. Certainly the computer security issue is not an exception from this rule. Indeed usability factors such as politics, organization policy and rules, human behaviours and modes, groups and individuals' interests are very much involved in the design of a secure computer system. For instance a long and difficult security procedure may affect the system availability and/or encourage users to skip some steps of the procedure. In addition to its coverage of the issue of computability, our model will also suitably fulfil the usability requirements since it considers direct participation of the users. For example it is not necessary, in our task-based model, to fully computerize a given task; it depends very much on the result of the negotiation between the parties involved in that task.

1.7. Thesis structure

The thesis is structured as follows. Chapter 2 (next chapter) covers analysis of the origin of security requirements. It includes general regulations such as:

1. Universal Declaration of Human Rights.
2. Data Protection Act.

and Medical Ethics such as:

1. Helsinki Declaration
2. Council of Europe
3. BMA (Ross Anderson)
4. Caldicott
5. Debate about the above including.
    a. Clause 67 Health and Social Care Act
    b. The British Medical Association (BMA)
    c. Administrators at The National Health Service (NHS)
    d. Other Groups
6. Patient Rights versus Public Interest
7. Consequences of computer use

At the end of Chapter 2 we discuss our findings from the analysis and review some related work.

Chapter 3 covers formal analysis for an existing security model (BMA). We analyze, in depth, the security model of Anderson using formal methods based on security policy languages: ASL, LaSCO and Ponder.

This is followed by a discussion that raises issues such as the difficulty of representing all the principles in a logical manner.

The conclusion of Chapter 3 includes a recommendation for our approach that is task-based. This prospect is more likely to deal with the multi-security security requirements that exist in medical applications and are not dealt with in the BMA model.

Chapter 4 covers the development of our Task-based Security Model starting with a review for security models with an emphasis on task-based approach. The development of the CTCP/CTRP model and its two protocols, the Collaboration Task Creation Protocol (CTCP) and Collaboration Task Runtime Protocol (CTRP), are discussed in detail including representation of the CTCP and CTRP protocols using Petri nets. A simple example is used to demonstrate the two protocols. It also covers a discussion for the model capability of handing errors and exception. In addition this chapter cover a discussion for the different approaches to implement the model.

Chapter 5 reviews our model against the requirements, in particular reflecting principles in DPA and Caldicott against TCP/TRP.

Chapter 6 covers the work in the case study.

Finally, in Chapter 7 we provide an overview of the work done, emphasize our contributions and compare it with other related works.

The appendices at the end include additional detail on aspects such as: the DPA principles and the Caldicott principles.

1.8. Conclusion and Contribution summary

Ross Anderson in his book *Security Engineering* [9] categorized security models according to the way the data flow: vertically named *Multi-level Security models* (MLS) or horizontally named *Multilateral Security Models* (MSM). Models such as Bell-Lapadula Model (BLP) [15], Harrison-Ruzzon-Ullman Model (HRU) [43], Biba Model [16] and Clark-Wilson Model [24] were listed as MLS, while Chinese Wall Model [17], lattice Model and British Medical Association (BMA) [10, 11] were considered as MSM. Section 1.2 discusses them in more detail. Security requirements in a multi-agency service environment come under Multilateral Security policy. However none of the three models covers all of the multi-agency security requirements. The lattice model shows how to isolate compartments but not to manage information flow [9]. The Chinese wall model deals with one specific security policy which is the conflict of interest. In addition the access rights assignment is centralized. The BMA model is analysed and verified against some of the multi agency requirements. Details of this study are discussed in Chapter 3 and reviewed in [4, 5]. We argue that a task-based prospect approach would properly deals with these requirements. A model based on

this prospect was developed and verified with an example of medical security principles and a real world case in health informatics. The developments of the model and its testing with a simple example are discussed in Chapter 4 and viewed in [2, 3]. Justification of health record security principles through our model is discussed in Chapter 5 and reviewed in [1]. Finally grounding of the model and its idea using a real world case study from health informatics are discussed in chapter 6.

1.8.1 Contributions

The contribution of our work can be summarised in the following points. We have:

- Looked at security in general including security policies, models and mechanisms.
- Introduced multi-agency security requirements.
- Used health informatics requirement as an appropriate example for multi-agency problem.
- Reviewed current declarations, legislation and regulations to bring together a global, European and national perspective for security in health services.
- Critically examined a British model, BMA, in formal terms using graphical and constraint-based languages. Showed strengths and weaknesses in handling security requirements. In particular need-to-know was a significant omission from the BMA model.

- Developed novel task-based CTCP/CTRP model based on two linked protocols. Collaboration Task Creation Protocol (CTCP) was used to establish a framework for handling a request for information. Collaboration Task Runtime Protocol (CTRP) was used to run the request under the supervision of CTCP.
- Reviewed the model for technical completeness, satisfaction of software engineering principles, completeness, focus, readability and procedural transparency.
- Tested the model against two case studies, a simple one for illustration purpose and a more complex one for evaluating the model's coverage, neutrality and focus.
- Evaluated the overall performance of the model.

Chapter 2

SOURCES OF SECURITY REQUIREMENTS

SECURITY REQUIREMENTS FOR MULTI-AGENCY SERVICES IN HEALTH CARE

2.1. Introduction

As introduced in Chapter 1 the security policy is the basis of computer system security, and we have seen that security policy is derived from security requirements. Indeed there is no single security solution and the security definition depends on security requirements. Often security systems fail because the security requirements were misunderstood or the wrong policy was implemented. Security goals are relatively clear but we have to have rules and regulations to meet these goals. These regulations are usually found to be not enough or/and conflict with each other (see Section 2.5). The need for new regulation and rules never stops. In our work we deal with security management in a multi-agency environment. The Electronic Health Record (EHR) is a good example of a multi-agency applications, as there are non-medical bodies that claim to have right to have access to the patient information. Moreover regulating the use of the patients' information is an

active research subject. Security requirements in health care information systems will be our security requirements example.

2.2. Security Requirements Resources

In business-oriented information systems, requirements are determined by interviewing a single client. For instance techniques such as OMNIS [35] have been particularly designed for handling the documentation and analysis of such user requirement. Fundamentally, requirements come into view as a result of the observation of existing systems along with information on how to improve, add more functions/services or maybe change to a better situation.

For requirements in general including those for security, the first stage of requirements is often rhetoric, such as a complaint about services, a request for new services or an invitation to react to environment changes or new regulations. The second stage of the requirements takes the form of statements/principles. These statements or principles aim to predicate the general requirements in rhetoric and make them more specific and appropriate for further developments.

In security systems the general rhetoric aims to achieve the three main aspects of security: confidentiality, integrity and availability. In some literature accountability is counted as a fourth aspect. However accountability is not an objective in its own right. Rhetoric in this case is regularly expressed as general security statements formally called a security

policy or security regulation depending on the application. There could also be concerns about existing threats to the system.

The concept stage in security requirements could be security principles, security policy models or any revised version of security statements such as official rules and regulations of an organization, ethical codes in a moral network and beliefs of an individual or group. Ross Anderson [9] illustrates general definitions, worth mentioning, for the security policy models along with some examples including his model for the British Medical Association (BMA).

In the following sections there will be a discussion of the better known related regulation documents by international, European and local (UK) organisations such as the United Nation, the Council of Europe, the World Medical Association, the UK Parliament, the UK NHS and the British Medical Association (BMA).

2.3. General data protection

2.3.1 Universal Declaration of Human Rights (UDHR) 1948-1998

Based on the foundations of freedom, justice and peace in the world, the development of friendly relations between nations; the protection of human rights by law and rules and the endorsement of the social progress and better standards of life in larger freedom on 10 of December 1948 the General Assembly of the United Nations adopted and proclaimed the Universal Declaration of Human Rights (UDHR) [85, 86]. UDHR, composed of 30

articles, aims for a general standard for the protection of the human rights. Since the personal data of a man or woman is a personal property, according to article 17 he/she has the right to own this data and should be aware of any use of this data. On December 1996 the International Covenant on Civil and Political Rights was adopted and opened for signature, ratification and accession by the General Assembly resolution, and was entered into force 23 March 1976, in accordance with Article 49. This covenant comprises 53 articles of which the 30 UDHR articles are the first part. It should be noted that the UK was among the countries that had signed this agreement.

2.3.2 Data Protection Act (DPA) 1984-1998

The first Data Protection Act 1984 [41] governs the processing (including obtaining, storage, deletion, manipulation and disclosure) of personal data. Personal data is any piece of information that refers to a living individual, who is referred to as a data subject. DPA 98 supersedes the Data Protection Act 1984. DPA 1998 in its eight principles attempts to comply with human rights declarations such as UDHR and particularly to implement the EC Directive 95/46/EC. The eight principles of the DPA 98 could be summarised according to each principle as following:

Principle 1: the limit of personal data processing. This principle limits the processing of personal data by an explicit consent from the data subject, or in circumstances where consent cannot be obtained and the data process is needed to protect the subject's vital interests or the processing is necessary for

medical purposes and is carried out by a health professional or someone whose duty of confidentiality is equivalent to that of a health care professional. In general terms the personal data should be processed fairly and lawfully.

Principle 2: limit personal data processing for specific purpose/purposes. Personal data shall not be processed outside of the proposed purpose/purposes.

Principle 3: processing only the adequate personal data.

Principle 4: processing accurate and up-to-date personal data.

Principle 5: limit processing personal data by specific period of time.

Principle 6: complying with the data subject's right under this act.

Principle 7: data protection and safety. Personal data should be protected by all the measures available against unauthorized access and/or loss/damage.

Principle 8: Data flow control. Personal data should not be transferred to another country, where there is not an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. For a complete list of DPA principles refer to appendix A.

2.4. Medical ethics

There are a number of official statements and principles from which security requirements for health information systems can be derived. All of these principles aim to protect the patient's sensitive information particularly person-identifiable information based on the patient's rights. However it has

been understood that some of these principles implicate high debates and conflicts. As a result an implementation of this requirement was a difficult task. In fact there are two general, equally rated, goals for health care services: a good quality of health provision (not only for a certain patient but for all of society e.g. medical research's requirements) and full respect for the patient rights.

2.4.1 World Medical Association Declaration of HELSINKI 1964-2000

The World Medical Association (WMA) [92] in its 18th general assembly in Helsinki on June 1964 has adopted the Ethical Principles for Medical Research Involving Human Subjects, which is known as the WMA policy, or the Declaration of Helsinki. This policy was later amended by the:

29th WMA General Assembly, Tokyo, Japan, October 1975

35th WMA General Assembly, Venice, Italy, October 1983

41st WMA General Assembly, Hong Kong, September 1989

48th WMA General Assembly, Somerset West, Republic of South Africa, October1996 and the

52nd WMA General Assembly, Edinburgh, Scotland, October 2000

The WMA policy comprises 32 principles developed to provide guidance to physicians and other participants in medical research involving human subjects including research on identifiable human material or identifiable data. In principle 10, in which the duty of a physician in medical research is considered, the privacy was valued as equal to the life, health and dignity of the human subject. In addition principle 21 invites every precaution to

respect the privacy of the subject and the confidentiality of the patient's information.

2.4.2 The Council of Europe Recommendation No. R (97) 5:

The Recommendation No. R (97) 5 [26], which superseded the Recommendation No. R (81) 1 on regulations for automated medical data banks. R (97) was adopted by the Committee of Ministers on 13 February 1997 at the 584th meeting of the Ministers' Deputies. This recommendation, based on the general principle of data protection, asks the governments of member states to ensure that the principles included in this recommendation are reflected in their law and practice. The principles of R (97) attempt to protect the automatic processing of three types of data: personal data, medical data and genetic data. The principles that deal with patients' rights in this recommendation can be summarised as following:

Principle 1 defines important terms such as personal data, medical data and genetic data. Principle 2 represents the recommendations' scope. Principle 3 highlights the high respect for the privacy recommending that privacy should be guaranteed during the collection and processing of medical data. Principle 4 regulates the patient data provision. Figure 1 illustrates the R (97)'s conditions that control the provision of patients' data. Also in principle 4 an unborn child owns his/her data although the holder of parental responsibilities may act as the person legally entitled to act for the unborn child. In addition principle 4 specifies two purposes for obtaining genetic data. However these purposes are already included in the general condition of

this principle. Principle 5 recommends that a data subject should be aware of the use of his/her data. In the case of the data subject being a legally incapacitated person the information should be given to anyone who can legally act in behalf of the data subject. Data subject consent was considered in principle 6 as it should be freely expressed and informed and once it is obtained should not be exceeded particularly in the formulation of results for a genetic data process. Comparing Figure 2, which illustrates conditions for principle 7, with Figure 1, which illustrates those for principle 4 the only difference is the condition dealing with the protection of the data subject's right and freedom. Principle 8 lists the data subject's right, such as that to have access to his/her data, and the exceptions where these rights are not applicable, for instance the interests of protecting state security, public safety or the suppression of criminal offences. Principle 9 recommends the appropriate technical and organisation measures to be taken to ensure the general data security requirements such as confidentiality, integrity and availability. Principle 10 asks for a proper archiving system particularly linking the data with the purpose for which they were collected and processed. Principle 11 recommends certain conditions to control the data flow to states where the recommendation R (97) or similar regulations are adopted. Recommendations in the last principle number 12, give guidelines to control the use of the confidential data in the scientific research.

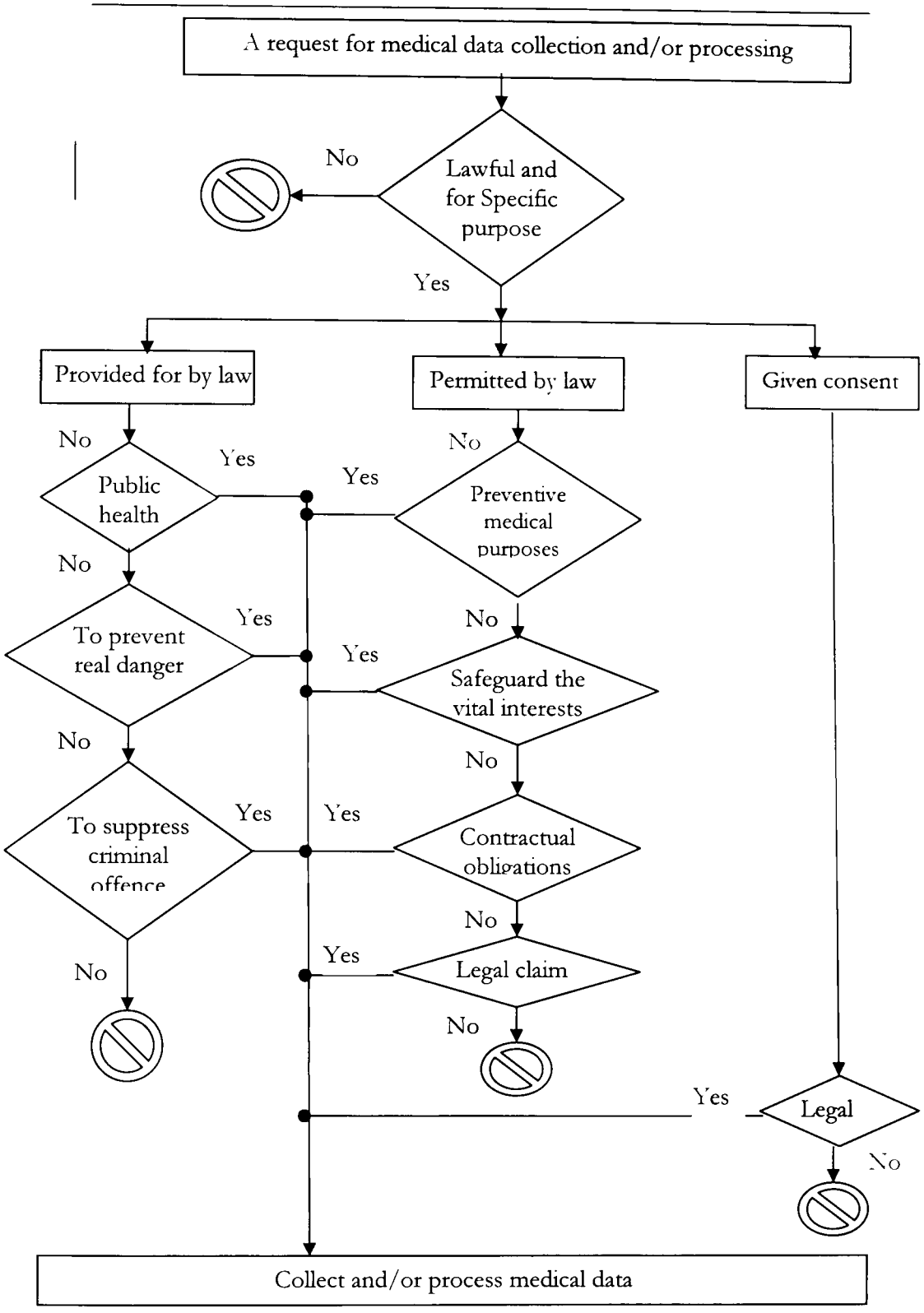

Figure 1: R (97)'s conditions for controlling the provision of patients' data

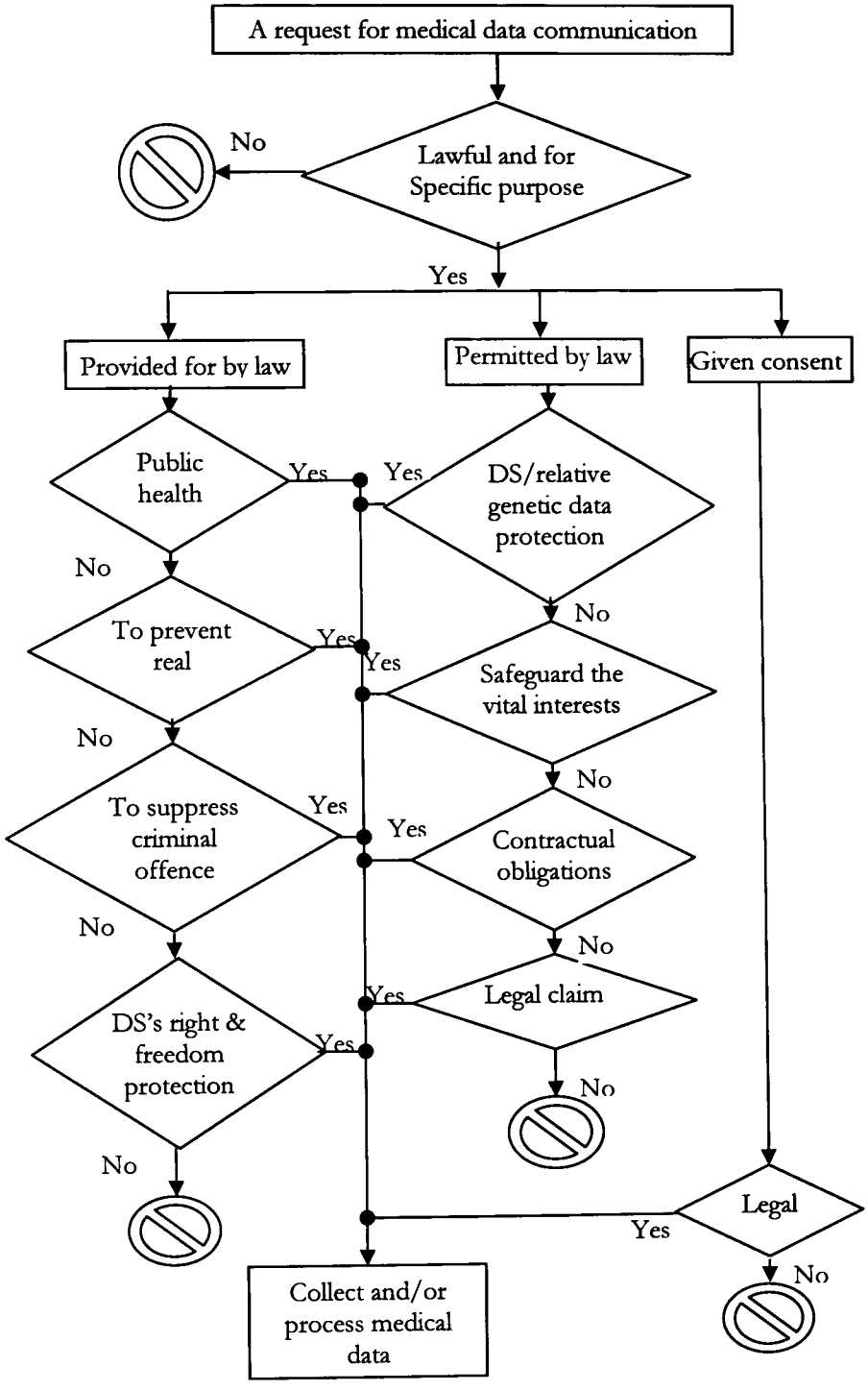

Figure 2: R (97)'s conditions for controlling the medical data communication

2.4.3 BMA Security Policy Model 1996

As a response to the remarkable number of reports considering the low care for the patients' privacy and the confidentiality of information in the medical data processing, the British Medical Association (BMA) invited Ross Anderson, a reader in security at Cambridge University, to consider this problem and prepare a security policy for clinical information systems [11]. Although some professionals in health care information technology believe that any implementation of Anderson's principles would be expensive to implement and unmanageable to maintain, others such as Denley and Smith [30] according to their experience in the implementation of these principles in three British hospitals: Conquest Hospital, Aintree Hospital and Royal Devon and Exeter Hospital, state that Anderson's principles can be applied to the electronic patient record to maximise privacy. However, the CEN (Europe Committee for Standardization) group [83] observes that Anderson's model is specified at too high a level for practical purposes and is not provable complete because it is neither precise nor exhaustive. Cohen [25] has proposed a formal model, complementary to Anderson's, which is again not accepted by the CEN group because it is not shown to be complete and because it is not based on basic security properties. The BMA model did not consider the multi-agency security requirements and it was found that the issue of sharing clinical information including collaboration activities with other agencies such as police, social services or the education authority was

not clearly considered. For instance the need-to-know problem was not addressed in the BMA model, as the BMA does not accept that need-to-know is an acceptable basis for access control decisions, although, as discussed in Chapter 2 there are cases where need-to-know cannot be avoided. Chapter 3 covers this work in detail where the BMA model's principles were examined logically by representing them using some selected languages for specifying security policies.

2.4.4 Caldicott Principles 1998

A different approach was taken in the Caldicott principles, which can be seen as specialisation of the DPA (Data Protection Act) for health care systems.

The Caldicott Committee was established by the Chief Medical Officer to review all patient-identifiable information, which passes from NHS organisations in England to other NHS or non-NHS bodies for purposes other than direct care. The committee work aims to met requirements set out in the Protection and Use of Patient Information issued under HSG(96)18. These requirements can be summarised in two points: 1) person-identifiable information should only be transferred for justified purposes and 2) only the minimum necessary information is to be transferred in each case. The work of the Caldicott Committee resulted six principles and sixteen recommendations.

For a complete list of the Caldicott principles and recommendations refer to appendix B.

2.4.5 Government Bills e.g. Health & Social Care clause 67 (2001)

As stated earlier in the introduction to this chapter the security policies keep changing to cover gaps left by the active security policies or to protect against new threats. However security vulnerability could be a result of a misplaced or misinterpreted security policy in whole or in part. In health care all regulations and security principles are supposed to support two main objectives: 1) a good quality of health provision, not only for a certain patient but for all of society (e.g. medical research's requirements) and 2) full respect for the patient rights. These objectives often are used as a context to evaluate health care regulation. Government bills are just an example. In health care the controversial Health and Social Care clause 67 2002 [18] is the latest regulation for the use of patient data. This clause attempts to empower the Health Minister for the authorised collection and use of patient information.

2.5. Debate

Although all the above mentioned regulations deliberately aim to preserve patient rights and to ensure good quality health services, their interpretations imply conflict with each other and are repeatedly misinterpreted. As a result much debate was raised immediately after each new declaration between groups supporting different principles. In the following subsections there will be a discussion of these debates. The debate can be summarized as a discussion about overriding one patient right by public interest or vies versa.

2.5.1 Patient right's side (e.g. BMA and Ross Anderson):

It is all about a balance between patient right and public interest such as using patients' data (medical and possibly personal) in research. Ross Anderson and his group are considered to fight on the patient side where they support their arguments by documents such as the Declaration of Helsinki and the Council of Europe Recommendation No. R (97) 5. The Anderson model for the BMA is strongly on the side of the patient as it tries to control use of the patient data by what is called patient consent. To keep the balance of power in medical informatics, this group keeps arguing against all rules following their model that gives more power for non-clinical bodies. Clause 67 was criticized [13] by Anderson for tilting the balance of power in medical informatics. In his comment about the Caldicott Principles, Anderson argues that making the patient data available for non-clinical use will cause much trouble and the use of NHS numbers as identifiers will not solve the problem as the de-identified data problem will still exist.

2.5.2 Public interest (National Health Service NHS)

This is motivated by the intention to improve the health services government's bodies such as the NHS. A number of regulations [18, 20] have been issued to give more power to non-medical staff. These regulations are seen by patient rights defenders as violating the general human rights declarations (see pervious section). However the patient rights were not completely ignored in these regulations. The Caldicott Principles aim to make the use of patient's identifiable information more secure so as to comply with

patient's right. Nevertheless these principles were seen as not strong enough to protect patient's privacy [8].

2.5.3 Further debate

Neutral directions exist such as those which argue that patient's privacy is essential but that it should not be given more weight than the quality of care and health status. An appropriate example for these directions is found in [32]. Detmer's arguments can be summarised in the following points:

- There is still no existing law in USA to penalise for the transgressions of medical privacy.
- Despite the European agreement about the personal data protection, the practice varies widely between and within nations.
- International policies concerning this issue in Europe and America are different and there is a need to resolve it but how?
- The major debate in personal information is resolved around the practical meaning of privacy. (Protection to be fair, useful and enforceable)
- Health has been considered as both an intrinsic and an instrumental good while privacy has been considered exclusively of instrumental value.
- The tradition of individualism, loss of trust, and a recent weakened concept of community are behind the legal problem of privacy.
- There might be a risk in the situation where the privacy is more heavily weighted than the quality of care and health status.

- The aim of the medical research is to improve medical care and human health, so if there is any need for access to personal medical information it should be allowed. (e.g. Sometimes you need to differentiate between two patients having the same name).
- There is scant research data to support the above arguments and almost all the available data is based upon public opinion.
- According to Harris-Equifax's survey only 30% of the American population greatly valued privacy, 55% were willing to trade-off privacy and 15% do not see what the issue is all about.

Detmer calls for research to address problems such as: patient's awareness of the use of his/her medical information, protecting patient data from unauthorised access and from misuse, and sufficiently penalising those who falsely obtain or misuse medical records. However these problems are general security requirements for any medical information systems.

Such arguments were implicitly supported by Den Hoven [88]. In addition he highlights the need for balancing between the improvement of the health care and privacy. Detailed studies for all sides of the problems are essential. Donald Willison [91] in a contribution to Detmer's argument focuses on how to ensure that researchers will not misuse the personal information rather than forbid any access to that information.

2.5.4 Balancing patient rights with public interests

The World Medical Association Declaration on the Rights of the Patient (WMA) explicitly states: in its first principle (Right to medical care of good

quality) that every person is entitled to appropriate medical care. This means that all possible measurements and mechanisms should be deployed to achieve the best possible health quality not only for individuals but for all society. Equally the patient right to confidentiality was considered (WMA principle 8). Although this principle calls for protection for all patient's identifiable information and for their disclosure only if the patient gives explicit consent, it does allow disclosing information on a "need to know" basis.

Other examples are found in regulations such as the Recommendation No. R (97) 5 (section 2.3.2), where Principle 3 emphasizes the high respect for privacy recommending that privacy should be guaranteed during the collection and processing of medical data. However principle 4 regulates the patient data provision in that it allows the disclosure of patient information in cases such as: considering public health, preventing real danger, suppressing criminal offence, preventive medical purposes, safeguarding the vital interests, contractual obligations and/or any other legal claim. A similar example is found in Caldicott principles (section 2.3.4) and Health & Social Care clause 67 (section 2.3.5)

2.5.5 Confidentially threats in comprised medical record

Information technology (IT) significantly helps to improve the quality of health care in the everyday administration and clinical work at the primary and secondary heath care units. For instance it might be used for easy patient registration, patient diagnoses, prescribing ...etc. It helps in long term medical

plans and projects such as medical research as it provides tools and techniques to make the most of the collected data in reasoning about existing diseases or to find a cure. There is a cost in preserving patient's rights including patient's privacy. Nevertheless as there are techniques to make data available so there are others to protect it, though this is not an easy task. Computers have made it easier to bring data together for research purpose but against this patients are worried that their details will be readily publicised.

2.6. Conclusion

Security requirements can take different forms: declarations, recommendations, rules and principles. The requirements and originate from a different level of authorities: local (e.g. Caldicott recommendation), national (e.g. DPA), regional (e.g. Council of Europe recommendations) and international (Universal Declaration of Human Rights (UDHR) 1948 and Declaration of Helsinki).

Capturing multi-agency security requirements is a difficult task as:

- The security requirements originate from different resources and takes different forms.
- There is no standard to interpret security requirements.
- Security principles and regulations are too general.
- Security principles and regulations are inherited from each other and may give rise to conflict.

- There is a lack of models and frameworks in which conflicting security policies can communicate.

Electronic health record security requirements can be summarised into the following points:

- Patients have the right to own their medical, personal and genetic data, and to be aware of any use of this data, and when possible their consent should be sought before any new authorisation is granted.
- For society, heath and safety are vital hence the data of individuals can be obtained in restricted cases such as: considering public health, preventing real danger, suppressing criminal offence, safeguarding vital interests, preventive medical purposes, contractual obligations and/or any other legal claim

Chapter 3

FORMAL ANALYSIS FOR EXISTING SECURITY POLICY MODEL: BMA

3.1. Introduction

In this chapter we will discus a security policy model for a clinical information system and investigate whether logical languages can represent the principles of this kind of model. We have used three security logical languages: the Authorization Specification Language (ASL), a Language for Security Constrains on Objects (LaSCO) and Ponder: a Language for Specifying Security and Management Policies for Distributed Systems. ASL focuses more on the access control policies and LaSCO attempts to express constraints on objects, while Ponder aims to specify security and management policies for distributed systems. Additionally they are different from the language's character point of view. Whereas ASL is based on logic and LaSCO policies are specified as logical expressions and as directed graphs, Ponder is a declarative language inheriting its syntax from the OCL "Object Constraint Language". We will also study whether these principles are sufficient to deal with the case of multi-agency services and sharing

information with the different agencies such as social services, police and education authority.

For economy of expression and to make it easy for readers to link with Anderson's model, we will assume that the clinician is female and the patient male.

The intent of the security policy model for clinical information systems proposed by Ross Anderson [10, 11] is to allow the British Medical Association (BMA) to meet security requirements of the electronic patient record (EPR) and to be the base of any proposed system claims to operate the EPR. Anderson's model is composed of a set of principles based on a statement found in the Good Medical Practice booklet issued by the General Medical Council (GMC), which says:

> *Patients have a right to expect that you will not pass on any personal information, which you learn in the course of your professional duties, unless they agree.*

This raises the following questions. Is a patient/patient's guardian qualified enough to give consent and be aware about all the consequences that could accrue in future including security threats? For instance some patients consider their clinician's instructions as a part of their treatments and must be obeyed. Are ordinary patients usually familiar with how their information could be used in future? Despite his guardian's help, the patient may permit an action that may consequently lead to security threats. For example patients with a little knowledge about the abuse of clinical information will assume that to reject giving consent is safer. Who is responsible in case a patient died

as a result of rejected consent? Nevertheless a patient may find himself forced to give a consent that authorizes other agencies to gain access to his medical record in order to obtain a particular service: for instance [38] to claim for a reimbursement for the cost of a visit to the doctor in US. There are also many examples in the UK. For instance, from your insurance company, you need to complete a form that includes the following part:

> *I authorize any physician, hospital, or other medical related facility, insurance company, or other organization, institution or person, that has any record or knowledge of me or my dependents, or our health to disclose, when ever requested to do so by CAN or its representatives, any and all such information. A photocopy of this authorization shall be considered as effective and valid as the original.*

3.2. The Model's Principles

Nine principles were defined by Anderson [10, 11]. These are given below with comments on obvious difficulties in their implementation.

Principle 1: *Each identifiable clinical record shall be marked with an access control list naming the people or groups of people who may read it and append data to it. The system shall prevent anyone not on the access control list from accessing the record in any way.*

Principle 2: *A clinician may open a record with herself and the patient on the access control list. Where a patient has been referred, she may open a record with herself, the patient and the referring clinician(s) on the access control list.*

The clinician-may-open-record clause in principle 2 makes this principle difficult to be logically represented. It can be only understood as the

following: a clinician **must** open a new clinical record associated with a new access control list for a patient if the new information appears to be hidden from users who already have access to this patient's clinical record unless this principle is not needed to be formally implemented. There should be, at least a measurement/mechanism to find out whether a clinician was right by opening/not opening a new medical record for a patient according to her judgment about the security level of the new information.

Principle 3: *One of the clinicians on the access control list must be marked as being responsible. Only she may alter the access control list, and only she may add other health care professionals to it.*

Let us consider the case where the responsible clinician is the only authorized user to alter the access control list for a certain clinical record. For instance she forgets her password or deletes her record from the access control list, which means losing access to the access control list of that clinical record. Who is going to make the access control list available again? We may assume that a new access control list has to be created for that clinical record to replace the inaccessible one and/or that there will be another higher level of security such as system administrator. However this assumption is against the goal of principle 3, which is based on the responsible clinician being the highest security level for a certain clinical record unless the super authorization (e.g. system administrator) might be made as an exception comparable to the accident and emergency staff authorization. The second

part of the confusion concerns the technical experience of the position of the responsible clinician at network level. Is it operating system level, middleware level or application level? Definitely it is going to be impracticable for a clinician to manage control on all these levels, so her control will be at one level, which very likely will be at the application level. Logically the levels beneath compromise security mechanisms at any higher level. For instance the security mechanism from the application level can be bypassed, as the operation system is hosting the applications.

Principle 4: *The responsible clinician must notify the patient of the names on his record's access control list when it is opened, of all subsequent additions, and whenever responsibility is transferred. His consent must also be obtained, except in emergency or in the case of statutory exemptions.*

Principle 5: *No one shall have the ability to delete clinical information until the appropriate time period has expired.*

Principle 6: *All accesses to clinical records shall be marked on the record with the subject's name, as well as the date and time. An audit trail must also be kept of all deletions.*

Principle 7: *Information derived from record A may be appended to record B if and only if B's access control list is contained in A's.*

Principle 8: *There shall be effective measures to prevent the aggregation of personal health information. In particular, patients must receive special notification if any person whom it is proposed to add to their access control list already has access to personal health information on a large number of people.*

Principle 9: *Computer systems that handle personal health information shall have a subsystem that enforces the above principles in an effective way. Its effectiveness shall be subject to evaluation by independent experts.*

The apparent manual nature of principle 9 makes it unsuitable to be represented by the logical languages. For this reason we will assume that it has no part to play in the following sections.

3.3. Using security logical languages to represent Anderson's Principles:

Three languages are assessed in turn for their effectiveness in handling Anderson's principles: ASL, LaSCO and Ponder.

General Definitions:

Some important definitions need to be stated before we start using a logical language to represent a security policy:

Closed Policies (positive authorizations):

An access is granted if there is an authorization stating that the user can access the object.

Open policies (negative authorizations):

A user can access any object unless it has been explicitly denied.

An access control policy is a set of rules defining what is authorized.

An access control mechanism is a policy implementation to ensure that all accesses are in accordance with the underlying policy.

3.3.1 The Authorization Specification Language (ASL):

Definitions and an overview:

ASL [47] is a language for expressing the authorization according to access control policies. ASL supports a model based on two elements, an object (o) which could be a file or directory in a operating system or table in relational database, and an authorized entity who could be a user (U), group (G) or roles (R). An authorization policy in ASL is a mapping that maps 4-tuples (*o, u, R, a*) to the set {+, -}, where *o* is an object, *u* is a user, *R* is a role and *a* is an action (access rights such as read, write and append), while + means authorized and - means denied.

ASL Rules

An authorisation rule has two sides: the left hand side is the rule itself and the right hand side is a condition that controls the rule and is either another rule or binary predicate such as:

Active: binary predicate to capture the concept of active rule/s for users. It takes two arguments, the first is a user and the second is a role.

In and *dirin:* binary predicate to capture direct and indirect member relationship between subjects. They take two arguments, both are subject.

Typeof: binary predicate to capture the grouping relationship between objects. It takes two arguments the first is an object and the second is an object type.

ASL is designed principally to express the following rules:

Authorization Rules: used by the System Security Officer (SSO) to allow or deny accesses to objects explicitly in the following form:

$$cando(o, s, <sign>a) \leftarrow L1\& \ldots. \& Ln$$

This predicate symbol states that a subject *s* can (*Positive authorization sign* = "+") or cannot (*negative authorization sign* = "-") perform the action *a* on the object *o* under the conditions specified by *L1& ..&Ln*. *L1 ,..., Ln* could be one of the following literals: in, dirin or typeof. Principle 1 in the following section is an example of this rule.

Derivation Rules: used to derive implicit authorizations from explicit authorizations and determine the authorization policy. Indeed they are for expressing propagation of authorization along a subject's hierarchies. In addition derivation rules can express some kinds of implication relationships such as the derivation of an authorization in the base of the presence or the absence of other authorizations. The derivation rule has the following form:

$$dercando(o, s, <sign>a) \leftarrow L1\& \ldots. \& Ln$$

The right hand side of this rule derives a positive or negative authorization The outcome is determined by <*sign*> for a subject *s* to perform the action *a* on the object *o* according to another authorization in the right hand side (*L1& ...&Ln*). *L1 ,..., Ln* could be one of the following literals: cando, dercando, done, do, in, dirin or typeof.

Resolution Rules: used to regulate how to resolve any conflict that could accrue between authorizations are specified by the authorization rules *cando* and *dercando* as in the following form:

$$do(o, s, <sign>a) \leftarrow L1\& \ldots. \& Ln$$

This form states the enforcement of exercising (if *sign* = +) or forbidding (if *sign* = -) an access on an object by a subject *s* in the case of a conflict in the authorization rules (*cando* or *dercando*) in the right hand side.

Access Control Rules: to be used to regulate access control decisions on the basis of authorization specified by the authorization rules.

Access control rules have the following form:

$$grant(o, u, rs, <sign>a) \leftarrow L1\& \ldots. \&Ln$$

This form states that a request submitted by a user *u* with active roles *R* to perform the action *a* will be allowed (*sign* = +) or forbidden (*sign* = -) based on an authorization condition on the right hand side *L1*& …. *&Ln*. *L1*& …. *&Ln* are either cando, dercando, done, do, in, dirin, or typeof

Integrity Rules: used to express different kinds of constraints on the specifications and the use of authorizations. An integrity rule is of the form:

$$error() \leftarrow L1\& \ldots. \&Ln$$

where *L1*& …. *&Ln* are either cando, dercando, done, do, in, dirin, or typeof This rule derives an error every time the conditions in the right hand side of the rules are satisfied.

Using the authorization language (ASL) for specifying the clinical security principles:

Principle 1:

A subject *s* can read from and write on a clinical record *clincal_record* if and only if she is in the access control list *Clinical_Record_ACL* (here called a role) of that record.

The following is simply an authorization rule. The left hand side part (*cando(clincal_record, s, +read/write)*) is the authorization that is to be given and the right hand side part (*in(s, Clinical_Record_ACL)*) is specifying conditions that must be verified for the authorization to be granted.

cando(clincal_record, s, +read/write) ← *in(s, Clinical_Record_ACL)*

Principles 3 and 4:

The following code states that a subject *patient* must read his access control list *Clinical_Record_ACL* if it has been appended by a subject *clinician* who is authorized to do so

cando(Clinical_Record_ACL, clinician, +append) ← *do(Clinical_Record_ACL , patient, +read)*

cando (Clinical_Record_ACL , patient, +read) ← *done (Clinical_Record_ACL, clinician, append)* ← *cando (Clinical_Record_ACL, clinician, +append)*

Observations:

ASL is a language for expressing the authorization in matter of allowing or denying an access to an object. There is no way to express consequent actions that should be carried out after some authorized access such as auditing operations (e.g. principle 6). In addition it is not clear in this language how to express authorization restricted by the number of accesses as is needed for controlling the aggregate access problem (e.g. principle 8).

3.3.2 A Language for Security Constraints on Objects (LaSCO):

An overview:

LsSCO [46] is based on a model where a system consists of objects and events. The attributes on an event denote the specifics of the event's execution. Policies in LaSCO are stated as policy graphs which describe a specific state of the system (domain) and specific access constraints (requirements). Predicates are annotations near the nodes (objects) and the edges (events) to describe the domains (in the graph written as bold style text. For example **Type="user"** and **Method="access"** in Figure 3 are descriptions of domains. Requirements are written in the graph as normal style text, for example $UID ∈ ACL. LaSCO uses variables called *policy variables*. A policy variable represents a value of an attribute and relates attribute values associated with different objects and events. Variables may appear as operands in domains (e.g. in figure 1 **ID=$UID**) and in requirement predicates (e.g. in figure 1 $UID ∈ ACL). They are denoted by a "$" prefix.

Using LaSCO to describe the clinical security principles:

Principle 1:

The policy graph in figure 1 indicates that a user/subject needs to have his/her/it ID represented by the policy variable SUID included in the access control list of the clinical record in order to have an access to it, that is SUID ∈ ACL.

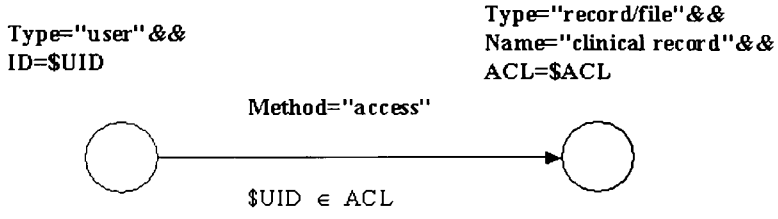

Figure 3: a security policy graph to represent principle 1 of the clinical security policy.

Principle 2:

If the user's security level/clearance, represented by the policy variable SUL, is not the same as the clinical record's security level, represented by another policy variable $FL, a clinician may create a new clinical record with the new access control list as shown in Figure 4. The requirement is that the security levels are different (SUL ≠ $FL).

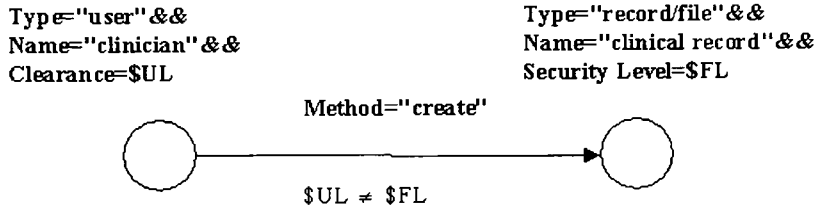

Figure 4: a security policy graph to represent principle 2 of the clinical security policy.

Principle 3:

The policy graph in Figure 5 states that a user, represented as an object, which is stated by a set of attributes *type* and *position* in addition to policy variable *$ID*, can only append the access control list for a clinical record if she is marked as responsible clinician. The event is represented in the policy graph as a method with value "append". The domain is represented as an object, which is stated by a set of attributes *type* and *name*. The requirement is that the ID of that user has to be the value of the attribute called *responsible_clinician*.

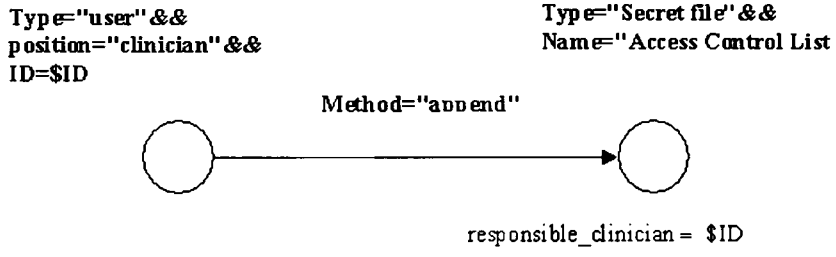

Figure 5: a security policy graph to represent principle 3 of the clinical security policy.

Principle 4:

Since principle 4 includes two events under different restrictions, we will divide it into two principles. Principle 4a considers the part that says the responsible clinician must notify the patient of all subsequent additions to the names on his record's access control list when it is opened. Principle 4b considers the part that says, whenever responsibility is transferred, the Patient's consent must also be obtained, except in emergency or in the case of statutory exemptions.

Principle 4a:

The policy graph in Figure 6 specifies the first part of principle 4 by restricting the method *add* to be executed after the method *message*. Both *add* and *message* are events and the restriction is ensured by a security requirement that enforces the order of these two events (*Time* > *$ST*). So adding a new user to the access control list will not be allowed until a message is sent to the patient containing the name of the user who it is proposed to add to the access control list of his clinical record.

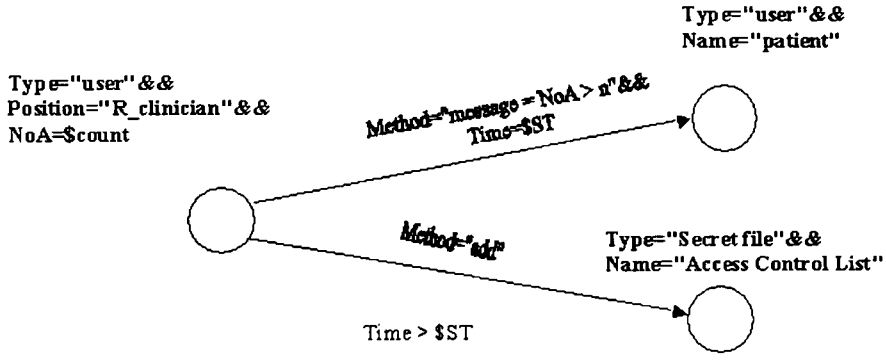

Figure 6: a security policy graph to represent the first part of principle 4 of the clinical security policy.

Principle 4b:

The policy graph in Figure 7 specifies the second part of principle 4 as following: the event *change responsibility* is restricted by either the case is an emergency or the other event *Name="Consent" && Permit=$PM* has been performed and the consent has been given, that is *SPM=true || Case="emergency"*.

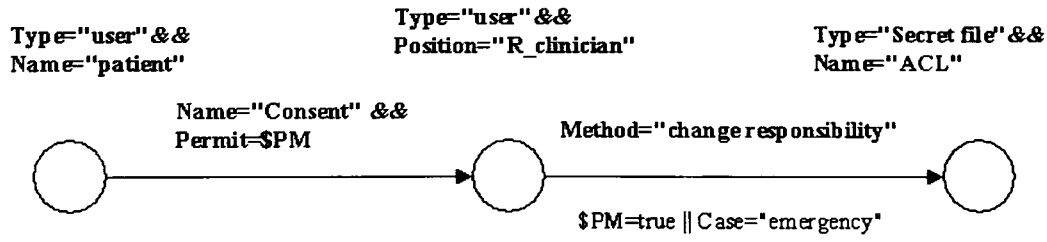

Figure 7: a security policy graph to represent the second part of principle 4 of the clinical security policy.

Principle 5:

The policy graph that is shown in Figure 8 states that event *delete* can he called by a *subject* to delete a *clinical record* object if and only if the system date *$sysdate,* a policy variable, is greater than or equal to the expiry date of that clinical record *$Edate,* another Policy variable.

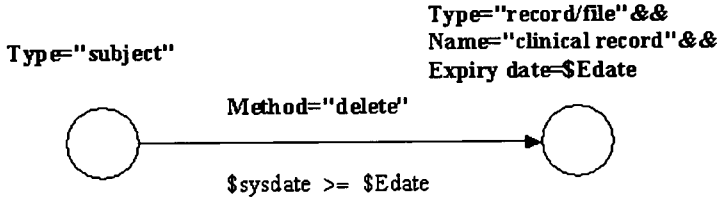

Figure 8: a security policy graph to represent principle 5 of the clinical security policy.

Principle 6:

The policy graph that is shown in Figure 9 specifies principle 6 by ensuring that a log record to be created contains a subject id ($SID), the access date and time ($DT), the access id ($ADID), and the accessed clinical record ($RID) for any access to the clinical record instance.

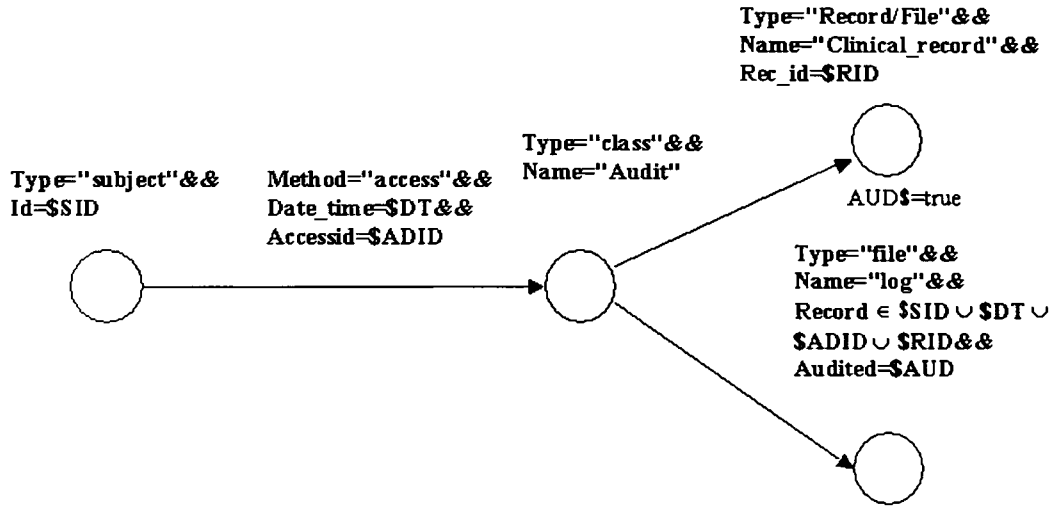

Figure 9: a security policy graph to represent principle 6 of the clinical security policy.

Principle 7:

The policy graph that is shown in Figure 10 represents the information flow control by ensuring that the access control list for the source record is a subset of the access control list of the destination record, that is $\$ACL\_B \in \$ACL\_A$.

Note that: this principle is also implicitly shown in the representation of principle 1.

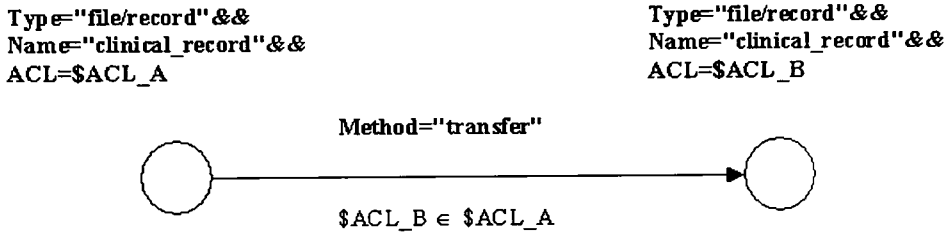

Figure 10: a security policy graph to represent principle 7 of the clinical security policy.

Principle 8:

The policy graph, shown in Figure 11, states that adding a new user to the access control list of a patient's medical record is not allowed before a message is sent to the patients. This message informs them that the user who it is proposed to add to their access control list already has access to personal health information on a large number of people such that $NoA > n$. NoA is the number of accesses for the proposed user and n is a constant.

Note that the order of the two events is enforced by ensuring that the time of the add method is greater than the time of message method, that is $Time > \$ST$.

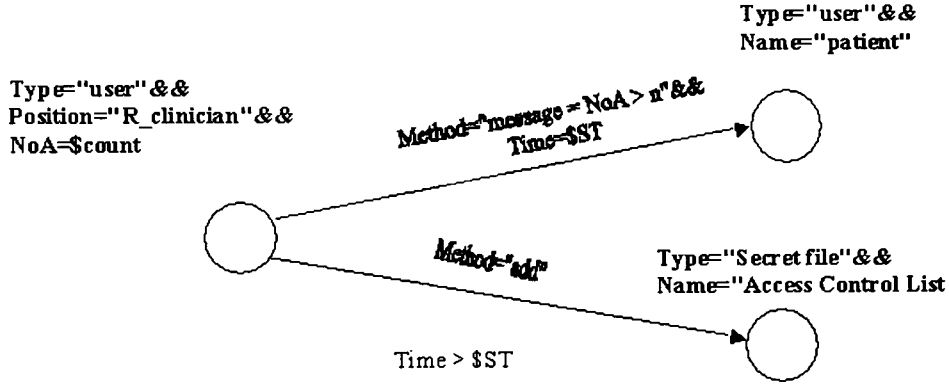

Figure 11: a security policy graph to represent principle 8 of the clinical security policy.

3.4. A Language for Specifying Security and Management Policies for distributed Systems (Ponder):

Definitions and an overview:

Ponder [28] is a declarative and object-oriented language that includes constructs for specifying the following basic policy types:

- Authorization policies specify what activities a subject is permitted or forbidden to do. In other words specifying either positive (**auth+**) and negative (**auth+**) authorization policies is possible. Principle 1 in the following section is represented as a positive authorization while principle 5 is an example of the negative authorization.
- Obligation policies specify what activities a subject must do. These policies are triggered by events and are usually interpreted by a manager agent. An example of this type is found in principle 2.
- Refrain policies define actions that subjects must refrain from performing.
- Delegation policies define what authorizations can be delegated and to whom.
- Composed policies are used to define a syntactic scope for specifying a set of related policies. There are four types of composed policies: groups, roles, relationships and structure management.

- Meta policies specify a permitted value for a valid policy.

The reader of this chapter will note in the following section that all Anderson's principles fall into two types of security policies, authorization policies and obligation policies, because these principles attempt to restrict the access control and/or enforce consequential actions such as the auditing process.

Using the Ponder language to describe the clinical security principles:
Principle 1:

A subject *s* of type *user* is authorized to read and/or append the clinical record *r* if and only if s is in the access control list of the clinical record *r.ACL* where *r.ACL* is the access control of the clinical record *r*.

Note that **type** is a type definition introducing a new user-defined policy type from which one or more policy instances of that type can be created, **auth+** is a reserved word indicating that the following is a positive authorization policy and *principle1* the name of the policy type. **subject**<user> s means that *s* is a subject of type *user*, **target** <clinicalRecord> r means that *r* is the **target** object of type *clinical Record* to be accessed by the subject *s*. **action** is a reserved word followed by the action, *read* and *append*, that is needed to be authorized. *belongs* is a user defined function to check whether the subject *s* is a member of the access control list of the record *r*. If so the positive authorisation will be allowed, that is **result** = enable;

```
type
    auth+ principle1 (subject <user>  s, target <clinicalRecord> r)
      {
        action read, append if belongs(s, r.ACL)
            {
               result = enable;
            }
       }
```

Principle 2:

In the case of new clinical information for a patient *NewInformation* appears to be in a different security level *isDifferentSecLevel*. From the existing access control list *currClinicalRecordAcl* a new access control list *newClinicalRecordAcl* has to be created

Note that ***on*** is a reserved word followed by the obligation condition, and *isDifferentSecLevel* is a user-defined function to compare the new information against the current security level and check whether it is a different security level. In this case the mandatory action has to be performed, that is do createNewACL(newClinicalRecordAcl)).

```
type
  oblig principle2 (subject <responsible_clinician> s,
                    target <ACL> currClinicalRecordAcl,
newClinicalRecordAcl,
                           <ClincalData> newInformation)
        {
         on isDifferentSecLevel (currClinicalRecordAcl, NewInformation);
         do createNewACL(newClinicalRecordAcl));
         }
```

Principle 3:

A subject *s* of type clinician is authorized to alter and/or append the access control list of a clinical record *clinicalRecordAcl* if and only if *s* is marked as a responsible user in the access control list.

```
type
    auth+ principle3 (subject <clinician>  s, target <ACL>
clinicalRecordAc)
        {
         action alter, append
         if position(s, clinicalRecordAcl) = "responsible"
                  {
                   result = enable;
                  }
        }
```

Principle 4:

This principle is divided into two parts. The first principle 4a concerns informing the patient about any new addition to his clinical record access control list via the responsible clinician. This part is represented as follows: in case of adding new record *addNew* to a patient's access control list of his clinical record *clinicalRecordAcl*, then that patient has to be informed through the action *informPatient*.

```
type
  oblig principle4a (subject <responsible_clinician> s,
                     target <ACL> clinicalRecordAcl, clinician newName)
        {
         on addNew (newName, clinicalRecordAcl);
         do informPatient (newName);
        }
```

The second part of this principle (principle 4b) deals with the case of changing the responsibilities in the access control list of the clinical records. This part is represented as follows: a subject *s* of type responsible clinician will be authorized to change the responsibilities in the access control list of a patient clinical record if and only if he has obtained that patient's consent.

```
type
  auth+ principle4b (subject <responsible_clinician> s, target <ACL>
clinicalRecordAcl)
        {
         action changeResponsibility  if PatientConsent (clinician,
newResponsibility)=true
                        {
                            result = enable;
                         }
        }
```

Principle 5:

A subject *s* cannot delete clinical record *r* until this record has expired, that is *todayDate() > expiryDate(r).*

Note that ***when*** is called the authorization filter and is used to restrict an action by a given condition.

```
type
    auth- principle5 (subject s, target<clinicalRecord> r)
          {
           action delete;
           when todayDate() > expiryDate(r);
          }
```

Principle 6:

An audit record contains the subject identifier *s*, date *aDate* and time *aTime* of action, type of action *aType*, and the record that has been accessed *r*. All accesses on the clinical record *r* by a subject *s* must be recorded.

```
type
   oblig principle4 (subject s, target <clinicalRecord> r)
      {
      on allAccess (s, aDate, aTime, aType, r);
      do createAuditRecord (s, aDate, aTime, aType);
       }
```

Principle 7:

Transferring data from clinical record *A* to clinical record *B* is not allowed unless all records in the access control list of b *clinicalRecordAcl_B* are included in the access control list of a *clinicalRecordAcl_A*.

```
type
    auth- principle7 (clinicalRecord A, <ACL> clinicalRecordAcl_A,
                    <ACL> clinicalRecordAcl_B, target<clinicalRecord> B)
                        {
                        action transfer(a.data, b.data);
                        when        List(clinicalRecordAcl_B)        in
                        List(clinicalRecordAcl_A)
                        }
```

Principle 8:

In the case of adding a new record which grants a new user access to a clinical record through a patient access control list, then the patient has to be informed of the number of records to which the new user has access.

```
type
  oblig principle8 (subject <responsible_clinician> s,
                    target <ACL> clinicalRecordAcl, clinician newName)
        {
          on addNew (newName, clinicalRecordAcl);
          do informPatient (newName, getNoAccess(newName));
        }
```

3.5. Results

The results are discussed in three ways. Firstly we compare the efficient uses of the formal approaches. Secondly we look at the coverage in Anderson's principles of multi-agency environment security. Finally we comment on the need-to-know problem.

3.5.1 Comparisons of formal approaches

Although all the above languages are basically targeting the specification of security policies, they focus on different aspects. For instance ASL focuses more on the access control policies and LaSCO attempts to express constraints on objects, while Ponder aims to specify security and management policies for distributed systems. Additionally they are different from the language's character point of view. Whereas ASL is based on logic and LaSCO policies are specified as logical expressions and as directed graphs, Ponder is a declarative language inheriting its syntax from the OCL "Object Constraint Language". According to the nature of each one of these languages we have found that some of Anderson's principles are not directly representable. For example principles such as those dealing with auditing operations (e.g. principle 6) and control aggregation problems (e.g. principle 8) were not representable at all by ASL and could be only indirectly expressed by LaSCO. On the other hand Ponder was more suitable for these kinds of principles since Ponder has got forms to deal with the management policies. Table 1 illustrates the comparison between these three languages according to their ability to express Anderson's clinical security principles.

Languages / Principles	ASL	LaSCO	Ponder
Principle 1	Explicitly represented	Explicitly represented	Explicitly represented
Principle 2	Not applicable	Indirectly represented	Indirectly represented
Principle 3	Indirectly represented	Explicitly represented	Explicitly represented
Principle 4	Indirectly represented	Indirectly represented	Explicitly represented
Principle 5	Not applicable	Explicitly represented	Explicitly represented
Principle 6	Not applicable	Indirectly represented	Explicitly represented
Principle 7	Not applicable	Explicitly represented	Explicitly represented
Principle 8	Not applicable	Indirectly represented	Explicitly represented
Principle 9	Not applicable	Not applicable	Not applicable

Table 1: Comparison of how far the ASL, LaSCO and Ponder languages can represent Anderson's principles.

3.5.2 Multi-agency services environment and collaboration issue

Only limited forms of cross-organizational access control were considered by Anderson[10, 11]. Such aspects include principle 4 that requires informing the patient about any addition to his record access control list and principle 6 concerning the auditing aspects. In general the issue of sharing clinical information including collaboration activities with other agencies such as police, social services or the education authority were not considered [62]. One possible reason could be that these principles were derived from a centralized system viewpoint at least from the responsibilities and ownership point of view.

3.5.3 Need-to-know problem

Need-to-know was not included in Anderson's principles, as the BMA does not accept that 'need-to-know' is an acceptable basis for access control decisions. Further details may be found in [10, 11]. However there might be a case where the need-to-know cannot be avoided. For instance a service provider such as social services offers its services conditioned by some information about the patient who applies for such services. There are two major problems in this case. Firstly who is authorized to decide about who needs to know in a multi-agency services environment where responsibilities are distributed. Secondly how can we resolve the conflict between the patient's consent and the need-to-know? Since there is no need-to-know without a purpose (task), we propose an approach based on associating the data with tasks and granting these tasks to performers rather than giving direct authorization to the secret data. The task could be in the form of an agreement between the information's owner and who needs to know (task's performer). This agreement would consist of full awareness about the task that requires the information, information size, release time, time of expiry and a guarantee to restrict the use of this information to the specified task. For a definition of "need-to-know" refer to Section 1.5.2

3.6. Concluding Discussion

Anderson in his security policy model [10, 11] argues that a security solution is an issue requiring great care to ensure that the security mechanisms work

together rather than operate independently. Although some professionals in health care information technology believe that any implementation of Anderson's principles would be expensive to implement and unmanageable to maintain, others such as Denley and Smith [30] according to their experience in the implementation of these principles in three British hospitals (Conquest Hospital, Aintree Hospital and Royal Devon and Exeter Hospital) state that Anderson's principles can be applied to the electronic patient record to maximise privacy. However, the CEN (Europe Committee for Standardization) group [83] observes that Anderson's principles are specified at too high a level for practical purposes and are not provable complete because they are neither precise nor exhaustive. Cohen [25] has proposed a formal model, complementary to Anderson's, which is again not accepted by the CEN group because it is not shown to be complete and because it is not based on basic security properties.

Our work contributes to the solution of the clinical information systems security problem by discussing Anderson's security principles for the clinical information systems, examining then logically and representing them using some selected languages for specifying security policies.

The ease with which the principles can be represented in a logical framework varies considerably. For example principles such as those dealing with auditing operations and control aggregation problems were not representable at all by ASL and could be only indirectly expressed by LaSCO. On the other hand Ponder was more suitable for these kinds of principles since Ponder has got forms to deal with the management policies.

Anderson's principles are mainly applicable to centralized systems. There were no precise principles in this model concerning either the multi-agency services environment or the need-to-know problem. The latter was not rated of high priority by the BMA. We consider that a task-based approach is promising in developing a need-to-know policy and on the next chapter introduce our task-based model. Other aspects of security in multi-agency services are still being investigated. CEN [83] also plan to broaden the model of security in healthcare to include all the potential needs of the different participants.

Chapter 4

DEVELOPMENT OF TASK-BASED SECURITY MODEL

4.1. Introduction

As introduced in section 1.2 basically security systems are built out of the available mechanisms to meet a security policy based on a selected security model [39]. Most of the security models that were designed subsequently were targeted at a specific security requirement. For instance multi-agency services and collaboration networks are based to some extent on these general models. However all these models are dealing with a single policy, whereas by definition the multi-agency and collaboration environment involves more than one policy.

A motivating example of an application that involves multi-agency services is the medical information services. The only model designed to meet the confidentiality requirements for the medical records in the UK was the BMA (British Medical Association) Security Policy Model [10, 11]. This model is examined in this thesis (see Chapter 3) [4, 5] against the multi-agency security requirements and it was found that the issue of sharing clinical information including collaboration activities with other agencies such as police, social services or the education authority was not considered for policy reasons. For

instance the *need-to-know* problem was not addressed in the BMA model (Chapter 3). However there might be a case where *need-to-know* cannot be avoided. For instance a service provider such as an insurance company offers its services conditioned by some information about the patient who applies for such services. An example is given in [38].

This Chapter covers a discussion for the proposed security model that we argue will alleviate the security difficulties that may arise in attempts to build a collaboration network. The model is constructed from a task-based perspective, as this approach seems to offer the best way forward (see Section 1.6). The general principles of the model are discussed and a diagrammatic representation is devised. Two task-based collaboration protocols, expressed in this chapter in the form of Petri Nets, represent the permitted states and transitions. An example of informal collaboration is used to illustrate the application of the model. Finally the model implementation is discussed.

4.1.1 A Task-based Perspective for Collaboration Networks

A collaboration business, by definition, is based on the needs of the collaborators from each other. Each side needs information or a service from the other participants. The obvious question that someone will immediately ask before he/she releases any confidential information or responds to an enquiry is: What for? For what purpose is the information required? Usually the expected answer will be the naming of a task for which the information required is essential, sometimes with a further explanation of the benefit of this task for the two sides (collaboration proposal). The information owner

may like to restrict the use of this information by some conditions (security policy). If they reach initial agreement a detailed negotiation will then take place until they reach a considered level of trust, which leads to a collaboration agreement to perform the task. One reasonable condition might be to limit the use of the information by other tasks. For instance it could be specified that the information should not be used outside the task for any purpose.

We have decided to build our model as a task-oriented model for the following reasons:

1. Fundamentally any collaboration scheme is based on specific tasks: there is no collaboration without a task.
2. The task-based approach is promising to address the need-to-know problem, satisfying a user requirement in any multi-agency services environment.
3. The collaboration task is the common object between the collaborators.
4. Shared information ownership can be granted to the collaboration task.
5. The task is scalable, flexible and dynamic.
6. Explicit responsibility is recognized in the task-based approach.

Overall the basis for any collaboration is an aim to share resources in order to achieve common benefits by performing shared operations. Other task-based approaches to security are discussed in Chapter 1.

4.2. General principles for our Model

4.2.1 Collaboration

In our model we consider any deal/trade between individuals or groups which aims to benefit the sides involved is a kind of collaboration. The following are some forms of collaboration:

- Trading between customers and service providers.
- Joint operation projects
- Research group collaboration.
- The clinician and the patient trade/relationship: the clinician's job exists because of the patient, and the patient needs the clinician for treatment. So both need each other and benefit each other. The clinician may need to know some information from the patient as part of the course of treatment. The relationship is in general based on trust. In this example there are two sides trading benefits through the task named treatment.

4.2.2 Ownership

Ownership is considered as a political issue and it is not only difficult to model but even more difficult to define who owns what. The following ownership aspects are to be understood well:

- Right to own: fundamentally according to the general principles of freedom and human rights such as the General Declaration of Human rights 1948 an individual or group reserve the right to own their properties including personal information.
- Ownership limitation: nevertheless an individual ownership is occasionally limited for the community/nation's benefit.
- Regulation effect: granting or limiting the ownership is based on regulation by the law.
- Ownership delegation: to meet the law and regulation requirements the ownership can be delegated but under explicit principles and for a specific purpose.

An item of information, in this model, is owned initially by its natural owner that is the person to whom the information relates. For instance information about the baby is owned by the baby although this information is controlled by guardian/parents. In computer security terms this is called *grant access* or *delegation.* Once this information is required to be shared among collaboration parties, an access will be granted to what we call the *collaboration-task* and will be controlled by the *task-policy.* The information owner and/or the access controller will be part of the negotiation that results in the task policy.

4.2.3 Authorization

There will be no absolute access by subjects on objects as in the traditional access control models. A subject to gain access to an object needs to participate in a collaboration task; hence we called it *task-participant. The task-participant* will be granted an access to object(s) for limited time to do specific job (called *task-activity*). The specification of the granted authorisation is explicitly declared in the *task-policy.*

4.2.4 Responsibilities

All responsibilities should be explicitly defined in the task policy in the way each individual *collaborator/task-participant* knows their responsibilities such as the required duties, the rules to follow (including ethical codes), the limitations (e.g. time, use of material and information) and the penalties.

4.3. Collaboration task characteristics

The following properties are required for a collaboration task:

- Unique: it is identified by the following components and change in any of them results in a new task:
    - Task Purpose/requirements: the task should aim to achieve explicit requirements and for a specific purpose.
    - Task Policy: is a set of enforceable rules that regulates task participants' duty (who is going to do what, when and for how long). A task policy can be inherited from other policies.

- Task participants: could be physical entities such as people and computer programs/processes or logical such as roles. Although the collaborators are usually task participants, there could be others who will participate in the runtime.
- Flexible: can be a single activity or group of activities sharing same policy, covering same requirements and carried out by same task participants system.
- Dynamic: can be updated even while it is running (supporting post-hoc justification). For instance a nurse can be replaced by another one if he/she is not, for any reason, able to complete his/her duty in a surgical operation. However any change in the task elements should be fully and carefully documented. To secure accountability.
- Secure: should be appropriately protected using all the available mechanisms.
- Scalable: can be upgraded, for instance to fill some gaps in the original task. A new collaboration task can be built starting from default tasks (task template).
- Accountable: all collaboration protocol states and all task run-time events of the collaboration must be well documented.

4.4. Diagrammatic Representation of Model

The architecture in Figure 12 illustrates the general components of our model. The main component is the collaborators (two or more), each of which will need to define three elements: requirements (what does he/she/it/they aim to gain from the other side), policy (rules that need to be obeyed) and material (e.g. information to release or services to offer). The second component is a pair of task-based collaboration protocols -- the Collaboration Task Creation Protocol (CTCP) and the Collaboration Task Runtime Protocol (CTRP), both detailed later in the following sections.

CTCP includes a negotiation between all collaborators where the proposed task will be discussed including all collaborators' policies and requirements. This process (negotiation) continues until a decision is taken either by rejecting the proposal or by accepting it. The acceptance of a proposal will lead to a formal agreement/contract, which will produce the proposed collaboration task in its final stage including all of the policies and requirements.

The task policy will move from a high level through the negotiation, decision and agreements stages to a low level at the task creation stage. Classifying security policy as high level and low level policies are discussed with examples in [59].

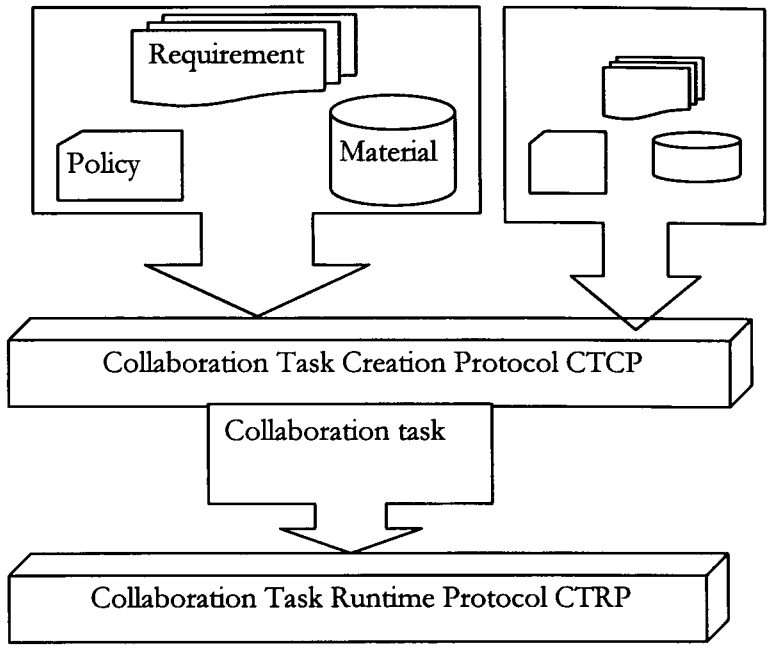

Figure 12: general architecture for secure collaboration environment

CTRP will start after a successful compilation of CTCP and as scheduled .in the *task_policy* (not necessarily immediately after the end of CTCP).

The main function of CTRP is to process the task that was previously created by the CTCP protocol and ensure that the *task_policy* is obeyed, the collaborators are aware of the circumstances and the right action is taken. CTRP is detailed in the following sections. In a special case of the abnormal termination of the task process the collaborators may need to go back to the CTCP protocol to create an alternative task. It should be noted that the *task_participants* (collaborators) are not necessarily the same subjects who were participants in the CTCP. However such differences should be included in the *task_policy*. The case of an emergency update for the participants list during

the CTRP will be covered by the CTRP process documentation (the CTRP log).

There is another way to view the CTCP/CTRP relationship. CTRP is very variable and its form is not predictable. It depends on what policy was agreed. CTCP can be regarded as the intension of the policy and CTRP as the extension. There is the normal intension-extension relationship, that is an instance in the extension must be consistent with the definition of the intension, here the security policies agreed. This is procedural transparency in contrast to the situation if one protocol were used.

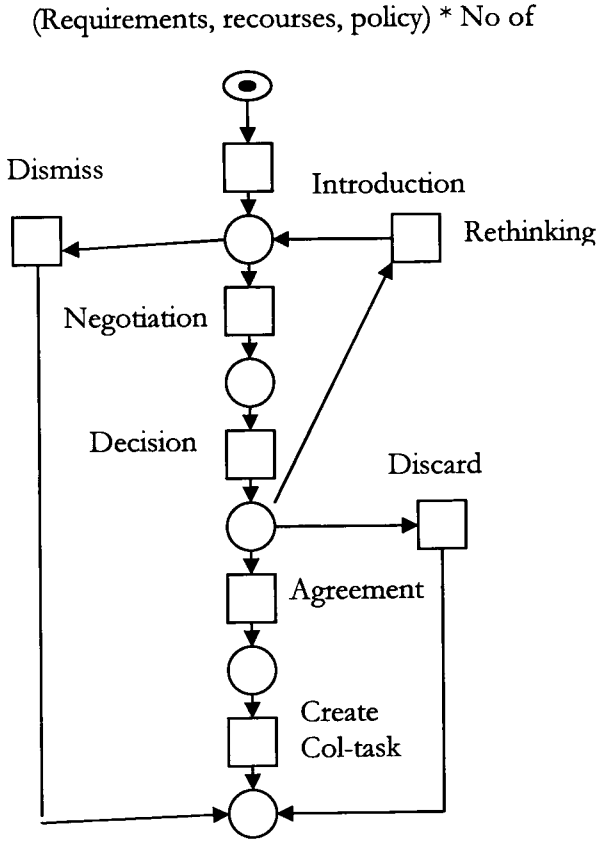

Figure 13: Petri Nets Graph representing the Collaboration Task Creation Protocol (CTCP)

4.5. Notations for Protocols

4.5.1 Selection of Formal Approach

There are a number of notations available for representing our model such as flow charts; state charts; state machine; data flow diagrams; entity life-histories; Petri nets; process algebra; process calculus and pi calculus.

The notations need to represent the events and processes. The actual choice is not critical for this work as the main thrust of verifying the model is to be the case studies and the validation against the regulations. Formal semantic verification is much more difficult as it requires detailed knowledge of the applications and a substantial amount of formal analysis outside the scope of this thesis.

We choose Petri nets for their suitability here as they provide 1) a diagrammatic representation; 2) facilities for syntactic verification; 3) methods for functional decomposition by nesting one net within another; 4) state-transition capture; 5) concurrency control; 6) constructively, we know how a Petri net will behave given particular inputs.

Not all these features have been used immediately but it is clearly advantageous to use a technique, which can be readily extended to capture more meaning rather than discard the results and recommence with a different notation. It is beyond the scope of this thesis to give a thorough comparison of the above notations. Nor is it claimed that the Petri net approach is the only valid option.

Petri net theory was originally introduced in a PhD thesis of C. A. Petri and Reisig [65] introduced it to the software engineering area in 1985. More recent advances in this formalism are described in [66]. The usefulness of Petri nets in providing a theoretical basis for handling object life cycles has been demonstrated by Van Der Aalst and Basten [87]. The Petri net in Figure 13 represents the CTCP protocol. The Petri nets shown in this thesis have been verified syntactically by the PEP[2] tools.

4.5.2 Petri Net Notations

A Petri net, usually represented as a graph, contains four elements: transitions, places, arcs, and tokens. A transition is drawn as a bar or a box. A place, drawn as a circle, contains zero or more tokens. A token is a black dot represents argument or return value. An arc, drawn as a directed line, represents an input-output relation between a place and a transition (see Figure 14).

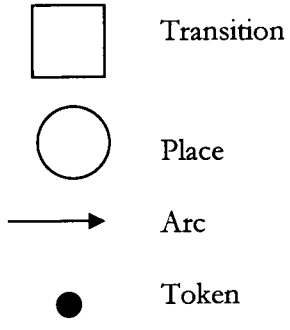

Figure 14: Petri Net Notations

[2] PEP is a Programming Environment based on Petri Nets

The initial state represents the aim of each collaborator including requirements, policies and offers. For instance, in the patient-doctor collaboration, the patient's requirements are treatments, the patient's policy is to keep personal information secret, the doctor's requirements may include information about the patient and the doctor's offer is a treatment course. These aspects will be initially discussed as to whether the task (at first an offer from one side or a requirement from another) is accepted as an offer or rejected without any further details. The *introduction* transition will not include discussion about the policies. If the proposed task is found to be reasonable then all collaborators will enter into a detailed *negotiation* in which all aspects including requirements, services and policies will be clarified for all collaborators. After that one of three decisions will be taken: the first option could be that one of the collaborators needs more time to think about the task/offer; the second option could be that the expected level of trust could not be ensured so the task is simply dismissed; the third option is that all collaborators trust each others so that an agreement between all collaborators will take place. This agreement at the end will be formulated in what we call the collaboration task. This task will be limited in scope by the *task policy*, which is a composition of all collaborators' policies, meeting all sides' requirements.

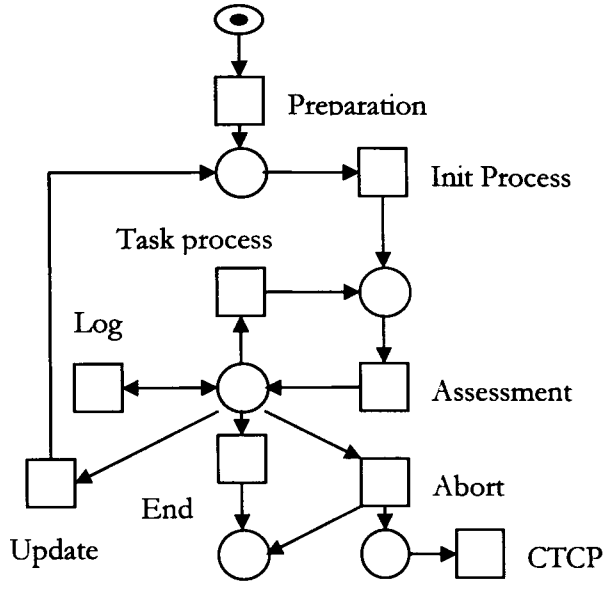

Figure 15: Petri Nets Graph representing the Collaboration Task Run-time Protocol (CTRP)

The Task Runtime protocol (CTRP), illustrated in Figure 15, starts after the task has been completely created by the CTCP protocol and when its schedule time, according to the *task-policy*, is due. Before starting the process of the task some tasks need some preparations. Then the task process starts following the policy that has been approved in the CTCP stage. Each state of this process is monitored, assessed (verified against the *task-policy*) and then documented. The task assessment may result in one of the following:

1. The task is proceeding satisfactorily, following the policy and the plan and has not finished yet, so the task should persist.

2. The task needs an update to meet its requirements. Depending on how the updates affect the process: the task may restart or continue from the last state of the process.
3. The task reaches its scheduled end, hence the task terminates normally.
4. There might be a case where the task abnormally terminates, for instance the *task-policy* has been violated, or the task exceeds the scheduled time without valid reasons. The abnormal termination could lead either to the end of the task and then of the collaboration or to a new session of the CTCP.

4.5.3 Using Security Languages to review the CTCP/CTRP model

In Chapter 3 we attempted to use security languages to represent the BMA principles. It is clearly important to also review the CTCP/CTRP model in terms of these security languages. Here we will demonstrate how these kinds of languages are applicable in our model. As these languages are only usable when there is an explicit security policy available, they cannot represent the open-ended nature of the CTCP/CTRP model. The security languages do not cover *negotiation, decision* and *agreement.* After the *agreement* stage in the CTCP protocol they could be used, particularly in the task creation stage. Hence the task policy or part of it could be written in one of the security languages such as Ponder, LaSCO or ASL. However fundamentally as the authorisation policy is task-based, none of these languages is suitable for representing the authorisation in a task policy as they are all subject-object based. In our model

there is no absolute access to the object by the subjects either authorised or authorised.

However, in the CTRP protocol particularly in the *task assessment,* PONDER in particular can be used to enforce the task policy. The following example uses the obligation policy in PONDER to enforce a task police for a task activity

```
oblig activity01Policy (subject s,
                        target anObject)
    {
      on policyViolation;
      do TaskAbort);
    }
```

4.6. Example of Informal Collaboration

Let us consider a situation of a son asking his father for some cash:

4.6.1 The Collaboration Task Creation protocol (CTCP)

Introduction:

Son: father, I need 20 pounds [35].

Father: what for?

Son: to buy a book. [Purpose]

Father: well I do not have enough cash and I cannot drive to the ATM at the moment. [Initial discussion]

Son: Would you please lend me any of your cards (Debit or Credit) with the PIN, so I can go myself? [Proposed task]

Negotiation:

Father: well, you understand that you will not use this card for any other purpose, you will not withdraw more than 20 pounds, and you will not give away the card or its PIN to anybody else [7].

Son: Yes, I do understand that [accepting policy].

Decision:

Father based on his experience with his son will go for one of the following three options:

1. Take more time to think about the matter and to ask more questions. [Back to negotiation],
2. Cannot trust his son, so he cannot give him his card. [Dismiss the task], or
3. Trust his son and give him the card [commit the task].

Agreement:

- Father: I agree to give you my card along with the PIN but you should remember that:
    i. You return the card to me within 20 minutes of obtaining the money.

ii. You will not withdraw more than 20 pounds and you will not use the card for any other purpose.

iii. You will use the money to buy a book.

iv. You should not give the card nor disclose the PIN to anybody else.

v. This agreement is based on trust between us.

- Son: Yes, I do understand all these conditions.

Rejection:

Father: I will go myself later to obtain for you the money that you want.

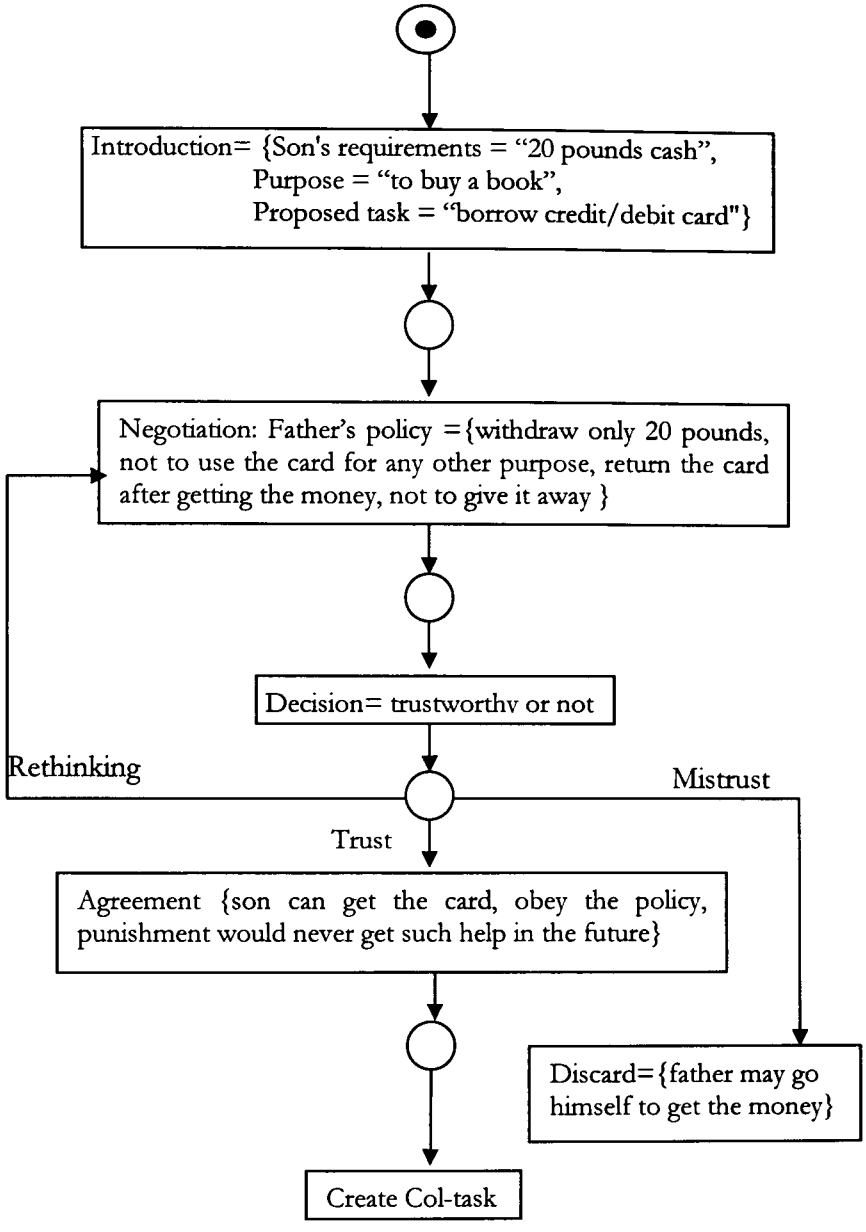

Figure 16: Petri Net representing the CTCP of the given example

4.6.2 The Collaboration Task Runtime Protocol (CTRP).

Preparation:

Farther: Explains to his son how to use the card and gives it to him.

Task process:

Son takes the card and starts using it.

Task assessment:

Father watches the time, maybe checks his account with another card if it takes more time than expected and takes decisions accordingly. Meanwhile he updates his relationship of trust with his son in the light of this experience.

4.6.3 Example modelling:

In this example we have two collaborators (*task-participant1*=son and *task-paticipant2*=father), *task_name* = borrow credit/debit card, *purpose* = withdraw 20 pounds to buy a book, *policy* = {withdraw only 20 pounds, not to use the card for any other purpose, return the card after getting the money, and not to give it away}, and *security-base* = {trust based on experience}. A Petri Net graph in Figure 16 represents this example in the CTCP layer/stage and Figure 17 represents it in the CTRP protocol.

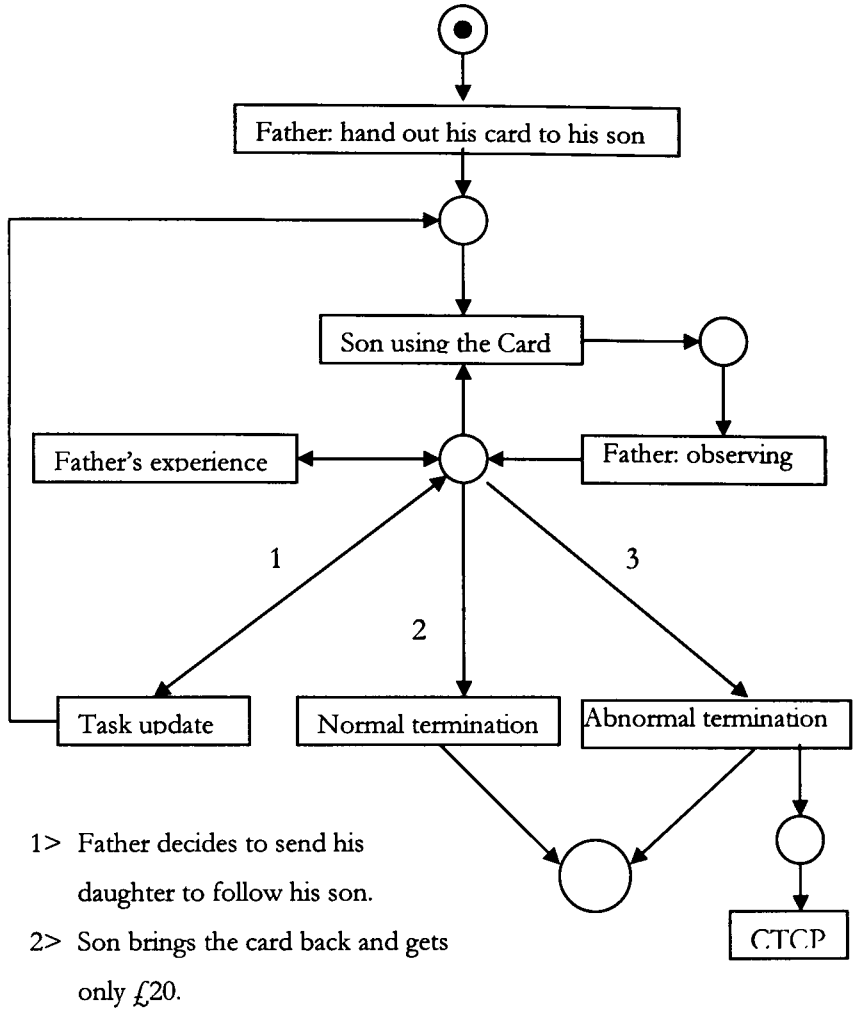

Figure 17: Petri Net representing the CTRP of the given Example

4.7. Exception and error handling

As it is almost impossible to design a 100% secure and dependable system and as there will always be exceptions and errors, systems need to handle exceptions and errors as they arise to meet most possible dependability situation (including security requirements).

Logically we cannot wipe out the errors and the exceptions because we are always going forward but we can remove the result of that error, in other words no backward recovery for security (e.g. unauthorised access to secret recourses). Backup and recovery usually helps availability and integrity but not confidentiality. As the time will never go back, handling errors and exceptions in our model is based on insertion of a new activity/process. A task is a set of activities, so if any exception is raised in an activity, another activity will be inserted after this activity to handle the exception.

In the CTCP/CTRP model exception and error will be treated as any other violation for the task policy, hence exception and error handling are built in.

The CTCP/CTRP model, particularly the CTRP protocol, complies with the Protect-Monitor-Response approach [76] where the task assessed against *task_policy* responds to any policy violating security deliberately (task participant misuse, an external attack) or accidentally (errors and exceptions). The task activities are protected by the *task_policy* (established in CTCP protocol and encapsulated with the task) and monitored by the task assessment component in the CTRP. In case of any error, exception or policy violation the response will be one of the following:

- Update the task and resume.
- Update the task and restart.
- Terminate the task and go back to the CTCP protocol to negotiate a new task where the experience gained (task process log) will be used

to create a new task and resolve problems raised in the process of before. See Figure 18.

- Terminate the task and stop.

Collaborators in the CTCP/CTRP model learn from their mistakes to create more dependable tasks.

4.7.1 Exception/error handling scenario

To demonstrate the exception handling in our CTCP/CTRP model we will consider simple scenarios (more challenging ones are found in the case study in Chapter 6):

- Signing an official letter/memorandum can be an activity in many tasks (let us assume it is an urgent letter/memorandum). The authorised person(s) may not be available at the time. This exception can be handled as following:

    1. If the system policy contains a principle to regulate an acting authorisation and indeed the acting authorised person(s) is/are available. This scenario is covered in the CTCP protocol where principles such as assigning acting authorisation are included in the *task_policy*. In the CTRP protocol in case of such an exception the task will be automatically updated to authorise the acting authorised person to sign the letter/memorandum and resume the process of the task.

2. If neither the authorised person(s) nor the acting authorised is/are available, the system policy may include principle to state a higher authorisation to overwrite, in emergency, any authorisation. As this is a major change in the authorisation policy, so the task will need to restart from the beginning to ensure constancy. though this case is manageable in the CTRP protocol.
3. However there could be situations where none of the above is granted. In such situations an initiative action by one of the responsible people (*task_participants* in CTRP) is required to resolve the situation. This attempt however must properly be recorded and audited. Such action results in a new authorisation, which was not in the pre-defined policy. This means the task fails to work with the agreed policy, which means a new task is required to handle this situation. However the new task will use the record (task process's log) of the original task to meet the original requirements and to avoid repetition.

4.7.2 Authorization Scenario:

The commandos team X3076, which is lead by General X has been commanded to carry out an intelligent operation somewhere abroad. To communicate with the headquarter General X is equipped with a laptop

computer including sophisticated software and encryption tools. Just after the operation started, General X is shot dead. Security policy of the operation advises that Major Y may act as leader in the absent of General X. Major Y turns the laptop on and attempts to login as a leader. The server rejects his login as for the system General X is still in charge. This is in fact an exception raised by the system. An action is urgently needed to handle this exception.

The problem in the view of the CTCP/CTRP model:

Using the Collaboration Task Creation Protocol, the National Intelligence Headquarter (NIH) has a number of tasks created to perform a number of operations as required. The above is just one example.

Collaborators: (The Prime Minster, the Minster of Defence, Agents, Officers ... etc) will participate in the creation of the task and its policy (Rules of engagement).

Task design: from the introduction through the negotiation to the agreement and final creation of the task (compiling the result of the above processes).

Task Creation: All the task activities are set up, all the task participants (General X, Major Y, etc) are named and associated with their roles. The participant in this task will not necessarily will be the same people involved in the creation of the task (e.g. the Prime Minster will have no roll here).

Running the Task:

After the task has been created and the time for running that task is due, the Collaboration Task Runtime Protocol (CTRP) starts. In the middle of the task process, while the task assessment component was verifying an activity supposed to be done by General X, the ID and the password were not General X's. This for the system is a policy violation, despite the fact that General X is dead and Major Y is the acting leader. Such an exception can be handled through the update component as follows:

Major Y logs on as normal user and sends a message to Headquarter. The message may include a video showing General X has died as evidence.

The Headquarters send a message to General Y and ask for a quick response

If there is no response from X the Headquarters will insert a new activity to update the task, so Major X is authorised as team leader.

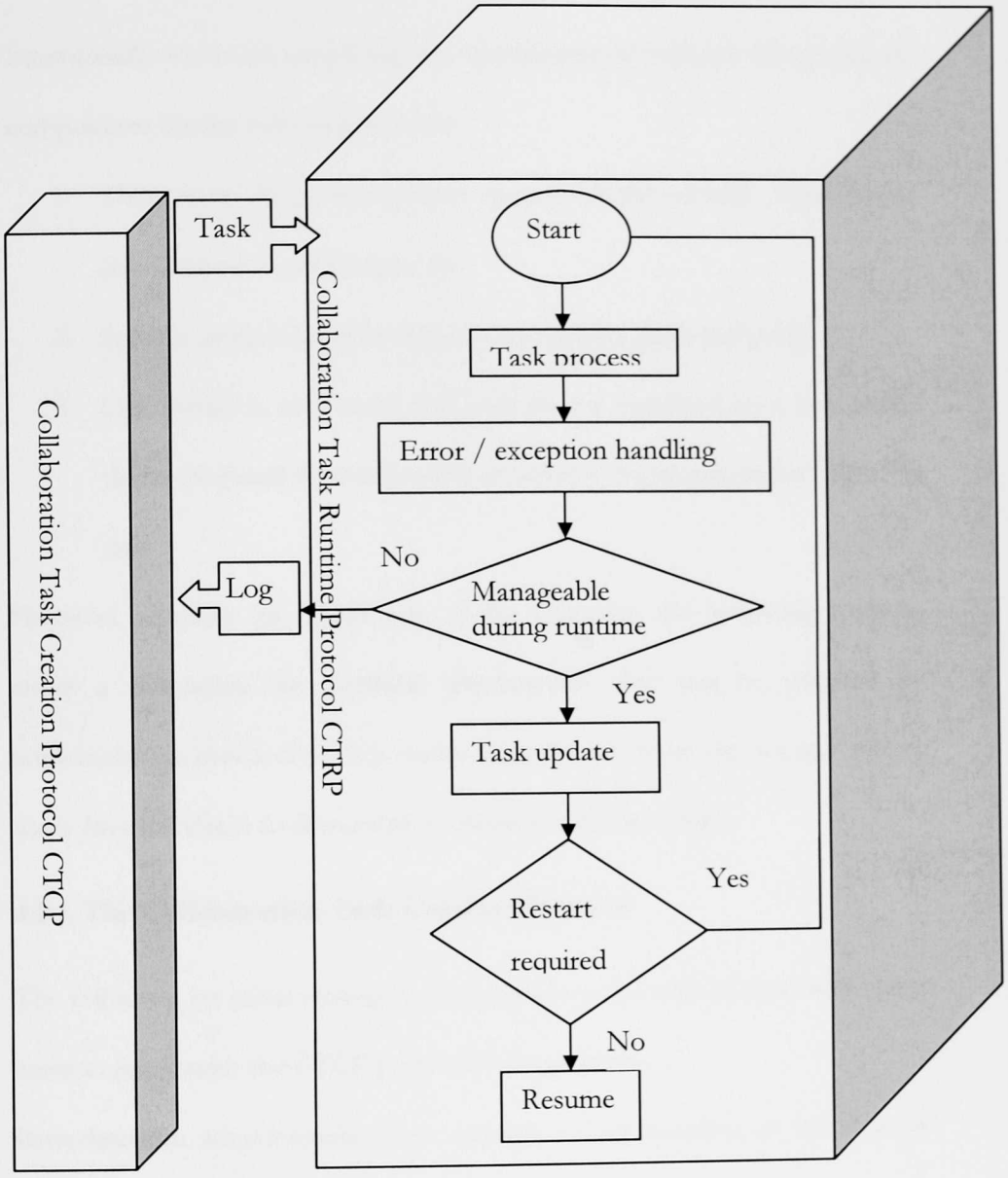

Figure 18: Exception handling cycle

4.8. Implementation guide lines

Intentionally we avoid proposing any mechanisms to enforce the protocols' components for the following reasons:

1. There is no single mechanism to meet all the security requirements (see Chapter 1 and Chapter 2).
2. Security implementation depends on security goals and policy.
3. Our model is task based and each task is regulated by a task policy that is prepared especially to meet security requirements for a specific task.

However to show the practicality of the approach the following sections cover a discussion for available mechanisms that can be adopted to implement the protocol's components in given scenarios, also we give below some Java interfaces to demonstrate simulation of the model.

4.8.1 The Collaboration Task Creation Protocol

The following are some examples of mechanisms that can be used with some cases to implement the CTCP protocols' components.

Introduction: advertisement is an example of mechanisms, in the case of service-provider-customer scenario. In the case of a doctor-patient scenario a visit to the clinic is a mechanism example.

For simulation purpose, the following is a Java interface for the *Introduction* component.

```
public interface Introduction
{
  public boolean collaboratorRegistration (Collaborator newCollaborator,
                        Policy policyList, Requirement  requirementsList)
                        throws IOException;
  public boolean collaboratorWithdraw  (Collaborator collaboratorToDelete)
                        throws CollaborationDeletionException;
  public boolean lookup (String CollaboratorName)
                        throws InvalidNameException;
  public void policyUpdate (Collaborator collaborator, Policy newPolicyList)
                        throws IOException;
  public void requirementsUpdate (Collaborator collaborator,
                        Requirement  newRequirementsList)
                        throws IOException;
  public boolean considerTheProposal () throws notEnoughInformation;
  public Boolean getLog () throws IOException; // used in the case that the
                                                task is based on a previously run task
}
```

Negotiation: there are many formal models and techniques offering different ways to address the negotiation problem. For instance there are a number of Artificial Intelligence models that can be deployed for aspects such as conflict resolution [23, 94]. Work in process by a team in OASIS (Organization for the Advancement of Structured Information Standards) aims to specify asimple process by which collaboration protocol agreements can be negotiated between patties [44]. Tools such as E-meeting (e.g. net-meeting), discussion groups (e.g. news groups) and email services can be used to put collaborators together.

For simulation purpose, the following is a Java interface for the *negotiation* component.

```
public interface Negotiation
{
  public TaskInstruction  negotiation ()  throws NegotiationException;
  public void addTaskParticipant (TaskParticipant newParticipant)
                                  throws InvalidParticipantException;
  public void policyUpdate (Collaborator collaborator, Policy newPolicyList)
                                  throws IOException;
  public void requirementsUpdate (Collaborator collaborator,
                                  Requirement  newRequirementsList)
                                  throws IOException;
}
```

Decision: often the negotiation models and protocols include a decision method. There is much software developed to support decision making. ERGO [14] is one example. It is a decision support system designed by Arlington Software Corporation to help users organize their decision criteria and their related priorities.

The following is the proposed Java interface for the *decision* component for simulation purpose:

```
public interface Decision
{
  public boolean decision (TaskInstruction initTask)  throws
DecisionException;
}
```

Agreement: is the final form of the task design stages (introduction to agreement).

Agreement is usually considered by the negotiation models and protocols, hence they usually offer methods and techniques to support it. There are a number of protocols that aim to meet some agreement between collaborators. An example is found in Collaboration Protocol Profile and Agreement (CPPA)[61].

In the case that the task is a computer program the result could be a program specification and compilation script.

The following is the Java interface for this component.

```
public interface Agreement
{
  public agreementScript agreement (TaskInstruction initTask)  throws
AgreementException;
}
```

Task creation: depends on the language used. For programming languages, it is the program compiling and linking.

The created task could be formed in a list of instruction along with another list of regulation (task policy) for each individual task participant by their task activities.

For different tasks different languages can be used. For instance we have introduced (see Chapter 3) three security policy languages (ASL, LaSCO and Ponder) and we have seen each of these targeting different security properties. For example if the task security policy is to deal with authorization and access control, any one of these three languages (perhaps, these issues were more clear in ASL) will be suitable but if the policy includes constraints LaSCO will be preferable, while Ponder deals better with policies, which include aggregation control.

The following is the Java interface for the task creation component, the last one in the CTCP protocol:

```
public interface TaskCreation
{
  public Task taskGeneration (TaskInstruction initTask, makeFile makeFile)
                                    throws GenerationException;
}
```

4.8.2 The Collaboration Task Runtime Protocol (CTRP)

Task process and assessment could be as simple as comparing one action against one straight forward security principle (e.g. Boolean operation). On the other hand it could be very complicated for instance including sophisticated algorithms and techniques to capture human behaviour. However in all cases the result must be the same.

Using Ponder to implement the task assessment:

In Chapter 3, we have used three security policy languages to represent the BMA model's principles, subsequently in Section 4.5.3 in this chapter we have seen that it is possible to use these languages particularly to represent the task polices. For example the obligation policy in ponder can be used to implement the process assessment.

```
type
  oblig processAssessment (subject <taskParticipant> s,
       target <taskResource> processResource)
       {
         on errorOrException ();
         do
            {
             createLog ();
             exceptionHandling ();
             }
       }
```

4.9. Conclusions

This chapter has introduced a task-based model to facilitate collaboration in trusted multi-agency networks, after a wide investigation of the existing security models dealing with the multi-agency environment and collaboration networks. Our model is based on the fundamental aspect of the collaboration environment, which has a task-based perspective. Two task-based collaboration protocols (CTCP and CTRP), expressed in the form of Petri

Nets, are used to represent the permitted states and transitions. Also security policy languages such as Ponder can be used to represent the task-policy. The model's capability of errors and exceptions handling is demonstrated and supported by examples. An example of informal collaboration is used to illustrate the application of the model. We have also discussed the extent to which task-based approaches have been used before in security systems. In addition to its coverage of the area of computability, our model suitably covers the usability requirements. Finally a number of mechanisms are suggested as implementation methods for the different components of the model's protocols.

Chapter 5

REVIEW OF MODEL AGAINST REQUIREMENTS

Satisfaction of Health Record Security Principles through Collaborative Protocols

5.1. Introduction

The CTCP/CTRP model developed in Chapter 4 and so far tested with one informal example. In this chapter after a brief discussion for the security requirements, the model is reviewed by showing how it handles the principles of two British approaches (DPA and Caldicott). These two regulations are carefully selected to cover both general regulations (DPA) and more specific health informatics regulations (Caldicott principles and recommendations). Finally the effectiveness of the CTCP/CTRP model in software engineering terms is reviewed. It is shown that the model exhibits maximal cohesion, loose coupling and an economical rule-based performance

5.2. Security requirements for the health care information systems

5.2.1 Rhetoric

We could summarize our scope of health care security requirements in two general, equally rated, goals: 1) a good quality of health provision (not only for a certain patient but for all society e.g. medical research requirements) and 2) full respect for the patient rights. Actually, the main security requirements are implicitly included in these two goals. For instance availability and integrity are included in the first goal while confidentiality is included in the second goal. It is understood that the first goal (good quality of health provision) is easier to achieve than the second one (the patient's right). In other words the main concern is now given to the second goal. In this work we will try to alleviate those difficulties that could prevent the health providers from achieving this important goal.

5.2.2 Confidentiality in heath care services: (patient's right requirements)

With respect to the patient's rights, recent legalisations and publication in the field support five important aspects:

1. Patient oriented approach: an item of information about a patient should be owned by the patient described by the information.

2. Privacy: patient privacy should be maintained to a high standard as a result of fair and lawful use of the patient's confidential information.
3. Transparency: the patient should be made aware of all the use made of his information.
4. Public interest: the need of the community may override the need of individuals in some exceptional cases.
5. Legal requirements: a trial case may require disclosure of a patient's confidential information. However this should be very restricted and limited by the case after detailed explanations of why the information disclosure is essential.

It is important here to mention some mechanisms that have been introduced to deal with these requirements so far, summarized as follow:

- Patient consents:
    i. Expressed consent to ensure the patient's ownership.
    ii. Informed consent to ensure transparency.
    iii. Implied consent to deal with emergencies or protect the patient's health when expressed consent may be difficult to achieve.
- Anonymisation/Pseudoanonymisation: to resolve the conflict between public interest and patient's right

5.2.3 Concept

There are a number of official statements and principles from which security requirements for health information systems can be derived. All of these principles aim to protect the patient's sensitive information, particularly person-identifiable information based on the patient's rights. However it has been understood that some of these principles result in much debate and conflict [8, 32]. As a result an implementation of this requirement is a difficult task. We will look at two accepted approaches: the Data Protection Act and the Caldicott Principles and Recommendations. These two approaches are both relevant to security in health care services. The Data Protection Act is the general law of Britain for controlling the use of personal data and the Caldicott Principles are an attempt to develop a specific means of controlling access to personal information in health services in the context of general British law and the culture of the health services. Both of the documents underpinning the approaches give lists of principles.

5.3. Data Protection Act

The Data Protection Act (DPA) [41, 69] is an implementation of the EC Directive 95/46/EC, which aims to protect the processing of personal information by 'data controllers'.

The DPA has been summarised into eight principles, which are discussed in the following paragraph with an attempt to examine how far these principles can be reflected in our CTCP/CTRP model:

5.3.1 Principle 1:

Personal data shall be processed fairly and lawfully, and, in particular, shall not be processed unless (a) at least one of the conditions in Schedule 2 is met, and (b) in the case of sensitive personal data at least one of the conditions in Schedule 3 is also met.

In our model sensitive data including personal data will be processed through a pre-defined task. This task is defined and created as a result of a collaboration protocol which in one of its steps involves negotiation between all parties, such as data subject (patient in EHR), service providers (who needs the information e.g. clinician, social worker), referee (optional, e.g. data controller) and legal agent. Table 2 shows how the conditions in *Schedule 2* of this principle will be meet by our model.

Condition	How to be meet in our model
Patient consent	Since the patient or his/her guardian is part of the negotiation, which has created the collaboration task, so he or she has got the right to allow or dismiss this task.
Legal obligation	A legal agent could join the negotiation about the task and should enforce any obligation and clarify the reason behind this obligation to get the support of other parties.
Vital Interests	As in the legal obligation it should be clear that the need of the collaboration task is a matter of life and death
Public functions	Same as in the legal obligation

Table 2 DPA principle 1's conditions against TCP/CTRP components.

5.3.2 Principle 2:

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

By restricting the use of data by a specific task so that it can be used only for one purpose, so we can ensure that the data will not be used for more than one purpose.

5.3.3 Principle 3:

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

The collaboration task will not be created unless the data subject and the referee (if any) make sure that this task will definitely need the required data.

5.3.4 Principle 4:

Personal data shall be accurate and, where necessary, kept up to date.

Since the data subject himself is involved in the team that creates the collaboration task, so the personal data can easily be verified and updated.

5.3.5 Principle 5:

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

In the CTCP protocol the start and the end date and time of a task should be explicitly specified and included in the task-policy. The CTRP protocol will ensure that all the task's activities will be processed within the specified time.

5.3.6 Principle 6:

Personal data shall be processed in accordance with the rights of data subjects under this Act.

In our model we consider a data subject (patient in EHR) to act as the only owner for his/her personal information and he/she will never lose his ownership.

5.3.7 Principle 7:

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

The task should be protected by law and by the available security mechanisms. In the CTCP firstly, at the *introduction* level there should be a proposal for the protection mechanisms/measures (including technical and legal aspects such as cryptography applications and prosecution) that can be used to protect a specific task that is going to use the patient information. If for any reason this proposal does not meet the security requirements then the task should be dismissed. At the *negotiation* level such mechanisms will be verified and tested and the task discarded if these mechanisms fail the test. All these mechanisms, after it has been found that they can do the job, will be encapsulated in the created task. The functionality of these mechanisms will be later described in the CTRP protocol while the task in process.

5.3.8 Principle 8:

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Data transfer task is a collaboration task that can be created using the CTCP/CTRP model. Data transfer will be allowed only among the collaborators who agreed in the CTCP protocol to adhere to each other's policies, which can include the protection for the rights and freedoms of data subjects in relation to the processing of personal data. The personal data will not only be protected against transfer abroad, it will also not be possible to transfer the data outside the task.

5.4. Caldicott Principles and Recommendations

In 1997-98 a committee chaired by Professor Caldicott at Cambridge developed security principles for the medical area [20]. The principles developed are an expansion and refinement of those found in the Data Protection Act. The emphasis is on control over the use of patient-identifiable information and the restriction of access to those who need to know information for particular purposes.

5.4.1 Principle 1

Justify the purpose(s)

Every proposed use or transfer of person-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an appropriate guardian.

This principle is right at the heart of our CTCP/CTRP model. In the CTCP protocol only one task will be created for each purpose. Later the extent to

which the task adheres to the original purpose will be fairly tested and verified through the CTRP protocol.

5.4.2 Principle 2

- Don't use person-identifiable information unless it is absolutely necessary

Person-identifiable information items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

This principle can be easily achieved at the early stages in the CTCP protocol (*introduction*), where a good reason must be given to create a task. If for any reason the task does not need to use personal information, this task will simply be discarded either at the introduction or the negotiation stage.

5.4.3 Principle 3

- Use the minimum necessary person-identifiable information

Where use of person-identifiable information is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out.

It is quite similar to the above principle (no. 2). In addition if it is found, in the process of the CTRP protocol (task assessment stage), that the task is using unnecessary information then the CTRP will be either aborted or updated.

5.4.4 Principle 4

- Access to person-identifiable information should be on a strict need-to-know basis

Only those individuals who need access to person-identifiable information should have access to it, and they should only have access to the information items that they need to see. This may mean introducing access controls or splitting information flows where one information flow is used for several purposes.

In our model the use of any material (person-identifiable information in this case) will be only through the task-participants. They are the only people authorised to use the information necessary to perform the defined task. The task will be for only one purpose. Our model deals with both aspects of need-to-know. Need-to-know defined in Section 1.5.2. In the CTCP protocol a collaborator can claim access to information/services, which is subject to a negotiation. In the CTRP protocol need-to-know is the basis of the access control by limiting access by the purpose of the task.

5.4.5 Principle 5

- Everyone with access to person-identifiable information should be aware of their responsibilities

Action should be taken to ensure that those handling person-identifiable information - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect confidentiality.

One of the main principles of our model is to clearly define the responsibility of all the task-participants before creating a task.

Responsibility is declared at the negotiation stage in the CTCP protocol and evaluated at the task process assessment at the CTRP protocol.

5.4.6 Principle 6

- Understand and comply with the law

Every use of person-identifiable information must be lawful. Someone in each organisation handling confidential information should be responsible for ensuring that the organisation complies with legal requirements.

This *someone* could participate at the agreement stage in the CTCP to prove or deny the tasks in which the use of the person-identifiable information appeared to be illegal. In addition at the stage of task process assessment in the CTRP this *someone* could monitor the task run and terminate it or update it if it is found to not comply with the task policy (either automatically or manually).

5.5. Coverage of Data Protection Act and Caldicott Principles

The correspondence between the DPA and Caldicott principles is shown in Table 3.

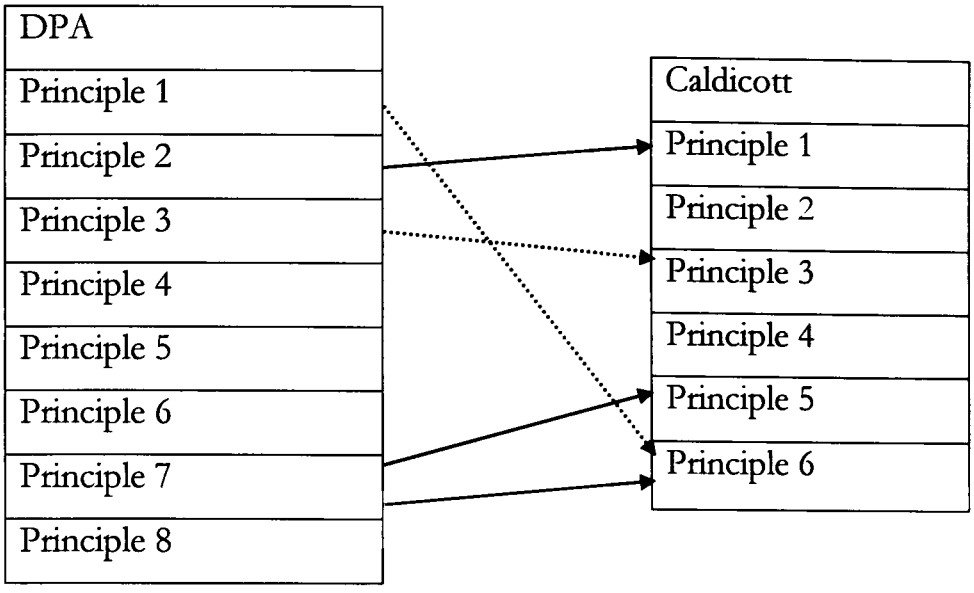

Table 3 Correspondence of DPA and Caldicott Principles

Not all the DPA principles, for instance 4,5,6 and 8, are covered by Caldicott. Principle 4, accuracy and timeliness of data, is assumed in medical data. Principle 5, length of time data is kept, does not apply to medical data as normally such data is kept while the patient is alive and longer if it can be used for tracing medical history for the community or a family. Principle 6, rights of data subjects, is within the context of the DPA only. Principle 8, transfer of personal data abroad, is not covered by Caldicott because the data is considered to be anonymous anyway. Overall, the main concern in Caldicott is with protecting the assignment of data to specific persons. The BMA model [10, 11] corresponds more closely to DPA than Caldicott.

From the other perspective, the Caldicott principles 2 and 4 are not reflected in the DPA. Both these are task based illustrating the need-to-

know approach in Caldicott in contrast to the patient consent approach of DPA and BMA.

The thick lines connecting one principle to another indicate an explicit correspondence such as the justification for obtaining personal data in principle 2 of the DPA and principle 1 of Caldicott. The thin lines indicate an implicit correspondence such as fair and lawful use of data in principle 1 of DPA and principle 6 of Caldicott requiring an understanding and compliance with the law by the people using the data.

5.6. Review of Satisfaction of Principles by CTCP/CTRP Model

To conclude a review is made to show the extent to which the CTCP/CTRP model covers the principles of DPA and Caldicott. The purpose of this review is to show succinctly firstly whether each principle is covered and secondly the extent to which the requirements of software engineering [79] are met by the CTCP/CTRP constructions. Ideally there should be a tick at least once for each principle for coverage, a clearly-defined single functionality for each protocol for maximal cohesion, an encapsulation of the protocols for loose coupling and an efficient execution of the protocols for low energy performance.

Table 4 shows the correspondence between DPA principles and CTCP/CTRP, using the abbreviation shown in Table 5 components. The ticks are shown only when the principle is explicitly covered by the

component at the intension level. Ticks are not shown where the activity might arise for a particular case or instance at the extension level but such activity is not compulsory at the rule-based or intension level. For instance agreement (Agr) is implicit in most components but is explicit in number 8 where personal data is transferred to another country. The decision protocol (Dec) is also implicit in many components but is explicit only in principle 2 where it is required that the data will be used only for a specific task. The component for preparation (Pre) is implicitly involved in CTRP but is not explicitly highlighted in the table as we deal with general principles. Similarly the component update (Upd) in CTRP is also a very general principle dependent only on a case and used in emergency. The component for creating the CTRP protocol (Cre) appears to be excessively employed. However it is a task performing a critical linking task between CTCP and CTRP.

Principle	CTCP					CTRP						
	Int	Neg	Dec	Agr	Cre	Pre	Pro	Ass	Log	Upd	Dis	End
1	✔	✔										
2			✔	✔	✔			✔	✔			
3					✔							
4					✔							
5					✔							
6					✔			✔	✔		✔	
7					✔			✔	✔			
8	✔	✔		✔	✔			✔	✔			

Table 4: Correspondence of DPA Principles and CTCP/CTRP Components

Collaboration Task Creation Protocol	Collaboration Task Runtime Protocol
Int for Introduction	Pre: Preparation
Neg for Negotiation	Pro: Task Processing
Dec for Decision	Ass: Task process assessment
Agr for Agreement	Log: Process log
Cre for Create collaboration task	Upd: Task update
	Dis: Task process discard
	End: Task termination.

Table 5: Abbreviations for protocols components

Table 6 shows the correspondence between Caldicott principles and CTCP/CTRP components. The pattern is different from that for the DPA as Caldicott is in general more task-based meaning that there is much more

explicit mention in the principles of the components we have created in CTCP/CTRP. For instance in Caldicott, principle 1 (justify the purpose) requires explicitly all the components of CTCP/CTRP. Principle 4 (need-to-know restriction on person-identifiable data) is tackled on a task-based approach using agreement (Agr), creation of CTRP (Cre) and process logging (Log). The DPA is task-based in principle 2 (data for specified and lawful purpose) corresponding to principle 1 in Caldicott as in Table 3 above. The pattern is similar in Table 4 and Table 6 for these principles except that the Caldicott principle is wider in scope and involves more activity.

Principle	CTCP					CTRP						
	Int	Neg	Dec	Agr	Cre	Pre	Pro	Ass	Log	Upd	Dis	End
1	✔	✔	✔	✔	✔			✔	✔		✔	
2	✔											
3	✔	✔			✔			✔	✔		✔	
4				✔	✔			✔	✔			
5				✔	✔			✔	✔			
6				✔	✔			✔	✔			

Table 6: Correspondence of Caldicott Principles and CTCP/CTRP Components.

Table 4 and Table 6 show that all the principles of DPA and Caldicott are covered by CTCP/CTRP. Every principle is cross-checked positively with one or more components in the model. CTCP and CTRP also exhibit maximal cohesion as the activities performed by these protocols are clearly differentiated. Thus CTCP creates the task including negotiation and

agreement and CTRP runs the task assisted against the agreed policy. There is loose coupling between CTCP and CTRP. CTRP is encapsulated: it can only be called after CTCP has successfully concluded. CTRP can be aborted resulting in a new CTCP session being started but this is simply a normal return mechanism. The high-level rule-based nature of CTCP/CTRP ensures an economical performance. Thus the model meets the software engineering requirements given earlier.

5.7. Conclusion

The CTCP/CTRP model appears to meet the general requirements of security for health informatics as outlined by Caldicott and the DPA. In terms of coverage a match is made with both the more specific task-based approach of Caldicott and the more general DPA. An analysis of the usage of the components of CTCP/CTRP against the principles of Caldicott and DPA shows that, while coverage is achieved in both cases, a more natural match is made with Caldicott than with DPA because Caldicott is at a more specific level in dealing with the patient record than DPA. The software engineering principles of maximal cohesion, low coupling and efficient execution are met by CTCP/CTRP. From a computing science perspective, CTCP/CTRP appears to be an appropriate way forward for handling security principles as developed in Caldicott and DPA. The next stage is to develop a case study using real case requirements in health care to test the whole approach.

Chapter 6

CASE STUDY

6.1. Introduction

In **Chapter 5** we have demonstrated a validation for our model against general security requirements (security regulations). Two security regulations were used: the Data Protection Act (DPA) and the Caldicott principles. These were carefully chosen to cover examples of top-level security regulation and medical related regulation respectively. The validation shows that the model is capable of meeting this level of requirements. However to build a solid ground for the idea of the model and its two protocols we thought a real world case study was essential. The case study attempts to validate the model against a real-world scenario, where exceptions may arise, and to show to what extent these exceptions can be handled.

It was not an easy task to find a suitable case study. Firstly we had to identify a challenging multi-agency services application. Two multi-agency applications were considered, the Electronic Health Record (EHR) and the Dynamic Coalition Environment (DCE). These two applications involve information

sharing among parties, who differ in polices, functions and interest and currently both are very active research areas. Secondly and more challenging, we had to look for a real world scenario among the selected applications (EHR and DCE) to cover all the parts of the model. For a DCE case study we constructed a scenario after a literature review for selected DCE projects. For the EHR case study we took advantage from being involved in collaboration with a number of projects at University of Newcastle, among them one run by the Sowerby Centre for Health Informatics at Newcastle (SCHIN)*. SCHIN is involved in the Durham and Darlington electronic health record project, for which we were provided with a scenario argued to be the ideal situation for handling an emergency case.

The following sections firstly discuss the environment of each case study followed by a mapping of the scenario events with the CTCP and CTRP protocols' components.

We attempt in the work discussed in this chapter to show how the multi-agency real world situations can naturally be reflected in our model. This chapter will cover the two case studies. The first will be an example reflecting a dynamic coalition situation and the second will be in the Electronic Health Record (EHR), an emergency scenario from County Durham and Darlington EHR project.

* Sowerby Centre for Health Informatics at Newcastle (SCHIN) is a research centre whose aim is to cover all areas of health informatics. The centre was founded in January 1993 and is academically based in the School of Health Sciences at Newcastle University, UK.

6.2. Dynamic Coalition Environment

Dynamic Coalition Environment (DCE) is a special case of the multi-agency environment and collaboration networks. As the Coalition forms quickly and dynamically the following problems will be more challenging than in the other collaboration networks [64]:

- Sharing information involves security risk.
- Partners in one crisis are adversaries in others.
- In addition to security and sharing information the Dynamic Coalitions problem include issues such as interoperability, extensibility and scalability.

A dynamic collation is formed in response to events such as humanitarian relief (e.g. refugee camps), natural disaster (e.g. earthquake and floods), international incidents (e.g. terrorist), war (Gulf war and Yugoslavia) and combat other than war (e.g. Bosnia).

A dynamic coalition may involve:

1. Civilian organisations such as agencies, embassies, bureaus, (government organisations), Local Fire and Police Departments, Doctors without Borders, Federal Emergency Management Agency, Press Crops and Red Cross (none-government organisations).
2. Military organizations such as Army, Navy, Air Force, Marines and Coast Guard.

6.2.1 Other Approaches:

The Dynamic Coalition problem is considered an active research area and there are a number of projects world-wide dealing with it. The following are selected approaches:

- A paper by Phillips, Ting and Demurjian [64] attempts to define the Dynamic Coalition and explores the challenging issue of sharing information in such situations. The authors of this paper draw attention to the lack of management in the current control systems using the Global Command and Control System (GCCS) as an example. GCCS is an U.S system on its own private network which needs to address several security issues to be acceptable for the Dynamic Coalition environment. In this paper they argue that the RBAC could be an approach to tackle the access control problem in these situations and DAC and MAC are both applicable. Aspects such as syntax, semantics, and pragmatics are considered as a core part of the problem.

  Advantages and disadvantages of DAC, MAC and RBAC are discussed in Chapter 1.

- Yalta [19] is one of a number of projects funded by DARPA to address the Dynamic Coalition problems. Yalta argued that the provision of secure collaboration space for dynamic coalition is based on four ideas:

1. Create a secure collaboration space from shared space developed in distributed computing community.
2. Build a Certificate Authority Service based on threshold cryptography.
3. Implement a Certificate Revocation Notification (CRN)
4. Support use of the collaboration space as a coordination channel.

The Yalta project aims to provide an infrastructure for sharing information among collaborators.

- The Distributed Role-Based Access Control dRBAC [36] is an access control mechanism for systems that involve multi-administrative domains. Briefly it is a combination of role-based access control and trusted management systems, using cryptographic applications such as: public-key and cryptographic signature.

6.2.2 Dynamic Coalition in the view of the CTCP/CTRP model

From a task-based perspective we define the Dynamic Coalition as a task to be carried out by a number of organisations with the aim of responding to certain events. A number of more specialised sub-tasks are inherited from the top-level task. Security policy of the inherited sub-tasks will include the parent security policy.

Table 7 and Table 8 illustrate a summary of CTCP protocols inputs for a simple coalition scenario. Table 7 summarise the inputs of top-level task and Table 8 summarises a sub-task input. There are two collaborators (Coalition Partners), partner_A is an organisation administrating the humanitarian relief in a refugee camp and partner_B is an organisation helping with food and medicines supply.

Coalition Task to provide Humanitarian relief in a refugee camp		
Top-level task		
	Partner_A	Partner_B
Requirements	Supply of food and medicines.	Information about the refugees (including medical data)
Resources	Information	Equipments, drugs and food.
Policies	Confidentiality and privacy	Availability and accuracy of information.

Table 7 summary of CTCP protocols inputs for simple coalition scenario (top level task)

1. Creating coalition tasks with the CTCP protocol
    a. Introduction:
        i. Partner_A: seeks partner_B's help to supply food and medicines (mechanism used: e.g. email).
        ii. If Partner_B replies negatively go to the end of CTCP, else go to the negotiation stage.

b. Negotiation:

i. Partner_B: insists that they may need information about the refugees.

ii. Partner_A: the information is confidential and the privacy of the refugees is highly respected, for instance complying with human right declaration such as Universal Declaration of Human Rights and general data protection rules such as Data Protection Act (see Chapter 2).

c. Decision: if Partners accept each other's policies and requirements go to the agreement stage else end the CTCP.

d. Agreement: the refugees' information will be used for the purpose of supplying food and medicines and to grant the information based on the requirements for each subtask and should not be available outside of any subtask. This task is a general task and no information will be granted to its participants.

e. Task creation: it depends on the way the task is going to be run. However as this task is a general one it appears as a container for its subtasks.

2. Running the created tasks with CTRP

The run of this task will be achieved by running all the subtasks.

Subtask to supply children food		
	Partner_A	Partner_B
Requirements	Supply and distribute children foods	Access to the refugee records
Resources	Information	Children foods
Policies	Access only children data; minimize the use of personnel identifiable data; use only the information related to the supply and distribution of children foods	none

Table 8: Summary of CTCP protocols inputs for simple coalition scenario (sub task)

1. Creating a subtask (supply children food):
    a. Introduction:
        i. Partner_A: orders children food from Partner_B.
        ii. Partner_B: needs to have access to the camp's database
        iii. Both agree and go to negotiation.
    b. Negotiation:

i. Partner_B: details the required activities:

1. Count the number of children grouped by their ages.
2. List the families and the number of children in each family.
3. Count the number of children with special needs.
4. Distribute foods.

ii. Partner_A: agrees as long as the required queries will not disclose confidential information such as personal identifiable information.

iii. Partner_A: requires the names or roles of those who will do the work.

iv. Partner_B gives the names and/or roles

c. Decision:

i. Both accept each other's policies

d. Agreement:

i. Partner_A: agrees to grant access to the subtask.

e. Task Creation:

Assuming that Partner_A is using a relational database the subtask in this case will be encapsulated in the form of an SQL procedure or package which grants Partner_B's defined users an access to it.

The manual activities, those not to be automated, will be placed formally in an order familiar to those in the work-place.

6.3. DCE case study evolution

Case study feature	CTCP/CTRP feature	Exceptions handling
Advertising food and medicine supply.	CTCP.Introduction	
Access grant	CTCP.Negotiation and CTCP.Decision	
Information use and product supply.	CTCP.agreement.	
Information use and product supply details and control.	CTCP.Taskcreation.	

Table 9: summary of the mapping between the DCE scenario (task one) and the components of the CTCP/CTRP protocols.

Case study feature	CTCP/CTRP feature	Exceptions handling
Order children food and medicine.	CTCP.Introduction	
Access control.	CTCP.Negotiation and CTCP.Decision	
Details of how to access the information.	CTCP.Agreement and CTCP.Taskcreation	
Using the information.	CTRP.Process and CTRP.Assessment	
Food and medicine supply.	CTRP.Process and CTRP.Assessment	

Table 10: summary of the mapping between the DCE scenario (task two) and the components of the CTCP/CTRP protocols.

The scenario here is very small; hence all the case study features were fully represented both in task number 1 in Table 9 and task number 2 in Table 10. In task number 1 not all the model features were used as it is a top-level task and its run is achieved by executing all its subtasks. As a result there were no uses for the CTRP protocol's components.

In task number 2 more model components were used, although components such as CTRP.update and CTRP.abort still have not been used as we have not assumed any exception in this example

6.4. County Durham and Darlington EHR Project

6.4.1 Preview

A Durham and Darlington electronic health record (now known as the Integrated Health Care Recorders) has been funded by the NHS information authority as a part of electronically record development and implementation programme.

As a part of this work a multi-media animator [27] has been developed. This animator is based on a real world scenario. The purpose of the animator is to raise issues and promote discussion about what electronic health care records could look like, and how they could be used. This version of the animator is being evaluated within the project focus groups involving the healthcare professional.

The idea of electronic health records was introduced by the government in the document *Information for Health* in 1998. It outlines the intentions to invest in technology, and bring the NHS to the 21st century. One of the targets is to introduce electronic health care records by 2005.

"*An Electro Health Records is used to describe the concept of a longitudinal record of patient's health and healthcare from cradle to grave*"

(EHR) has been described as a cradle to grave record, which would provide a framework for NHS professionals in different parts of the house service to act together to deliver better quality and better coordinated care

A particular focus of the Durham and Darlington electronic health records project has been to understand the potential problems as well as the benefits of an electronic health record system. This includes a technical requirements as well as the potential impact on current work practices.

For example there are many issues surrounding sharing of confidential information across barriers of NHS healthcare organisations. This presentation is based on an emergency case scenario. It is intended to provoke debate and raise discussion to help in a development of an EHR which can successfully meet our needs.

In the space of a few years, Durham, Darlington, and Tees have become single strategic health authority and 10 primary care trusts are in full operation. There are three care trusts supported by ambulance trusts and mental health trust teams operating within the community. Patients have begun to understand the idea of managed care pathways and to expect different parts of the health service to coordinate their activities and the care that they deliver. It is important to note that the text of this case study is a transcript from a multimedia animator; accordingly the language is informal to some extent.

6.4.2 The story (an emergency incident Scenario)

The story of the EHR scenario concerns Mr Jones a 58-year old ex-miner who was diagnosed as a non-insurance dependent diabetic in 1996. Mr Jones has been experiencing chest pains and has been diagnosed as suffering from coronary heart disease. He has been introduced to the coronary heart disease

national service informed by his GP and as we can see he has an electronic health record.

We begin our story at the point where Mr Jones experiences a severe chest pain after going to bed. He calls NHS Direct.

NHS Direct: NHS Direct, I am Kathleen, how can I help you?

Mr Jones: I have got a terrible pain in my chest

NHS Direct: Can you tell me your name please?

Mr Jones: My name is Edward Jones

NHS Direct: and where are you Mr Jones?

Mr Jones: I'm at home

NHS Direct: can you tell me your address?

Mr Jones: 23 High Streets in Esinglee.

NHS Direct: 23 High Street in Esinglee, is that right?

Mr Jones: That is right.

NHS Direct: Have you called us before Mr Jones?

Mr Jones: No, this is the first time, this pain is appallingly bad.

NHS Direct: Could you describe it to me Mr Jones?

Mr Jones: It is like my chest is in a vice, like a big weight on me.

NHS Direct: Have you had the pain very long?

Mr Jones: About 20 minutes, but it was not quite as bad at first.

NHS Direct: I think I need to call an ambulance Mr Jones, and get you in a hospital right away. Is there any one with you?

Mr Jones: No, I'm on my own.

NHS Direct: OK, Mr Jones, I have called out an ambulance for you, and I can see that you have got an electronic health record.

At this point we will look in detail at how the NHS Direct patient-adviser accesses Mr Jones' electronic health record from within the NHS Direct Clinical assessment system.

When the patient-adviser selects the EHR button the card system send the basic information about Mr Jones to the EHR.

The EHR responds quickly with a list of three close matches -- all named Jones and two of them named Edward. The patient-adviser selects the first patient in the list as it matches Mr Jones' address and confirms the date of birth with him to ensure the correct record is selected. She is now presented with an emergency record for Mr Jones from the EHR. This contains clinical information such as current medical problems and medication he is taking. It also contains information about Mr Jones' domestic circumstances that the ambulance staff can use to ensure that the emergency is handled quickly and efficiently.

NHS Direct:: OK Mr Jones I have sent some details to the ambulance men and notified the hospital. They will be expecting you.

Mr Jones: Oh, thank you.

NHS Direct: Have you tried to use an aspirin?

Mr Jones: That was the first thing, I did but it does not seem be working this time.

NHS Direct: I can see from your record that your neighbour at number 25 has a key to your house; will they be in?

Mr Jones: Oh yes, Edith, she is always in at this time. Will it be long?

NHS Direct: They should be with you shortly. I'm looking at the screen and they're only a few minutes away. Shall I tell your daughter Janice that you have been taken to the hospital?

Mr Jones: Oh, I don't want to get her all worried about me.

NHS Direct: Oh, don't worry Mr Jones we are really careful about this sort of thing. But someone needs to know that you have been taken to hospital especially as you are living on your own.

Mr Jones: Oh, right, then she is a good lass, but she does worry...Oh the ambulance has maybe arrived.

NHS Direct: I hope you get well soon Mr Jones I will call off now.

The information sent to the ambulance is quite specific. It includes demographics, the fact that Mr Jones is a diabetic and his current medication. It also contains the message, that Mr Jones' neighbour at number 25 has a key to his house.

Any interventions in an ambulance such as giving aspirin and taking blood pressure and NCG are all recorded on board the ambulance using supplied equipment. When the ambulance arrives at accident and emergency, this information together with the confirmation of the patient identity is transmitted automatically to the hospital system. The ambulance system has also printed out a paper version of this information with a receipt form which is signed by the receiving nurse.

Meanwhile before the ambulance has arrived, the accident and emergency team assistant has received a notification of the incident by accessing the

electronic health record system. She is able to assemble any notes from the information that Dr Alperton, the GP and Mr Jones himself placed in the EHR.

In particular she discovers that Mr Jones attended a cardiology outpatient clinic at hospital some six week earlier. The relative ECG results give clinical information on treatment from the hospital electronic patient record system.

So, on arrival at accident and emergency and with confirmation of Mr Jones' identity the staff were able to print out care pathway forms, which already have been furnished with initial EHR data and a set of labels for Mr Jones' samples.

This scenario raises a number of questions particularly about how and when (EHR) information is produced in the first place and how it would be maintained.

So let us go back a few months, before the events we have just been looking at and see how the information got there. Mr Jones had presented himself at the surgery complaining of chest pain.

As part of the recommended care pathway Mr Jones was booked in for an exercise ECG at the hospital. As a result of this Mr Jones was diagnosed as suffering from coronary heart disease and was placed on an appropriate register within his primary care trust. In a consultation with his doctor, the use of the electronic health record was explained to him.

Doctor: now Mr Jones, we have seen from the results from the hospital, that the pain you have been having is Angina, and that you have coronary heart disease. Lots of men in your age and a lot younger have this, and if we are

careful we can manage it very well. You'll have a session with your nurse to talk about your data exercise, and then I want to talk to you about what we can do to make sure you get the right treatment if there is an emergency.

Mr Jones: Oh, do you think I am going to have a heart attack?

Doctor: Not necessarily, but it is a possibility, and if you get the right treatment quickly, then you could make a complete recovery, and that is what I want to discuss with you. If we put the important information from your record here at the surgery into a system called the electronic health record, then this information can be shared with other health care professionals based in the UK.

Mr Jones: Who would that be doctor?

Doctor: Well, the information you have given us here could be important for doctors in the hospital. If you want to call NHS Direct or the ambulance service for example, they can find out all the things they need to know about your heart condition and diabetes, and that will help them give you the right treatment.

Mr Jones: That sounds grand doctor, but would it mean that the ambulance men and nurses can see everything about me?

Doctor: Well, look here at my screen. If I press this button we can look at the sort of EHR information we need to give to emergency staff. This is what the ambulance service would see. It includes things like your current condition, medication, and allergy.

Mr Jones: Oh, that is OK, I would have expected you to know that anyway.

Doctor: Is there some thing concerning you, Mr Jones?

Mr Jones: Well, it is going back a bit, but you remember when you first came to the valley lots of years ago. I had a spot of bother with my neighbours.

Doctor: Don't worry about that Mr Jones, the only things that will go in the EHR for that long ago is the record of major surgery and things that have long term importance to your health.

Mr Jones: That is good, doctor.

Doctor: As well as medical information there is a space for you to put things in your EHR like your next of kin and any preferences for treatment.

Mr Jones: I do not know how to use one of those things.

Doctor: Do not worry, what I will do is book you a session with Judith, the Trust Health Record Counsellor and she will take you through all the things and help you. Is that OK?

Mr Jones: Thank you doctor. It all looks a bit complicated.

Doctor: Do not worry Edward, Judith will be able to sort everything out with you. Now that is all, let me show you out.

6.4.3 The scenario in the sight of the CTCP/CTRP model

In the above scenario there are two tasks. The first task (Emergency Incident Task) involves two collaborators, Mr Jones (patient) and Kathleen (NHS-Direct adviser) and a summary of the CTCP protocol inputs are shown in Table 11. The second task which is summarised in Table 12 involves two collaborators Mr Jones (patient) and Dr. Alperton (Mr Jones' GP).

Emergency Incident Task		
	Patient (Mr Jones)	NHS-direct (Kathleen)
Requirements	To be treated for chest pain	Information: Name, address, some details about the incident and name of anybody that can help him and to be informed about his case.
Resources	Information (including EHR record)	Medical Care Services
Policies	Not to inform his daughter.	Grant access to part of Mr Jones' EHR record to other units such as: ambulance crew, medical staff at the paramedic unit and to primary care (GP)

Table 11: Summary of the Emergency incident Task inputs

Task Creation Protocol CTCP:

Collaborators: 1. Mr Jones (patient)

2. Kathleen (NHS-Direct Adviser)

Introduction:

Mr. Jones calls the NHS-direct complaining from pain in his chest.

The NHS-direct make sure that it is a sort of pain needing an emergency task.

Negotiation:

Kathleen: required the following information:

i. Full name and address.

ii. Whether anyone is there with Mr Jones at home.

iii. A bit more detail on how bad is the pain.

iv. Has the patient called before?

v. Whether to inform your daughter Janice (next of kin) about your case.

Mr Jones

i. Full name Edward Jones, address: 23 High Street.

ii. Living alone.

iii. The pain lasted for about 20 minutes.

iv. No it's first time.

v. No, do not inform her, I would not worry her.

vi. His house's keys left with his neighbour Mrs Edith Smith. (?? No qiv)

Decision:

Kathleen: will send the Ambulance.

Agreement:

Kathleen: agreed not to inform Mr Jones' daughter.

Mr Jones: Agreed information about him will be propagated to the health care units dealing with his incident (ambulance crew, paramedic medical staff and his GP).

Task creation:

This task is composed of three groups of activates as following:

Kathleen (NDA):

i. Fetch the EHR record of Mr Jones.

ii. Forward information to the ambulance medical crew and to the paramedic unit (through the hospital system).

Ambulance Medical Crew (names in this role):

i. Receive the information and use it to reach Mr Jones' address and to give him the medicine that he needs to take on his way to the hospital (aspirin and blood pressure test).

ii. Pick up Mr Jones.

iii. Give him some medicine.

iv. Print a receipt including information about Mr Jones identity and information about medicine he took on his way to the hospital.

v. The receipt will be handed to the paramedic staff at the hospital and an electronic copy will be transmitted to the hospital system.

Paramedic Medical staff (names in this role):

i. Access the EHR record of Mr Jones.

ii. Discover previous visit to the coronary care unit.

iii. Diagnose (e.g. ECG)

iv. Store results in the hospital system.

v. Send results to Mr Jones' GP.

Running Task 1 using the CTRP protocol:

The following entities (in this task are all human) are the task participants: Kathleen: NHS-direct Adviser role, Janet (nurse) and Kim (Driver): Ambulance Crew role, Dr. Smith (ECG Doctor) and Lora (Paramedic Nurse): Paramedic Medical Staff role, and Mr. Jones (the patient).

Preparation:

Call the Ambulance and inform the paramedic unit at the hospital.

Task process and assessment:

Activity No 1:

Process: Kathleen fetches the EHR record of Mr Jones.

Assessment: Is she authorised?

Activity No 2:

Process: Kathleen: forwards information to the ambulance medical crew and to the paramedic unit.

Assessment:: Was it really sent to the ambulance medical crew and to the paramedic unit. One possible implementation by receiving authenticated acknowledgments from both the ambulance medical crew and to the paramedic unit.

Activity No 3:

Process: Kim receives name and address of Mr. Jones'.

Assessment: none.

Process: Kim picks up Mr. Jones.

Assessment: Picked up the right person?

Did she find the right person at the right place?

Process: Janet gives Mr. Jones the medicine that he needs to take on his way to the hospital.

Assessment: Check whether the medicine was subscribed before.

Process: the ambulance arrived at the hospital (A & E). Janet prints a dispatch receipt including the start and the arrival time of the ambulance and any medicine given to Mr. Jones during the journey. Janet signs it and give it to Lora with Mr. Jones.

Assessment: Lora checks the information against the information received electronically from the NHS Direct.

The above is just an example on how the task can be run. It should be noted that some policies used to assist the task activities were not in the task policies. In fact a task can inherit any general policy or ethical code.

Exception handling:

Firstly before handling an exception a system needs to capture it. Any strange behaviour is considered as a task policy violation and the exception is captured in the CTRP protocol as a policy violation.

In our model exceptions are divided into three types according to the handling process:

1. Exceptions with which the task can still continue to its normal end. Exceptions of this type are handled within the CTRP protocol by the task update component. Case 2, in the following examples, is an

example of this type of exception. Figure 19 illustrates the CTRP protocol and shows the path of the exception type as a double line.

2. Exceptions with which the task must be terminated and another task is required to complete the planned function.

   Such cases are handled partially in the CTRP protocol. The task in such cases is aborted and the process log (task history) used by the CTCP protocol to create another task to redo the function that could not be done by the terminated task with consideration for the exceptions that have arisen. The exception-handling path for this type is shown as a thick line in Figure 19.

3. Exceptions with which the task must be terminated and there is no need for any further actions.

   There are cases where the task is immediately terminated and no further actions are possible. Exceptions from this type are handled within the CTRP protocol through the ABORT component. Case 3 is an example. The exception-handling path for this type is shown as a dotted line in Figure 19.

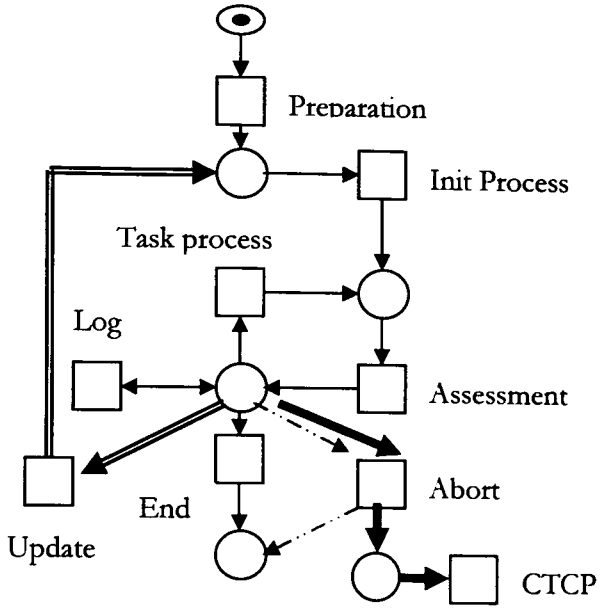

Figure 19 Petri net graph shows the exception handling types in the CTRP protocol.

As the scenario was for an ideal situation no exception or error occurred. However in the real world, exceptions do happen and systems need to be prepared. For further details about exception handling in our model see **Chapter 4**. To demonstrate the exception handling in our model we will use some exceptions proposed by Professor Mike Martin[3] in a discussion about the possible exceptions in such scenario.

Case 1: multiple ambulances:

This could happen if for instance Mr Jones' daughter found her father unconscious and called for an ambulance even though he has already arranged

[3] Professor Mike Martin is the technical director for the County Durham & Darlington EHR project

for one through the NHS Direct and the ambulance is already on its way to Mr. Jones' address.

This exception can be captured at the *introduction* of the CTCP protocol as it will appear as a duplicate task for NHS Direct. To handle this exception the new task will be discarded.

Case 2: ambulance breakdown

On its way to the hospital the ambulance has a breakdown due to a mechanical/electrical fault.

This exception will be reported by the ambulance crew to the task generator -- NHS Direct. This reflects the situation that the process of the task experiences a problem. The CTRP will prompt to be able to allow insertion of activities to resume the task. In this case the new activity is to send another ambulance.

Case 3: Mr. Jones found dead in his house:

Mr. Jones breathes his last before the ambulance arrived.

The CTRP protocol, while processing and assessing the activities of the emergency task particularly the activity of picking up Mr. Jones. The CTRP protocol will prompt that it is not possible to take Mr. Jones to the hospital. In this case no further activities can be followed in this task, which will cause the task to be aborted and no further action needs to be done.

Task 2: Mr Jones' visit to his GP

This task in fact happened before task number 1 and some data that had been used by task number 1 was created by this task.

There was another task before this task, which is Mr Jones' visit to the hospital, where he was diagnosed as suffering from coronary heart disease.

Emergency incident Task		
	Patient (Mr Jones)	GP (Dr Alperton)
Requirements	Further follow up for his case.	Information, consent to use the stored information about him and to make them available for other medical staff
Resources	Information (including EHR record)	Medical care services
Policies	To restrict the use of the information by doctors, NHS Direct and emergency staff	Grant access to part of Mr Jones' EHR record to other medical staff

Table 12: Task 2 (the GP visit) inputs summary

Introduction:

According to the hospital report you have angina.

Negotiation

GP:

Information related to this case is stored in the EHR. This data will be shared with other health care staff.

Mr. Jones:

Who?

GP:

Doctors at hospital, NHS Direct and emergency staff.

Decision

GP:

The GP will follow the treatment of Mr Jones

Agreement:

Mr Jones:

Agrees his medical record will be available to any medical staff dealing with his treatment.

Task Creation:

The following are the activities of this task:

EHR training tutorial for Mr Jones.

Arrangement for regular visits for Mr Jones to GP.

EHR case study evolution

Case study feature	CTCP/CTRP feature	Exceptions handling
Call the NHS-direct	CTCP.Introduction	
Call the NHS-direct (duplicate call)	CTCP.Introduction	CTCP.Introduction
Required information	CTCP.Negotiation	
Case verification	CTCP.Negotiation	
Informing relatives	CTCP.Negotiation	

Informing relatives	CTCP.Decision	
Case identification	CTCP.Decision	
Patient consent	CTCP.Negotiation CTCP.Agreement	
consent accept/reject	CTCP.Decision	
Responsibility and roles	CTCP.TaskCreation	
Access the EHR record of Mr Jones	CTRP.Process CTRP.Assessment	
Information forward	CTRP.Process CTRP.Assessment	
Ambulance arrangement	CTRP.Process CTRP.Assessment	
Pick up Mr Jones (patient dead)	CTRP.Process CTRP.Assessment	CTRP.abort
Test and treatment on board	CTRP.Process CTRP.Assessment	
Taking Mr. Jones to the A&E (ambulance breakdown)	CTRP.Process CTRP.Assessment	CTRP.update
Arriving at the A&E	CTRP.Process CTRP.Assessment	
Test and treatment at the A&E	CTRP.Process CTRP.Assessment	

Table 13: Illustration of the mapping between the events of the emergency scenario and the components of the CTCP/CTRP.

We have included some exceptions that were added to the scenario and discussed in section 6.4.3. Table 13 shows that:

- All the case study's processes are represented in the model

- The mapping between the case study's processes and the model components are readily matched.
- All the model features are used to represent the case study.

The above points respectively demonstrate the coverage, neutrality and focus of the model. It is important to notice that the case study (EHR) is independent of the model development.

Case study feature	CTCP/CTRP feature	Exceptions handling
Informing Mr Jones about the result of his test at the hospital	CTCP.Introduction	
Consent for Information sharing	CTCP.Negotiation CTCP.Decision	
Patient training	CTCP.TaskCreation	

Table 14: Illustration for the mapping between the events of the GP visit and the components of the CTCP/CTRP.

In task 2 as shown in Table 14 all the case study features are represented, demonstrating the coverage of the model. However, from the model focus point of view, not all the model features were used in this task because the task is very simple and no further actions/processes were required.

6.5. Conclusion

The purpose of the work discussed in this chapter is to challenge the model with a real case study.

Two case studies were used. The first demonstrates how the protocols worked in a simple environment for tutorial purpose. The second showed how the model coped with an example of real-world complexity, exhibiting its ability to deal with the exceptions that inevitably occur in complex scenarios. The second case study demonstrates the coverage, neutrality and focus of the model, that is all the case study's process were represented. The mapping between the case study's processes and the model components are readily matched and all the model features are used to represent the case study. This case study showed that all the exceptions were captured, and safely handled.

Chapter 7

DISCUSSION AND CONCLUSION

7.1. Thesis summary and discussion

Multi-agency services have proved very difficult to supply. Both technical and political problems occur. Technical difficulties include the integration of various networks and databases and political difficulties include policy conflicts and rapid change in organisations. Security management in such an environment is a major challenge as dynamic policies and different views and interests need to be modelled and prioritised. Security management therefore has both political and technical aspects. This thesis attempts to alleviate difficulties, which may otherwise discourage the development of collaboration networks. The area selected for regulations, principles and case studies was the medical area as it naturally involves multiple agents and we could take advantage of collaborative links with a medical informatics group at the Medical School, Newcastle University for obtaining advice and information.

The approach taken in this thesis has involved a number of stages. The regulations, declarations, rules and principles have been analysed, discussed

and classified so as to achieve an understanding of the nature of the security requirements in this area (Chapter 2). Sources consulted included the general purpose Universal Declaration of Human Rights and the Data Protection Act for Britain. More specialised regulations, on the application area of medical multi-agency applications selected for study, included the World Medical Association Declaration of Helsinki and the Council of Europe Recommendation and two British collection of rules, the principles of BMA and Caldicott. The discussion of these requirements, relationships between them and the debate that was invoked by the declaration of some of them helped to identify the fundamental security requirements for an integrated health care record such as the Health Electronic Record.

Regulations such as the Data Protection Act and the Caldicott principles explicitly request that the use of any confidential data must be restricted by a purpose (e.g. DPA's principle 2 and Caldicott's principle 1). In addition there is no need without purpose leading to the concept of need-to-know, which can be used to restrict access to confidential data for only specific purposes.

A study of the existing security models such as the Bell-Lapadula Model (BLP), the Clark-Wilson model, the Biba model, the Chinese wall model and the Harrison-Ruzzon-Ullman model (HRU) showed that none of these models will meet the security requirements in a multi-agency services environment. This is because they are designed to meet specific security

policy, for instance the BLP deals with confidentiality in a multi-level security environment and Biba in the same environment deals with integrity; in these models, apart from the Chinese wall model, the information flows vertically (Multi-Level Security Policies), while in a multi-agency service environment it flows horizontally (Multilateral Security Policies); none of these models control the use of data.

In addition the examination of the BMA model, the only existing security model for the health care information systems, demonstrated that this model fails to meet the multi-agency security requirements as it lacks any facilities for handling need-to-know (Chapter 3).

Other conventional approaches and techniques of access control (Chapter 1) such as Discretionary Access Control (DAC), Mandatory Access Control (MAC) and Role-Based Access Control (RBAC) were also considered. Although almost all the available operating systems, software and application are based on these approaches, they were found not up to the challenge imposed in any attempt to build a secure multi-agency service environment. For instance they do not have any explicit solution for problems such as need-to-know, control of the use of data, relationships, responsibilities and dynamic ownership management.

The task-based approach was carefully selected as an approach for our model as it is logically more suitable for such an environment. Indeed the task-based approach supports the control of data access and its usage by

purpose. The task is a common object between collaborators, responsibilities are explicitly recognized and the task is scalable, dynamic and flexible.

There are some existing task-based approaches but examination showed that none of these models meet the multi-agency requirements. For instance TBAC only deals with the authorisation, the Fischer-Hubner model deals only with the privacy aspect and GSM is only suitable for hierarchical systems. This matter is discussed further later in this chapter.

The solution identified in this work (Chapter 4) for the security requirements was to develop a task-based model, CTCP/CTRP, comprising a Collaboration Task Creation Protocol which provides a negotiating framework for producing CTRP and a Collaboration Task Runtime Protocol, for monitoring and running the created task. The model handles exceptions and errors.

The model was tested in a number of ways. Firstly the model was represented in Petri net form, a notation suited to a distributed, asynchronous, concurrent, parallel and non-deterministic environment. Secondly the model was validated against the regulations, the Data Protection Act and Caldicott principles, forming the requirements for the security and against software engineering principles (Chapter 5). Thirdly a simple example for tutorial and demonstration purposes was developed. Fourthly two case studies were made (Chapter 6), one on a relatively simple problem (dynamic coalition), the other on a more realistic problem

(emergency scenario taken from a real project in health care) independent from the development of the model. Finally implementation guidelines were suggested for the protocols' components.

The model satisfied all these tests. The Petri nets produced were validated by PEP software for consistency including reachability. The model met the requirements and covered the critical aspects in both the more specific task-based approach of Caldicott and the more general DPA. The software engineering principles of maximal cohesion, low coupling and efficient execution were met by CTCP/CTRP. The simple example was very helpful for explaining the protocols at conferences.

The case studies, including a real-world one, were realisable in the model. The results of this work showed that the protocols can cope with real-world scenarios. Although the case study was for an ideal situation, in which there was no error or exceptions, a number of exceptions were suggested by a person, who is directly involved in the projects that resulted in the scenario. The test showed that the protocols are able to handle these exceptions. The mapping between the protocols components and the case study processes demonstrates the property of neutrality in the model. The test also showed that all the case studies processes were representable, which means that the property of coverage is achieved. Not all the protocols components were used in the first case study as it was a simple one. However the focus property was achieved in the second case study, which is more realistic as all the protocols components were used.

7.2. Related works

Existing work addresses one part of the requirements but not the other. The solutions can be classified as multi-agent but not task-based and task-based but not multi-agent. These are discussed below.

7.2.1 Solutions for Multi-agency Applications that are not a task-based

Solutions in health care information system in Europe and US such as the collaboration environment (WebOnCOLL) [21] and the TIHI (*Trusted Interoperation of Healthcare Information*) project [90] are not capable of addressing the security requirements in a multi-agency environments as they rely on traditional access control mechanisms and they cannot effectively support requirements such as data using control, responsibility tracing and ownership management (see Section 1.4).

In the UK the only security policy model developed to meet the security requirements for the health care information systems is the BMA model. Considering its importance this model was considered in depth in this research and Chapter 3 covers a detailed study in which the model was verified and investigated against the multi-agency security requirements. The result of this investigation showed that the model is not capable of meeting a number of these requirements (Section 3.5).

Yalta [19] and dRBAC [36] are two from a rather short list of contributions to the solution of the security problem in another multi-agency services application, the Dynamic Coalition. Yalta is one of a number of projects funded by DARPA which aims to provide an infrastructure for sharing

information among collaborators. The Distributed Role-Based Access Control dRBAC [36] is an access control mechanism for systems that involve multi-administrative domains. However neither Yalta nor dRBAC explicitly support requirements such as control data use and ownership managements. In addition there is no framework in which the collaborator can negotiate.

Section 6.2.1 covers a discussion for a number of Dynamic Coalition projects. [51] Addresses the negotiation and management of resources in Dynamic Coalitions and [89] show a mathematical framework that is capable of expressing negotiation.

However multi-agency security requirements are more than just negotiation support.

Another related area is the cross-organization security management (Section 1.4.) where the following are examples for different applications: Access Management Broker server and a plug-in module for web servers [58], the Digital Library Authentication and Authorisation Architecture (DLA3) and Coalition for Networked Information (CNI) [54]. None of these support any framework enables collaborators to negotiate issues such as access privileges and any authorised access will be limited by the intent or purpose.

7.2.2 Task-based models but not for multi-agency applications:

The task-based approach as discussed thoughout the thesis (section 1.63.5.3 and 4.1.1) is a promising approach to deal with security requirement. Researchers have studied the task-based approach and tried to use it to address some security requirements. Mahling, Coury and Croft [55] have noted the important of this approach and tried to build a task-based collaboration model. The Steinke model or the Group Security model (GSM) [80] seeks to provide access to information on the basis of a user's task. Thomas and Sandhu in 1994 used this approach to address integrity issues in computerized information systems [81]. In 1997 they used the Task-based approach to develop their TBAC (Task-based Access Control). This model aims to address the authorization management problem. Fischer-Hubner and Ott [34] developed a task-based model to deal with privacy issue.

None of the above task-based models seeks to address the security problem in the multi-agency environment. For detailed discursion of these models refer to Section 1.6.

7.3. Limitation and future research

For the model to be general and to be capable of dealing with human-involved tasks, a 100% implementation (computerization) for the model with one standard will be a major research topic. Further research will be invited to divide the different tasks into categories and then create a template for each category. The templates at the beginning will be acceptable in different

formats as it will be difficult to find one format to fit all task types. Such research could lead firstly to a standard for writing task templates. This step will encourage researchers to look for a standard for the CTCP/CTRP model implementation, which will work in all cases.

More research is needed to formally verify all the components of the CTCP/CTRP protocols and establish standard interface between these components. A possible way forward is to use a combination of logical mathematics (e.g. category theory) and Petri nets which is under development but is a very substantial topic in its own right [6]. Petri nets are increasingly accepted as a useful technique for formulating security policies [71]. Category theory provides a logical framework within which the details of Petri nets can be embedded.

Previous work by Furuta and Stotts [37], using Petri Net in collaboration networks, can be built upon. In particular the negotiation and introduction components in CTRP can adopt the method used by Furuta and Stotts.

In CTRP the Petri nets will be expanded to examine the possibility of dead lock cases in a parallel activity processing situation.

In this thesis we have introduced the idea of validating models against security regulation. This can be the basis for more research in this area. For instance it may be possible to develop languages to convert security regulation into formal security policies.

The research reported in this thesis draws attention to the advantages of the task-based approach and how this approach can be an alternative to the rather exhausted approaches such as the Role-Based approach. These advantages will encourage researchers to challenge the task-based approach with other security requirements. It may also be possible to implement operating systems or standard network protocols based on this idea.

In this thesis the CTCP/CTRP model was tested with two case studies, one of which was a real-world case study. These two case studies were in two applications: Dynamic Coalition (an example) and Electronic Health Record (a real-world scenario). With more time and availability of collaboration we would like to challenge the model with more real-world scenarios in these two applications and in other multi-agency scenarios.

In this research we have used three security languages to represent a security policy model. These languages for the first time were challenged with independent policies and the results of this works express the need for more research in the area of security languages.

Workflow systems are used extensively in business to run processes in a controlled environment. Workflow systems and our model CTCP/CTRP are both task-based. Therefore it should be possible to apply the CTCP/CTTRP model directly to a workflow system. It should be investigated whether security policies specified through CTCP and implemented through CTRP can to be applied effectively to a complete workflow system. In particular we

aim to investigate the possibility of using workflow management systems and techniques to implement the task process component within the CTRP.

7.4. Conclusion

In this research we contributed to the solution of the multi-agency services and collaboration networks security problem. We have shown how a study for the security rules and regulations leads to better understanding for the security requirements. The study reviewed current declarations, legislation and regulations to bring together a global, European and national perspective for security in health services. This study helps to properly identify an appropriate approach to tackle difficult problem such as multi-agency security problem and helps to identify security requirement for potential electronic health record.

We have examined a British security policy model, BMA, using the security languages and showed that the BMA model is incapable of supporting multi-agency security requirements such as need-to-know.

We developed a task-based CTCP/CTRP model based on two linked protocols. The CTCP (Collaboration Task Creation Protocol) is designed to enable collaborators to negotiate (include decision and agreement) and create tasks that comply with their policies and meet their requirements. The CTRP (Collaboration Task Runtime Protocol) is designed to enable the collaborators

to follow up the execution of their tasks and to ensure that tasks are running under the agreed policy and on the right track to meet the potential goal. The models were represented by Petri nets.

The developed model was validated against two regulations the DPA and the Caldicott principles and reviewed for technical completeness and satisfaction of software engineering principles.

The model was finally tested against two case studies from two different applications, one of them is real-world case study. The coverage, neutrality and focus of the model were examined.

The final outcome of this research is to draw attention to the need of further research in areas such as security policy languages, security requirements investigation and alternative access control approaches.

References

1. Aljareh, S., Dobson, J. and Rossiter, N., Satisfaction of Health Record Security Principles through Collaborative Protocols. in *the 8th International Congress in Nursing Informatics*, (Rio de Janeiro, 2003).

2. Aljareh, S. and Rossiter, N. Modelling Security in Multi-agency environment, Report no CS-TR-764, Newcastle University, Newcastle upon Tyne, 2002.

3. Aljareh, S. and Rossiter, N., A Task-based Security Model to facilitate Collaboration in Trusted Multi-agency Networks. in *ACM SAC 2002 symposium on Applied Computing*, (Madrid, 2000), 744-749.

4. Aljareh, S. and Rossiter, N., Toward security in multi-agency clinical information services. in *In proceedings of workshop on dependability in healthcare Informatics*, (Edinburgh, 2001).

5. Aljareh, S. and Rossiter, N. Toward security in multi-agency clinical information services. *Health Informatics Journal*,2002, *8* (2). 96-104.

6. Aljareh, S., Rossiter, N. and Heather, M., A Formal Security Model for Collaboration in Multi-agency Networks. in *2nd Workshop on Security in Information Systems (WOSIS 2004)*, (Porto, Portugal, 2004), 157-169.

7. Al-Kahtani, M. and Sandhu, R., A Model for Attribute-Based User-Role Assignment. in *18th Annual Computer Security Applications Conference ACSAC*, (Las Vegas, Nevada, US, 2002).

8. Anderson, R. Remarks on the Caldicott Report, http://www.cl.cam.ac.uk/~rja14/caldicott/caldicott.html, 1998.

9. Anderson, R. *Security Engineering: a guide to building dependable distributed systems.* John Wiley, New York, 2001.

10. Anderson, R. Security in clinical information systems. BMA Report, British Medical Association, 1996.

11. Anderson, R., A security Policy Model for clinical information systems. in *IEEE Symposium on Research in Security and Privacy, Research in Security and Privacy*, (1996), 30-43.

12. Anderson, R., Why Cryptosystems Fail. Communications of the ACM. in *Communications of the ACM*, (1994), 32-40.

13. Anderson, R., Hanka, R. and Hassey, A. Clause 67, medical research and privacy: the Options for the NHS, http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/hcbillc67.pdf, 2001.

14. Arlington Software Corporation. ERGO: Decision Support System, http://www.arlingsoft.com/, 2002.

15. Bell, E.D. and LaPadula, L.J. Secure Computer Systems: Mathematical Foundations. Mitre Report, Mitre Corporation, Bedford, MA, 1974.

16. Biba, K. Integrity Considerations for Secure Computing Systems, Mitre Corporation, Bedford, MA, 1975.

17. Brewer, D.F.C. and Nash, M.J., The Chinese Wall Security Policy. in *IEEE Symposium on Security and Privacy*, (Oakland, CA, 1989), 206-214.

18. British Parliament. Health and Social Care Act 2001, London, 2001.

19. Byrd, G., Gong, F., Sargor, C. and Smith, T., Yalta: A Secure Collaborative Space for Dynamic Coalitions. in *IEEE Workshop on Information Assurance and Security*, (United States Military Academy, 2001).

20. Caldicott Committee. The Caldicott Committee Report on the review of patient-identifiable information, Department of Health, 1997.

21. Catherine, E., Chronaki, Dimitrios, G., Katehakis, Xenophon, Z., Manolis, T., Stelios, C. and Orphanoudakis Medical collaboration in regional healthcare networks. *IEEE Transactions on Information Technology in Biomedicine*,1997, *1* (4). 257-269.

22. Ching, N., Jones, V. and Winslett, M., Authorisation in the Digital Library: Secure Access to Services across Enterprise Boundaries. in *Third Forum on Research and Technology Advances in Digital Library*, (Washington, D.C. USA, 1996), IEEE Computer Society Press, 110-119.

23. Chu-Carroll, J. and Carberry, S. Conflict Resolution in Collaborative Planning Dialogues. *International Journal of Human-Computer Studies*,2000, *53* (6). 969-1015.

24. Clark, D.D. and Wilson, D.R., A Comparison of Commercial and Military Computer Security Policies. in *IEEE Symposium on Security and Privacy*, (Oakland, CA, 1987), 184-194.

25. Cohen, B. A Formal Model of Healthcare Security Policy, European Standardization of Health Informatics, 1996.

26. Council of Europe. Recommendation No. R (97) 5 of the Committee of Ministers to Member States on The Protection of Medical Data, www.cm.coe.int, 1997.

27. County Durham & Darlington EHR. The Animators, Health Information Zone, http://www.durham.nhs.uk/ehr/animators.asp, 2002.

28. Damianou, N., Dulay, N., Lupu, E. and Sloman, M. Ponder: A Language for Specifying Security and Management Policies for Distributed Systems The Language Specification Version 2.2, 2000.

29. DARPA (Advanced Research Projects Agency). Boundary controller, http://www.darpa.mil, 1999.

30. Denley, I. and Smith, S. Privacy in clinical information systems in secondary health care. *British Medical Journal*,1999, *318* (7187). 1328-1329.

31. Department of Health. Confidentiality, Use and Disclosure of Personal Health Information, London, 1994.

32. Detmer, D. Counterpoint. Your privacy or your health - will medical privacy legislation stop quality health care? *International Journal for Quality in Health Care*,2000, *12* (1). 1-3.

33. Diaper, D. Task Analysis for Knowledge Descriptions (TAKD): A Requiem for a Method. *Behaviour and Information Technology*,2001, *20* (3). 199-212.

34. Fischer-Hübner, S. and Ott, A., From a Formal Privacy Model to its Implementation. in *21st National Information Systems Security Conference*, (Arlington, VA, 1998).

35. Flynn, D.J. *Information Systems Requirements Determination and Analysis.* McGraw Hill Text, London, 1998.

36. Freudenthal, E., Pesin, T., Port, L., Keenan, E. and Karamcheti, V., dRBAC: Distributed Role-based Access Control for Dynamic

Coalition Environments. in *22nd International Conference on Distributed Computing Systems (ICDCS'02)*, (Vienna, Austria., 2002), IEEE Computer Society, 411-420.

37. Furuta, R. and Stotts, D., Interpreted collaboration protocols and their use in groupware prototyping. in *ACM conference on Computer supported cooperative work*, (Chapel Hill, North Carolina, United States, 1994), ACM Press, 121-131.

38. Garfinkel, S. *Database Nation - The death of privacy in 21st century*. O'Reilly & Associates, Sebastopol, CA, 2000.

39. Gollmann, D. *Computer Security*. John Wiley and Sons, 1999.

40. Graham, G. and Denning, P., Protection: Principles and Practice. in *Joint Computer Conference*, (1972), AFIPS Press.

41. Great Britain *Data Protection Act 1998 : Chapter 29*. Stationery Office, London, 1998.

42. Griew, A., Briscoe, E., Gold, G. and Groves-Phillips, S. Need to know allowed to know. The health care professional and electronic confidentiality. *Information Technology & People*,1999, *12* (3). 276-286.

43. Harrison, M.A., Ruzzo, M.L. and Ullman, J.D. Protection in operating systems. *Communication of the ACM*,1976, *19* (8). 461-471.

44. Hayes, B.S. Collaboration Protocol Agreement Simple Negotiation Business Process Model, http://home.attbi.com/~brianhayes/TR/2002/CpaSimpleNegotiation-0.06.pdf, 2002.

45. Hayton, R. and Moody, K., An Open Architecture for Secure Interworking Services. in *IEEE International Conference on Distributed Computing Systems (ICDCS)*, (1997), 315-321.

46. Hoagland, J., Raju, P. and Levitt, K. Security Policy Specification Using a Graphical Approach, University of California, Davis, California, 1998.

47. Jajodia, S., Samarati, P. and Subrahmanian, V., A Logical Language for Expressing Authorizations. in *IEEE Symposium on Security and Privacy*, (Oakland, CA, USA, 1997), IEEE Press, 31-42.

48. Johnson, P. *Human Computer Interaction: psychology, task analysis and software engineering.* McGraw-Hill, London, New York, 1992.

49. Johnson, P., Task Knowledge Structures. in *Task analysis in Human Computer Interaction*, (1989), Ellis Horwood.

50. Johnson, P. and Wilson, S., Task-Based Design and Prototyping. in *ACM SIGCHI Basic Research Symposium*, (Boston, 1994), ACM.

51. Khurana, H. Negotiation and Management of Coalition Resources *Department of Electrical and Computer Engineering*, University of Maryland, Maryland, 2002, 149.

52. Kling, R. Information and computer scientists as moral philosopher and social analysts. in Kling, R. ed. *Computerization and controversy: Value conflicts and social choices*, Academic Press Inc, 1991, 32-37.

53. Lampson, B., Protection. in *5th Princeton Symposium on Information Science and Systems*, (1971).

54. Lynch, C. A White Paper on Authentication and Access Management Issues in Cross-organisational Use of Networked Information Resources, Coalition for Networked Information CNI http://www.cni.org/projects/authentication/authentication-wp.html, 1998.

55. Mahling, D.E., G, C.B. and B, C.W., User Models in Cooperative Task-oriented environment. in *23rd Annual Hawaii IEEE International Conference on System Science*, (1990), 94-99.

56. McLean, J. Security Models. in Marciniak, j. ed. *Encyclopedia of Software Engineering*, Wiley & Sons, 1994.

57. McLean, J., Security models and information flow. in *IEEE Symposium on Security and Privacy, pages*, (Oakland, 1990), 180--187.

58. Millman, D. Cross-Organisational Access Management: A Digital Library Authentication and Authorisation Architecture. *Digital Library Magazine*,1999, *5* (11).

59. Moffett, J., Requirements and Policies. in *Policy Workshop*, (HP-Laboratories, Bristol, UK, 1999).

60. National Institue of Standerd and Technoloy NIST. Role Based Access control: site to provide access to NIST's awarded winning RBAC research, http://csrc.nist.gov, 2002.

61. OASIS Technical Committee. Collaboration-Protocol Profile and Agreement Specification Version 2.0. From OASIS ebXML Collaboration Protocol Profile and Agreement, http://xml.coverpages.org/ni2002-12-03-b.html, 2002.

62. O'Conor, R. Commentary: Organisational and cultural aspects are also important. *British Medical Journal*,1999, *318* (7187). 1330-1331.

63. Osborn, S., Sandhu, R. and Q, M. Configuring Role-Based Access Control to Enforce Mandatory and Discretionary Access Control Policies. *ACM Transactions on Information and Systems Security*,2000, *3* (2).

64. Phillips, C., Ting, T. and Demurjian, S., Information Sharing and Security in Dynamic Coalitions. in *7th ACM Symposium on Access*

Control Models and Technologies (SACMAT 2002), (California, USA, 2002), 87-96.

65. Reisig, W. *Petri Nets: an introduction.* Springer-Verlag, Berlin, New York, 1985.

66. Reisig, W. and Rozenberg, G. (eds.). *Lectures on Petri Nets: Advances in Petri Nets* . Springer, 1998.

67. Röscheisen, M. A Network-Centric Design for Relationship-based Right Management *Department of Computer Science*, Stanford University, Stanford, CA, 1998.

68. Röscheisen, M. and Winograd , T. A Network-Centric Design for Relationship-based Security and Access Control. *Journal of Computer security*,1997, *5* (3). 249 - 254.

69. Rosemary, J. *Data Protection Act 1998.* Sweet & Maxwell, London, 1999.

70. Russell, D. *Computer Security Basics.* O'Reilly & Associates, Sebastopol, CA, 1991.

71. Ryan, P., Theoretical Challenges Raised by Information Security. in *24th International Conference on Application and Theory of Petri Nets*, (Eindhoven, The Netherlands, 2003).

72. Samarati, P. and Di Vimeracti, D.C. Access Control: Policies, Models, and Mechanisms. in Focardi, R. and Gorrieri, R. eds. *Foundations of Security Analysis and Design*, Springer-Verlag, 2001.

73. Schneider, B., Fred Least Privilege and More. *IEEE Security & Privacy*,2003, *1* (5). 55-99.

74. Schneier, B. *Applied cryptography : protocols, algorithms, and source code in C.* Wiley, New York, 1995.

75. Schneier, B. *Applied cryptography : protocols, algorithms, and source code in C.* Wiley, New York, 1993.

76. Schneier, B. Managed Security Monitoring: Network Security for the 21st Century. *Computer & Security*,2001, *20* (6). 491-503.

77. Schneier, B. *Secrets and lies : digital security in a networked world.* John Wiley, New York, 2000.

78. Shen, H. and Dewan, P., Access control for collaboration environment. in *ACM Conf. Computer-Supported Cooperative Work, CSCW*, (1992), 51-58.

79. Sommerville, I. *Software Engineering.* Addison-Wesley, Harlow, England, 2001.

80. Steinke, G. A task-based Approach to Implementing Computer Security. *Journal of computer Information Systems*,1997, *fall.* 47-54.

81. Thomas, R. and Sandhu, R., Conceptual Foundation for a Model of Task-Based Authorization. in *7th IEEE Computer Security Foundations Workshop*, (Franconia, NH, 1994), 66-79.

82. Thomas, R. and Sandhu, R., Task-based Authorization Controls (TBAC): A Family of Models for Active and Enterprise-oriented Authorization Management. in *IFIP WG11.3 Workshop on Database Security*, (Lake Tahoe, California, 1997), Chapman & Hall, Ltd, 166-181.

83. Trouessin, G. Health Informatics, Framework for Formal Modelling of 20 Healthcare Security Policies, European Committee for Standardization, 1998, 1998.

84. Tsiknakis, M., Chronaki, C.E., Kapidakis, S., Nikolaou, C. and Orphanoudakis, S.C. An Integrated Architecture for the Provision of Health Telematic Service based on digital Library Technology. *International Journal on Digital Libraries*,1997, *1* (3). 257-277.

85. United Nations *Universal declaration of human rights*. United Nations, New York, 1997.

86. United Nations. Universal Declaration of Human Rights, www.un.org, 1948.

87. Van, d.A. and Basten, D., Identifying Commonalities and differences in Object Life Cycles using Behavioral Inheritance. in *Application and Theory of Petri Nets 2001, 22nd International conference ICATPN*, (Newcastle, 2001), Springer, 32-52.

88. Van den Hoven, J. Counterpoint. Privacy and health information: the need for a fine-grained account. *International Journal for Quality in Health Care*,2000, *12* (1). 5-6.

89. Virgil, G., Bharadwaj and John, B., Towards Automated Negotiation of Access Control Policies. in *IEEE 4th International Workshop on Policies for Distributed Systems and Networks*, (Lake Como, Italy, 2003), IEEE Computer Society, 111-119.

90. Wiederhold, G. and Bilello, M., A Security Mediator for Health Care Information. in *AMIA Conference*, (1997).

91. Willison, D. Counterpoint. Privacy and confidentiality concerns - are we up to the challenge? *International Journal for Quality in Health Care*,2000, *12* (1). 7-9.

92. World Medical Association. Declaration of Helsinki / Ethical Principles for Medical Research Involving Human Subjects, The Association of Research in Vision and Ophthalmology, 2000.

93. Yao, W., Moody, K. and Bacon, J., A Model of OASIS Role-Based Access Control and its Support for Active Security. in *Sixth ACM Symposium on Access Control Models and Technologies, SACMAT*, (2001), 171-181.

94. Zlotkin, G. and Rosenschein, J., A domain theory for task oriented negotiation. in *the Thirteenth International Joint Conference on Artificial Intelligence*, (1993), 416-422.

Appendix A

PRINCIPLES OF THE DATA PROTECTION ACT (DPA)

Principles verbatim from DPA 1998

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Appendix B

CALDICOTT PRINCIPLES AND RECOMMENDATIONS

Caldicott Principles

Principle 1 - Justify the purpose(s)

Every proposed use or transfer of patient-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an appropriate guardian.

Principle 2 - Don't use patient-identifiable information unless it is absolutely necessary

Patient-identifiable information items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

Principle 3 - Use the minimum necessary patient-identifiable information

Where use of patient-identifiable information is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out.

Principle 4 - Access to patient-identifiable information should be on a strict need-to-know basis

Only those individuals who need access to patient-identifiable information should have access to it, and they should only have access to the information items that they need to see. This may mean introducing access controls or splitting information flows where one information flow is used for several purposes.

Principle 5 - Everyone with access to patient-identifiable information should be aware of their responsibilities

Action should be taken to ensure that those handling patient-identifiable information - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

Principle 6 - Understand and comply with the law

Every use of patient-identifiable information must be lawful. Someone in each organisation handling patient information should be responsible for ensuring that the organisation complies with legal requirements.

Caldicott Recommendations

Recommendation 1:

Every flow of information, current or proposed, should be tested against these principles as a matter of course. Continuing flows should be re-tested regularly and routinely.

Recommendation 2:

It is recommended that a programme of work, led by the NHS Executive, be established to reinforce confidentiality and IM&T security requirements amongst all staff within the NHS, with senior managers being specifically targeted to remind them of their responsibilities for maintaining security and confidentiality within their organisations. This programme should include:

- effective dissemination of existing guidance;
- the establishment of local codes of conduct aimed at safeguarding patients' rights in this respect;
- appropriate awareness training to ensure that all staff who have access to patient-identifiable information are fully aware of their

obligations to respect and protect the confidentiality of that information;

- a duty of confidence requirement in staff contracts and induction processes that ensure newly recruited staff are informed of policies and procedures as part of standard induction processes;
- undertaking work in conjunction with the clinical professions and patient groups, to produce readily accessible material for patients which will clearly inform them about the uses to which information about them may be put, and to establish the most effective ways of disseminating this information;
- Ensuring that, in all cases where access to patient-identifiable information held electronically is necessary, computer systems must adhere to the requirements set out in the NHS Executive's IM&T Security Manual, implement appropriate security controls and provide audit trails of access to such information.

Recommendation 3:

A senior person should be nominated in each NHS organisation, including the Department of Health and associated agencies, to act as a "guardian". The "guardian" should normally be a senior health professional or be closely supported by such a person. The NHS IM&T Security Manual (Section 18.4) requires each organisation to designate a senior medical officer to oversee all procedures affecting access to person-identifiable health data. This role and that of the "guardian" may be combined, providing there is no conflict of

interest. The Department of Health should take the development of this role forward in partnership with interested parties.

Recommendation 4:

Guidance must be provided for those individuals/bodies responsible for approving uses of patient-identifiable information (for example. the "guardian" or research ethics committees) to enable them to critically appraise new proposals and continuing practice.

Recommendation 5:

We wish to see the Department and the NHS, along with partner organisations, jointly identify the key areas in which protocols are required and prepare and publish good practice frameworks for local adoption in these areas

Recommendation 6:

It is further recommended that consistent with the framework of responsibility advocated by this report, each NHS and non-NHS organisation clearly establishes and communicates to partner organisations who is responsible for monitoring the sharing and transfer of information within the agreed local protocol.

Recommendation 7:

The possibility of an accreditation system, which would recognise those organisations which follow good practice with respect to confidentiality, should be explored by the Department of Health in partnership with interested groups.

Recommendation 8:

The new NHS number should replace patient-identifiable data, as soon as practically possible, in every data flow where there is a need to distinguish between individuals but where there is no immediate corresponding need to identify those individuals. Continued use of additional patient-identifiable data items for other purposes must be robustly justified. The Department of Health should urgently pilot the use of the NHS number as the main identifier, e.g. in contracting flows.

Recommendation 9:

The NHS Executive, in partnership with professional bodies, should develop strict protocols to define which individuals are authorised to gain access to patient identity, (e.g. where the new NHS number is the main identifier, through use of the NHS Number Tracing Service or through access to administrative or other population registers), and under what circumstances access should be authorised

Recommendation 10:

Where particularly sensitive information is to be transferred, the use of privacy enhancing technologies (e.g. encrypting the NHS number) must be urgently explored.

Recommendation 11:

We recommend that the appropriate trade and professional associations are encouraged to raise awareness amongst their members, and that institutions

providing training in healthcare informatics are encouraged to include privacy enhancing technologies as part of those training programmes.

Recommendation 12:

The internal structure, and administration, of databases should reflect the principles developed in this report, e.g. separating patient identifying details from event, treatment, or condition information with linkage possible only under specific and controlled circumstances. Whilst it is recognised that there may be practical barriers to restructuring existing databases, the practicalities of doing so should be explored.

Recommendation 13:

The new NHS number should replace the patient's name on Items of Service Claims made by General Practitioners as soon as is practically possible. The software used by all General Practitioners, the Dental Practice Board and Health Authorities should be reviewed to determine the resource consequences of specification changes which would be required to support changes in practice as recommended in this report.

Recommendation 14:

The design of new systems for the electronic transfer of prescription data should incorporate the principles developed in this report.

Recommendation 15:

Negotiations on pay and conditions for GPs should have regard to the desirability of avoiding systems of payment which require patient identifying details to be transmitted.

Recommendation 16:

The practicalities of piloting new procedures for claims and payments which do not require patient-identifiable information to be transferred should be urgently considered, e.g. batched claims with details held in general practice for audit purposes.