

Developments in confidentiality and consent functions to support wider sharing of electronic health records in the UK

Stephen Elgar

Technical Report
RHUL-MA-2011-06
8th March 2011



Department of Mathematics
Royal Holloway, University of London
Egham, Surrey TW20 0EX, England

<http://www.rhul.ac.uk/mathematics/techreports>

Developments in confidentiality and consent functions to support wider sharing of electronic health records in the UK

Executive summary

Electronic health records have become essential tools for the support of Medicine. At one time access to these records was limited within the boundary of a health service organisation; increasingly use is extended beyond this boundary. This extended use presents a security challenge in management of patient consent and confidentiality. Practical examples of shared health records can be seen in the UK National Health Service where there have been significant recent investments in IT systems. The goal of this dissertation is to analyse the UK legal framework for consent and confidentiality and, using this, identify shortcomings in current arrangements. A security policy and model is then developed based on Clark-Wilson and conclusions are drawn from comparison of this model with these developments.

Developments in confidentiality and consent functions to support wider sharing of electronic health records in the UK

Section	Contents	Page
	Executive summary	1
	List of figures, tables, abbreviations and acronyms	2
1	Introduction	5
2	Literature review of shared use of electronic health records and associated security models	7
3	The UK legal framework and a definition of the key concepts for confidentiality and consent for sharing health records	12
4	Practical issues of confidentiality and consent for existing systems in NHS organisation	18
5	Confidentiality and consent for UK NHS Care Record Service and other examples	21
6	Analysis of threats, security services, a policy and a proposed use of the Clark-Wilson security model	30
7	Comparison of the model with examples of shared use of electronic health records	42
8	Conclusions	46
Appendix		
A	Interviews	48
B	References	49

Developments in confidentiality and consent functions to support wider sharing of electronic health records in the UK

List of figures		Page
1	Balance between clinical access and patient privacy for different forms of consent	9
2	Number of English NHS service provider organisations, staff (subjects) and health records (objects) 2006/7	11
3	Single organisation with integrated set of systems with limit of accountability at boundary	17
4	De-identification of secondary use information	18
5	Structural elements of an electronic health records	20
6	Flow of patient information in and out of GP Practices	21
7	Hospital set of integrated systems with flows of patient information	22
8	Security functions for the Care Record Service	24
9	Several organisations sharing use of a CRS with access to patient information through a portal	26
10	Care Record Service Interoperability Toolkit, four examples of information passing into and out of the CRS security domain	28
11	Several organisations exchanging information to Personal Health Record	30
12	Basic principles of access control in the Clark-Wilson Model, annotated to illustrated use for electronic health records	36

List of tables		Page
1	Desirable characteristics of electronic medical records	8
2	Security marking of NHS electronic health record	11
3	Summary of UK legal basis for confidentiality and consent functions of health records	14
4	UK NHS Best Practice Guide for Consent obligations for healthcare organisations using the Care Record Service	17
5	Care Record Service consent functions in London	24
6	Threats to electronic health records	30
7	Summary of Technical Controls for electronic health records	31
8	Security Policy for an electronic health record	31
9	Clark-Wilson Transaction Processes for an EHR	33
10	Clark-Wilson; the association of Transformation Procedures (TP) with Role-Based Access Control (RBAC)	34
11	Clark-Wilson; Constrained Data Items for an EHR	34
12	Clark-Wilson; Consent flag for view and edit functions for Constrained Data Items for an EHR	35
13	Clark-Wilson; Digital certificate for Constrained Data Items within an EHR	36
14	Clark-Wilson; Team and organisation codes for an EHR	36
15	Clark-Wilson; integrity verification procedures for an EHR	37
16	Clark-Wilson; Certification Rules for an EHR	37
17	Summarised features of Clark-Wilson Model	41
18	Comparison of the Care Record Service with the policy	44
19	Comparison of the Care Record Service with the model	45

List of abbreviations and acronyms	
National Health Service (UK publically funded health, free at the point of care, delivered by independent and public organisations)	NHS
United Kingdom	UK
Electronic health record	HER
Care Record Service	CRS
Summary Care Record	SCR
Personal Health Record	PHR
General Practitioner	GP
Care Record Guarantee	CRG
Data Protection Act	DPA
Short Message Service	SMS
Accident and Emergency Department	A&E
European Union	EU
Role-based access control	RBAC
Public Key Infrastructure	PKI
Personal Health Record	PHR
Interoperability Toolkit of the Care Record Service	ITK
Open System Interconnection Reference Model	OSI
Clark-Wilson	CW
Transaction Programs	TP
Constrained Data Items	CDI
Public Key Infrastructure	PKI
Integrity Verification Procedure	IVP
Certification Rules	CR

1. Introduction

- 1.1.1. In this dissertation we consider the implications of sharing electronic patient information across organisation boundaries. Electronic Health Records (EHR) have gone into widespread use. EHRs can be a single systems in one organisation or a summary shared across participating organisations [HO10]. Other forms include a longitudinal and life long record for a patient pulled together when required from distributed locations. In addition there are investments in progress in development of Personal Health Records by Microsoft and Google [TA06], [GO10], [MI10] in which the patient controls access to the record and either adds and maintains their own record or health service provider organisation increment the record from their systems.
- 1.1.2. Each health care organisation is responsible for security of the health records that are generated and held to support care and for recourse should there be a need to establish liability. This responsibility continues wherever patient information is held. The legal framework for sharing patient information has a principle of sharing information on the basis of consent complicated by the need for an override in emergency and a number of exceptions.
- 1.1.3. Hospital Medicine is practiced in large complicated organisations in which confidential information moves freely along the pathway of the care. The clinical team includes many staff members who are non-Medical or professionally qualified, e.g. administrative support. A principle of implied consent is often cited in this context to justify access to confidential information.
- 1.1.4. This is a time of change for record keeping. In this dissertation a number of examples of EHR in the United Kingdom (UK) National Health Service (NHS) are considered in terms of consent and confidentiality. Examples will include the £12B Care Record Service (CRS) [NA06] in England, a number of provincial Summary Care Records (SCR), Personal Health Records (PHR) and more general extension of use of current systems including integration of systems from several organisation to provide a single service to the patient in one building (Polyclinic) [DH08]. Analysis of these arrangements reveals common approaches and weaknesses in terms of legal compliance. Academic security models are briefly reviewed to see what they can offer in addressing this challenge. A model is then developed based on Clark-Wilson and comparison is made of this against these practical examples. Conclusions are drawn on the development of consent and confidentiality functions

1.2. Aims and Objectives

- 1.2.1. In this dissertation we look at how the NHS is responding to the challenge of maintaining confidentiality and following the consent decisions of patients as information is shared across organisation boundaries. We develop a security model to address these challenges. The objectives are:
 - 1.2.1.1. Establish the UK legal basis and a definition for consent and confidentiality to share electronic health records,
 - 1.2.1.2. Review examples of shared electronic health record systems in the UK,
 - 1.2.1.3. Consider security services and functions relevant to consent and confidentiality and develop an appropriate security policy and model,
 - 1.2.1.4. Compare example security arrangements with this policy and model

1.3. Methodology

- 1.3.1. Methodology is based on literature review, case studies of London NHS organisations and interviews with people involved with set up and use of confidentiality and consent functions for the Care Record Service, Polyclinics and other developments.

1.4. Outline

- 1.4.1. Section 2 contains a literature review of EHRs, confidentiality and consent functions and associated security models. In Section 3 relevant aspects of the profession of Medicine and the UK legal framework are reviewed, Professional and Government Policy is summarised to establish the security requirements for shared electronic health records. Practical issues concerning patient records and information movements in NHS existing systems are introduced in Section 4. This sets the context for looking at examples of shared health record systems in Section 5. These include CRS, provincial SCRs, PHRs and Polyclinics. Problems in compliance with the legal framework are identified. In Section 6, a review of threats associated with shared records is undertaken, a security policy and a version of the Clark-Wilson model is developed. In the conclusion (Section 7) the practical examples are reconsidered based on the model.

1.5. Exclusions

- 1.5.1. In this dissertation the key concept considered is consent for sharing of a patient's record taking the perspective of the organisation employing staff rather than privacy for the patient. This is an important distinction as EHRs result in information being gathered together in one place. It is possible to argue against such aggregation as an unnecessary and intrusive risk to the privacy of patients [RA96]. In this dissertation such aggregation is a given and attention is given to how organisations can best meet their obligations to patients.
- 1.5.2. Articulation of the security model developed in this dissertation is in natural language rather than mathematical. This has the disadvantage of ambiguity and consequent lack of assurance.
- 1.5.3. Informed consent has a philosophical and complex legal aspect that is not considered in this dissertation. A simple assumption is made that it is possible to gain, record and act on the wishes of a patient.
- 1.5.4. Another exclusion is the subject of identity management. At most NHS service delivery locations the patient identifies themselves. Staff check this information with the contents of the system index. There are examples of record confusion and identity theft in the NHS but these represent a small proportion of patient records.
- 1.5.5. There are distinctions in the legal and policy position of consent for information for social care as opposed to health care in the UK; consideration of this is excluded.
- 1.5.6. The UK NHS provides services in the constituent provinces of England, Scotland, Wales and Northern Ireland. Most of the examples of shared health records are taken from England with one from Scotland and Wales. In this dissertation when NHS or NHS policy is referenced, this means for England. The legal basis for consent and confidentiality issues are common for all the provinces as there is little difference in the law of privacy.

1.5.7. The concept of Confidentiality in information security has a broad meaning of protecting a record from unauthorised viewing. Relevant services exist for protecting information in communication and at rest. Although there is limited reference to this diversity and depth of such services for the Care Record Services, this dissertation is mostly concerned with application functionality.

2. Literature review of shared use of electronic health records and associated security models

There is considerable academic literature on issues of consent and confidentiality for extended access to electronic health records and also for security models. In this Section a review is undertaken of this literature

2.1. Consent and confidentiality for extended access to electronic health records

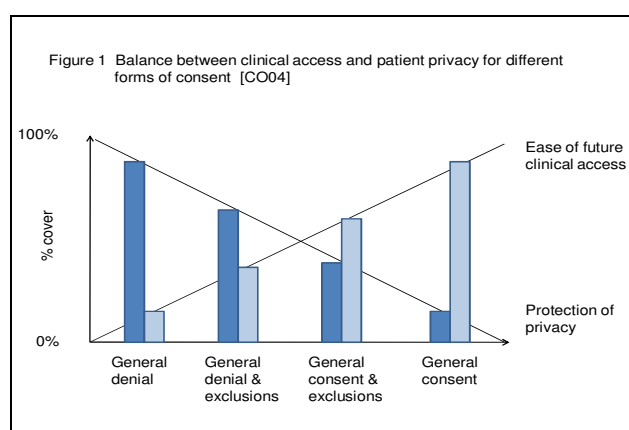
2.1.1. Noting the unlikely possibility of one organisation providing care for a patient in a life time and the resulting fragmentation of records across health care organisations, Mandl et al advocate assembly of the record at the point of care from wherever it is held [MA01]. To achieve this there is a need for standards in record structure and for patients to have control as to how their records are made available: -

“Giving patients control over permissions to view their record as well as creation, collation, annotation, modification, dissemination, use, and deletion of the record is key to ensuring patients’ access to their own medical information while protecting their privacy”

2.1.2. An expectation of privacy allows trust and improves communications between doctors and patients [HGJ99]. Without privacy the patient may withhold facts or avoid treatment through concerns with stigmatisation, loss of employment or insurance. With web and mobile services becoming standard, there is an expectation in the medical profession that patient’s records will be available and controlled by the patient [TF97]. Mandl et al identify six desirable characteristics of electronic medical records - see Table 1.

Comprehensiveness	The importance of a complete record of the lifetime of a patient and being available at the point of care
Accessibility	Care can be provided on a predictable basis or in emergency and should be universally available for research and public health purposes with adequate controls
Interoperability	Different computerised medical systems should be able to share data from multiple sources and in various formats
Confidentiality	Patients should have the right to decide who can examine and alter what part of their medical records
Accountability	Any access to or modification of a patient’s record should be recorded, visible and available to challenge by the patient, this requires use of strong authentication
Flexibility	Patients should have control over availability of their information for research including at a granular level to enable engagement with particular studies as well as more generally through anonymisation

- 2.1.3. All contributors acknowledge the need for emergency access in which consent controls are bypassed when, for example, the patient is unconscious. This function is open to abuse and must be carefully handled if security is not to be breached. Coiera et al present a trade off between confidentiality and accessibility – see Figure 1 [CO04]. If there is no emergency override then the record can only be viewed by the direct care team, similarly, if there is a general right of access then there is no privacy. The setting of this balance is a fundamental attribute and examples of open and closed systems will be discussed in Section 4 when we consider current systems in NHS organisations.



- 2.1.4. Coiera et al describe 3 types of consent function, the recording of consent wishes for a patient, an active acknowledgment of this status when a record is handled and the “gatekeeper” role, an active use of the consent to inform whether a system will allow an action, i.e. create, view and edit [CO04]. Embedded objects containing the consent status of each item of data (e.g. document) or, more practically, episode of care could be created as a standard.
- 2.1.5. In reviewing early use of the Summary Care Record Greenhalgh et al identify usability as critical to uptake in the busy Accident and Emergency departments [GRb08]. The concept of “permission to view” is introduced at the point of care as alternative to reference to a record of consent. The advantages of this approach are immediacy and ease of explanation for both patient and members of the clinical team. If the patient is present the principles of informed consent are not thought to have been lost through use of this simplification (see Section 5). Greenhalgh stresses the need for the development of confidentiality and consent functions with social and workplace considerations rather than a technical perspective of operation of the functions within systems [GRb08]. E. Coiera et al add that in a pressured work context a new task must replace an existing one [CO04]. Staff have to negotiate the complexity of explaining consent to patients and if use of the associated EHR system is onerous, this may lead to avoiding the system or circumventing the consent function.
- 2.1.6. Anderson cautions against consolidation of repositories of electronic records at a wider level than that of current organisations because of the consequent and new risks of aggregation (see Section 6) [GRb08]. He advocates making records available as required from distributed locations. Tang et al note the growth of Personal Electronic Health record (PHR) [TA06]. PHRs provide data, knowledge, and software tools, which help patients to become active participants in their own care. When integrated with health service provider EHR, they offer further benefits. Lewis et al note the potential for use of the patient controlled PHR in social networking and new ways to participate and collaborate [LE05].

2.2. Standards for EHR

2.2.1. There are a series of standards being developed for EHRs, for the most part, in Europe as part of the CEN initiative [CE10], [Ka06]. These include requirements for representing and communicating faithfully the meaning intended for a particular entry, and support for analysis for professional and organisation purpose. Other significant components are content value (e.g. formal representation of data types), clinical interpretation context (e.g. presence, absence and severity) and care process context (e.g. cause and effect, request and result). In terms of consent: -

“communication of EHR entries between professionals working on different sites, whilst respecting the privacy wishes of individual patients incorporating medico-legal constructs”

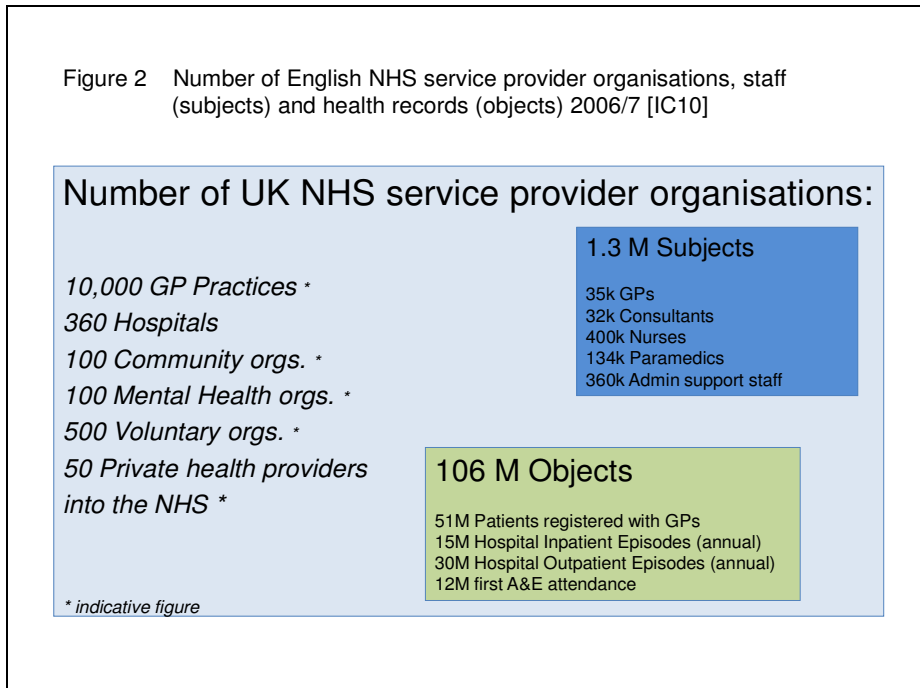
2.2.2. At a communication level there is considerable consistent use of standards. Digital Imaging and Communications in Medicine (DICOM) is an international communications protocol standard for representing and transmitting radiology image standards [NE10]. In addition International Organization for Standardization's (ISO) Technical Committee (TC) on health informatics ISO/TC 215 works on the standardization of Health Information and Communications Technology (ICT), to allow for compatibility and interoperability between independent systems [IS10]. Health Level Seven (HL7) has gone into widespread use to support clinical messaging [HL7, 2010]. For the most part, current use of HL7 messaging is v2 which has been developed pragmatically and does not include handling of the meaning of terms.

2.2.3. Kalra concludes that effective standards are not yet available for EHR, a significant problem being preservation of clinical meaning across heterogeneous systems [Ka06]. Systematized Nomenclature of Medicine - Clinical Terms (SNOMED CT) is a systematically organized collection of medical terminology covering most areas of clinical information such as diseases, findings, procedures and microorganisms [SN10]. It allows a consistent way to index, store, retrieve, and aggregate clinical data across specialties and sites of care. It also helps organise the content of medical records, reducing the variability in the way data is captured, encoded and used for clinical care of patients and research. SNOMED is not in widespread use outside of laboratories where there is significant automation. In the absence of standards for EHR, summaries and subsets of EHR are shared as designers and suppliers implement in haste with limited budgets [Ka06]. In later Sections 4 and 5 UK examples are considered.

2.3. Security models relevant to electronic health records

2.3.1. A security model and policy for electronic health records must be focused in the application layer of the Open System Interconnection Reference Model because of the need to capture the complexity of circumstance and meaning that has to be handled (e.g. is the user of the system providing direct care to the patient?) [GO06]. As a result assurance is difficult and may be impossible. A security model for EHR has two points of control: users as subjects and records as objects. Figure 2 illustrates the relative scale of subjects (over a million) and objects (over 100 million episode records a year) in England. Subjects access objects in over 10 thousand organisations.

Developments in confidentiality and consent functions to support wider sharing of electronic health records in the UK



2.3.2. The first security models that went into mass use were that based on Bell-LaPadula (BLP) [BE96], [GO06]. The BLP can be summarised as supporting a security policy linking multilayer security marked objects with subjects with different levels of access. Table 3 illustrates security classification for the UK. Whilst there is a multilayer Government scheme, for the health records in the NHS only one layer, Confidential, is available. It is possible to add layers either on the basis of what concerns a patient (see CRS Section 5) or on the basis of clinical speciality (e.g. sexual and reproductive health). All Clinicians could be given access to the confidential layer with a smaller number given access to the second layer. A care association (direct provision of care) could be added which could add compartments or departments within organisation and organisation boundaries with certain groups of clinicians (such as A&E) having access across boundaries. A variation of this would be to allow cross organisation access on a risk basis for all [CR07]. If there is experience of abuse of consent as information is made available across an organisation boundary then this transfer could be stopped.

Developments in confidentiality and consent functions to support wider sharing of electronic health records in the UK

Table 2 Security marking of NHS electronic health record [DH10]		
Data Protection Act	UK NHS security marking of electronic health record	UK Government security marking
		Top Secret – national / international significance
		Secret – national / international significance
Sensitive - to be processed according to a stricter set of conditions, in particular any consent must be explicit	NHS Confidential - appropriate to paper and electronic documents and files containing person-identifiable clinical or NHS staff information and other sensitive information.	Confidential - effects of leakage include considerable infringement on personal liberties, material damage to diplomatic relations, or to seriously disrupt day-to-day life
Personal - data about a living and identifiable individual	NHS protect – discretionary marking that may be used for information classified below NHS Confidential but	Restricted - effects of leakage include significant distress to individuals, adversely affecting the effectiveness of military operations, or to compromise law enforcement
		Protect
Unclassified, non-personal	Unclassified	Unclassified

- 2.3.3. A problem for any access control mechanism based on hierarchy is that clinical support staff are an essential part of the clinical team and also need to access the confidential record (see Section 4), e.g. administrative staff booking appointments. A model based on hierarchy could degrade in use as there could be justification for many staff to see the confidential layer.
- 2.3.4. BLP models are used, for the most part, where the number of subjects is significantly greater than objects [RA96]. There are 10 times the numbers of Objects compared to subjects in the context of health records. In the context of health records and it is more appropriate to place controls on object rather than on subjects.
- 2.3.5. An adaptation of the BLP model of relevance to health records concerns screening of access based on conflicts of interest, termed “Chinese walls” [BN89]. In this variation of the BLP model, subjects could be Clinicians and objects parts of health records. Records for a particular department or organisation could be defined as a datasets with conflict of interest classes for each object. A clinician cannot view records marked as belonging to another organisation because this is a conflict of interest. When staff move a new association of department or organisation can be given to them opening up access to parts of record previously withheld.
- 2.3.6. Another model of relevance is that of Clark-Wilson [CW89]. This was developed to maintain information integrity and has other characteristics which include a focus on access control, separation of duties, audit trails and external consistency. It is a descriptive framework and can potentially be seen as supporting a wider set of security policies and contexts. Health records can be seen as being distributed horizontally across multiple organisations. An example of a security model for health records based on the Clark-Wilson concept is that of Andersons’. Anderson placed access control lists against each record and use of audit trials to make access information available to patients and third party, potentially a professional body [RA96].

2.3.7. It is possible to use any of these models for electronic health records. In this dissertation the criteria used to select one are:

- the numbers of objects compared to subjects,
- the horizontal character of health records as existing within many organisations
- without a simple layered security classification and
- the need for a flexible definition within a framework

A variation of the Clark-Wilson model is used with detail given in Section 6.

2.4. Conclusion

In summary, patients must be given choice as to how their health information is shared. An emergency override is necessary and use of consent functions is a compromise. As a consequence there has to be accountability for exchange of health information. Sharing of health records should be on the basis of standards and without these pragmatic exchanges of summaries are likely to be an interim step. In terms of security models, BLP, Chinese Walls and CW could be applied. In this dissertation the CW is selected.

3. The UK legal framework and a definition of the key concepts for confidentiality and consent for sharing health records

This dissertation is focused on the challenge of maintaining obligations to patient as information is shared across organisation boundaries. In this section relevant characteristics of the practice of medicine are introduced, the English legal context, government policy and professional guidance are considered and the key concepts of confidentiality and consent that define these obligations are summarised.

3.1. Medicine

“All that may come to my knowledge in the exercise of my profession or in daily commerce with men, which ought not to be spread abroad, I will keep secret and will never reveal.”

8TH sentence of Hippocratic Oath, translated into English [HO10]

Medicine and allied professions provide the context for electronic health records. In this 6thBC century expression we can see confidentiality recognised as one of the ethical foundations of the profession. The practice of Medicine 25 centuries ago in Greece may have been a solitary affair, today it is organised into specialist teams in multiple organisations [PO99].

3.1.1. Patient information is rapidly shared as required to support clinical process. Referral to specialists within and in other organisations is driven by the requirement to diagnose and treat the patient. Administrative staff are part of the clinical team and need to have access to clinical information. The business process that underpins the provision of care can involve staff in teams remote from the point of care such as pathology and radiology.

Stephen Elgar

- 3.1.2. Different models of care are identified [CR07]. The first is an engineering model; the patient has a problem to be fixed. This is seen in specialisms such as pathology where the patient provides a specimen remotely, processing is automatic and there maybe no patient contact. The Pathologist oversees quality and supports interpretation. The second model is that of a healing relationship between patient and clinician, an encounter in which there is mutual understanding, respect and trust. This can be seen in General Practice (GP) where contact is personal and long term. The third is of a contract between clinician and patient with rights and duties for both parties. All three models coexist. In terms of confidentiality, in the second model, the patient could be asked their feelings on how their information should be shared and in terms of the third, patient's rights and the duties of care of the team can be invoked. An expectation of privacy allows trust and improves communications between doctors and patients. If trust is lost then the patient may withhold information or withdraw from treatment [HGJ99]. There is also an assumption among Clinicians of a move toward greater involvement of the patient in understanding health, illness and decision making concerning their care [TF97].
- 3.1.3. In summary, confidentiality in Medicine has a practical and ethical basis, it's preservation is problematic given the scale of specialism, number of teams and the proportion of non-professional staff who support clinicians. The speed and complexity of flow of information to support care presents a challenge to any system elements which are intended to limit movement of the health record.

3.2. The UK legal context for sharing healthcare records

- 3.2.1. Heath care organisation seek to follow polices and procedures motivated by the requirement for legal compliance. In the UK the legal framework for confidentiality of electronic health records has a number of parts. Common Law articulates a duty of confidentiality in any encounter. The Data Protection Act 1998 provides a framework of rights for patients with informed consent as the basis for any sharing of information. Organisations are registered as Data Controllers and have obligations to data subjects. The purpose of information use must be stated, in this context the provision of care. Such statements often take the form of posters and leaflets. For any other purpose permission must be gained from the patient or the information must be anonymous (see Figure 4). There are legal exceptions to this, e.g. the occasional need to protect the public from a violent patient. Additionally, The Human Rights Act provides a right to privacy and a series of other Acts give further detail. These are summarised in Table 4.

Table 3 Summary of UK legal framework for confidentiality of health records [DH07] [DH03] [GM09]	
Common law	Duty of confidentiality between clinicians and patients; maintenance of frank discussion is dependent on trust.
Data Protection Act 1998	<p>Individuals have rights and healthcare organisations have duties of care which include the need to limit use of information to the purpose for which it was collected and for sharing to be based on positive consent. Patients may make a Subject Access Request to view their record and have it corrected if inaccurate.</p> <p>Exceptions to this consent are identified through legislation (e.g. reporting of an infectious disease) or if there is an overriding legitimate reason (e.g. the Public good in the case of a potentially violent patient). Organisations are required to have adequate security measures including technical (e.g. for electronic information access control and firewall protected networks) and organisation methods (e.g. staff training).</p> <p>Each health care organisation is registered with the Information Commission Office as a Data Controller. If personal or confidential information is lost then the Data Controller is identified and held to account. Fines of £500k have been introduced [ICO10].</p>
Human Rights Act 1998 (Article 8)	Patients have a general right in respect of privacy including family life, home and correspondence. This is subject to restrictions such as national security. The UK Government is committed to maintaining compliance of UK law with the Human Rights framework.
Other relevant enabling acts:	
Sexual Health Records Act NHS (Venereal Diseases) 1974 Regulations	Allows patient anonymity to encourage service uptake. Disclosure of information for contact-tracing is supported in the case of sexually transmitted diseases. This disclosure can only be by a Doctor or someone working on instruction. It forbids disclosure to an Insurance company. GPs are not routinely informed, although the patients are encouraged to allow this.
NHS Act 2006	Allows the common law duty of confidentiality to be set aside in specific circumstances, e.g. Section 251 for research or management collection of personal information for the common good. The NHS exchanges datasets between service provision (e.g. Hospitals) and commissioning organisations (e.g. area-based Primary Care Trusts) – see Section 4, Secondary Use Service. These datasets contain patient information without any form of de-identification. Managers have no right to see confidential information as they have no relationship with the patient based on clinical care.
Health and Social Care Act 2008	Exemption to consent can be sought through review by National Information Governance Board, e.g. a national audit for a disease such as diabetes. Without a survey of GP records, an accurate picture cannot be gained from other sources. The survey must be as complete and representative as possible.
Table 3 Summary of UK legal framework for confidentiality of health records	

(continued)	
Others	There are special permissions within 'The Health Service (Control of Patient Information) Regulations 2002' Statutory Instrument 1438 which gives the UK Health Protection Agency generic permission to collect patient identifiable information under certain conditions, e.g. HIV infection. There was a legal challenge to this practice at the time of the initial HIV outbreak. For reasons of Public good it was agreed that patients could not stop the reporting of this condition. This has allowed a tracking of the progress of the condition.

3.2.2. A patient or group of patients can take legal action against organisations on the basis of this legal framework. For organisations and patients there are a series of NHS policy and professional guides that simplify this legal framework [DH03], [GM09], [DH07], [NI09]. An example statement for patients on confidentiality illustrates this: -

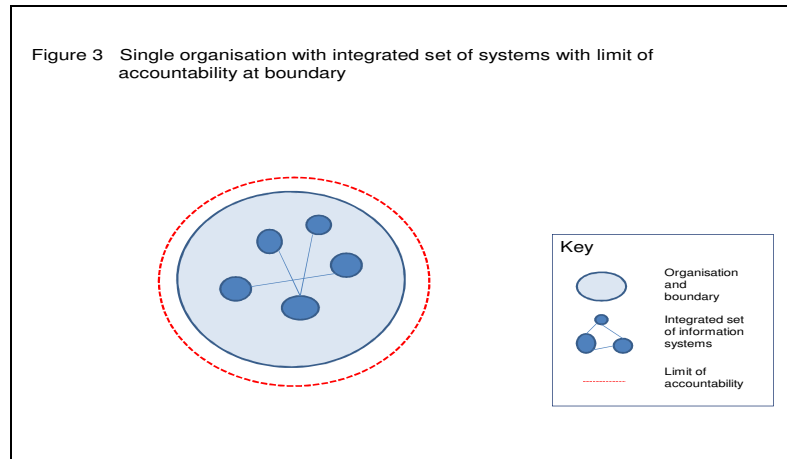
“You should make sure information is readily available to patients explaining that, unless they object, personal information about them will be shared within the healthcare team, including administrative and other staff who support the provision of their care.” [DH03]

3.2.3. We have noted the scale of clinical teams and the speed and complexity of the movement of patient information to support care (3.1.1.) and this quotation introduces the principle of implied consent within an extended care team and is seen as critical to the function the NHS. The team should be seen as a fluid entity encompassing clinical need. Within the organisation implied consent operates, typically, with no controls other than through the judgement and professional responsibility of staff. The assumption is that informed consent is only required when information moves across the organisation boundary. The referral process across organisation boundaries is seen as having consent as an integral element, e.g. for the treatment of cancer practical arrangements to attend another facility mean that the patient is aware of the movement of information.

3.2.4. One complication to implied consent is co-location of staff employed by other organisations. This is typically handled by procedural controls such as partnership agreements between the organisations, honorary contracts, acceptable use policies and training. In addition there are some specialties for which there are particular sensitivities and exceptions, e.g. sexual and mental health (see Section 4).

3.2.5. Figure 3 illustrates the assumption of the organisation boundary as a consent constraint. This may seem simplistic but it is the legal construct. Access rights for internal IT systems are used to provide and control access. Where possible a concept of care relationship is the basis of granting or denying access, where not possible there is open access if there is clinical or business justification. In Section 4 we will look at the practicalities of information sharing across this boundary.

Developments in confidentiality and consent functions to support wider sharing of electronic health records in the UK



3.2.6. Direct patient care includes administrative tasks where there is clear and relevant benefit such as clinical audit of the quality of care, booking appointments and management of waiting times. Where patient information is used for any purpose which is not concerned with direct patient care, it must be de-identified so that the identity of the patient cannot be inferred. This is illustrated in Figure 4 and we shall see in Section 4 that the ease of data extract and reporting from systems has led to a culture a problem with confidential patient being available outside the team providing direct patient care.

Figure 4: De-identification of secondary use information

People	Confidentiality Controls	
Patient present with clinical and administrative staff	Informed & implied consent	Care Team
clinical and administrative staff (patient absent)	implied consent	
Who help investigate any patient concerns or complaints about your healthcare;	access to full patient details	Patient absent
Who check the quality of care (such as a clinical audit);	<i>access control, aggregation, anonymisation and pseudonymisation</i>	
Who protect the health of the general public		
Who keep track of NHS spending		
Who manage the health service		
Who teach healthcare professionals;		
Who help with research.	Consent required for access to full patient details or use of anonymisation It is also possible to gain exemption	

3.3. UK NHS Policy guidance

3.3.1. A security management regime has been developed to simplify these obligations for NHS organisations based on ISO/IEC 27002, the Information Governance Toolkit [DHf10]. From 2010 each organisation must provide an audited public assurance statement. In addition, the NHS Care Record Guarantee [NI09] is published as a statement of patient rights. Table 5 lists the consent obligations in this Guarantee. The obligation of health organisation for Subject Access Requests (DPA 1998) has been extended to include the identity of staff and justification for access to the health record.

Developments in confidentiality and consent functions to support wider sharing of electronic health records in the UK

Table 4	UK NHS Best Practice Guide for Consent obligations for healthcare organisations using the Care Record Service [NI09]
	Allow patient to control whether the information recorded about them by an organisation providing them with NHS care can be seen by other organisations that are also providing them with care;
	Show only those parts of patient record needed for patient care;
	Allow only authorised people to access patient record;
	Allow only those involved in patient care to have access to records about them from which the patient can be identified, unless the patient gives permission or the law allows;
	Allows use of information about patient healthcare, in a way that doesn't make patient identity known, to improve the services offered or to support research;
	Keep a note of everyone who accesses a patients records; and be operated in line with internationally approved information security standards.

3.3.2. Clinical oversight of electronic record keeping, access control decisions and management of the movement of patient information is achieved through giving responsibility to a senior clinician [DHe10]. In a large organisation such as a Teaching Hospital, this is a considerable task and there is usually a team of support staff.

3.3.3. Also of relevance to electronic health records, is an NHS policy that demographic personal details such as name and address are not confidential. Accurate identification of a patient using a shared index is an essential foundation for an EHR – see Sections 4 and 5. It is not difficult to find address information in the UK; however, there are risks to some patients e.g. people fleeing a violent partner and those in witness protection schemes. For such individuals there is an arrangement for the demographic record to be flagged so no address detail is returned and an alert is generated whenever it is accessed. A more general risk is that of inference. If a patient can be associated with a particular health organisation, and perhaps specialty, assumptions can be made about their state of health and any treatment they may be having. (There will be further discussion of security mechanisms to address inference in Sections 4 and 5).

3.4. Conclusion

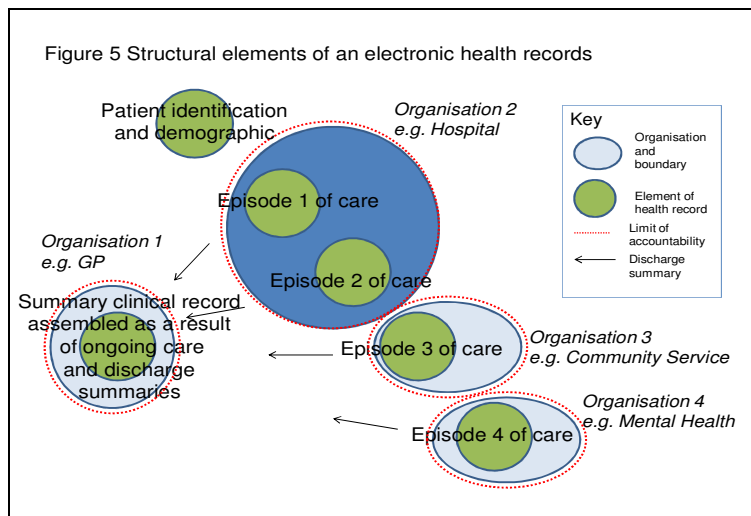
3.4.1. Key concepts for consent and confidentiality are active consent for information sharing outside of the team providing care. Patient care pathways can be complex and varied and an assumption of implied consent means that any staff not in direct patient contact must sometimes access records. Implied consent does not apply across organisation boundaries. In addition, for the organisation there is a requirement for appropriate security management. Clinical oversight of confidentiality including appropriate authorisation of access to health records is provided by the role of the Caldicott Guardian. Health provider organisations are accountable to patients in a number of ways. They must satisfy Subject Access Requests (DPA 1998) and be able to state which staff member has accessed a record. NHS organisations must hold information securely. Compliance assurance statements and any significant data loss incidents must be published to ensure commitment and transparency. Recourse to the legal system is available to patients but happens rarely. Finally, a formal guarantee to be patients has been published by the Government in the context of development of shared records.

4. Practical issues of confidentiality and consent for existing systems in NHS organisation

Practical issues concerning health records and information movements in the NHS are considered in this Section 4. Although the focus for Section 5 is the Care Record Service, CRS holds the national patient index and provides a number of other services such as referral booking for all NHS organisations and so is introduced in this section.

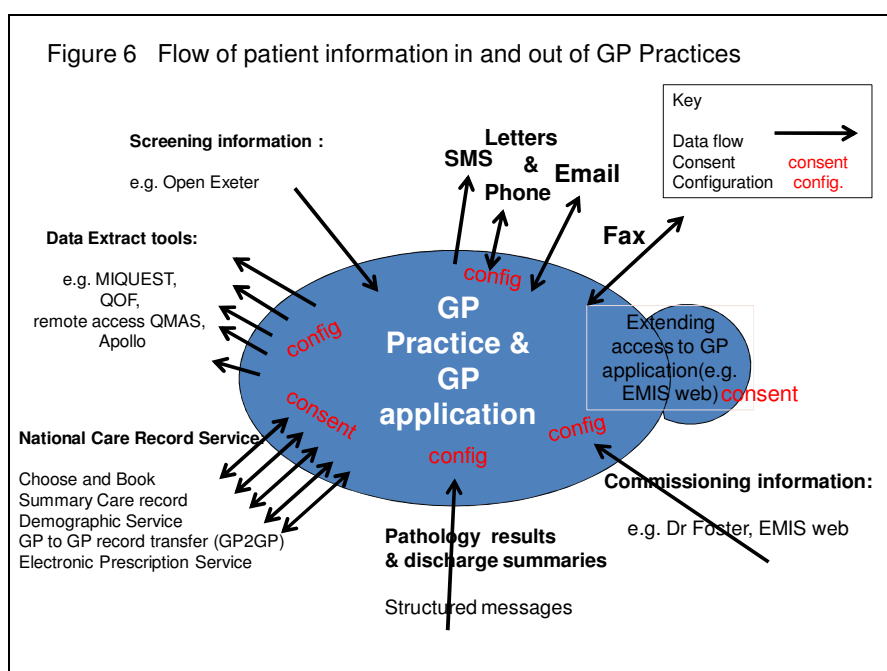
4.1. Healthcare organisations and electronic health records

- 4.1.1. Clinicians and their support teams have a duty of care to patients which includes record keeping. Health records are primarily kept to support the provision of care and to support questions of liability should they arise [CO02]. Patient information is also used to maintain the quality of care through peer review and clinical audit and for the organisation for recovery of cost. Records are created and maintained by teams of clinicians and support staff with the employing organisation as the custodian - see Data Controller 3.2.1 and Caldicott Guardian 3.3.2.
- 4.1.2. To access NHS healthcare a patient registers with a GP. The GP and her team provide primary care and act as a gatekeeper to more specialised services including Hospitals by a process of referral. Services are also directly available through the phone (NHS Direct), GP out-of-hours services and Accident and Emergency (A&E) departments.
- 4.1.3. A traditional arrangement was for each department within an organisation to hold a separate paper record for the patient under its care. This is illustrated in Figure 5; four organisations provide care for a patient. Care has been initiated by the GP and a summary of each episode of care has been returned to the GP. Each organisation has accountability for the records which resides within its boundary. Transfers of information are stated in contract or through custom and practice. This fragmentation is an issue. In an emergency the absence of information can be a significant problem. The development of Summary Care records and extended access to the GP record addresses this issue (e.g. Hampshire Health Care Record and the Care Record Service Summary Care Record - see Sections 5).



Developments in confidentiality and consent functions to support wider sharing of electronic health records in the UK

4.1.4. Electronic health records hold an index of patients that contains address and contact details, this is termed the demographic component of the record. Demographic items (see 2.3.3) are treated as non-confidential. A CRS national index is shared across health care organisations (see Section 5). Most systems support scheduling of care (waiting lists and appointments) and a summary of some description. A central paper record often continues to exist alongside the electronic record. Many health organisations are paperless or paper-light depending on the electronic health record with attachment of scanned documents. In the UK this is particularly true of General Practitioner (GP) Practices.



4.1.5. All GPs have a single electronic health system with the capacity to record a detailed health record based on a national specification. Figure 5 illustrates the flow of information to and from GP Practices. The patient index is shared through an interface with an associated set of applications (the Care Record Service – see Section 5) that also provide functions of referral (Choose and Book), prescriptions (Electronic Prescription Service) and transfer to record to other GP Practices (GP2GP). FAX, emails SMS and are also used to communicate. Scanned documents are an important addition to the structured record. Pathology and other investigation results are available through structured messages which can be automatically incorporated into the record. A series of data extract tools actively export structured data sets, for the most part, in anonymous format. Consent mechanism for the Care Record Service and for extended access to the GP application will be discussed in Section 5; other information flows are controlled by system configuration and supported by an assumption of implicit consent for referral and discharge notification.

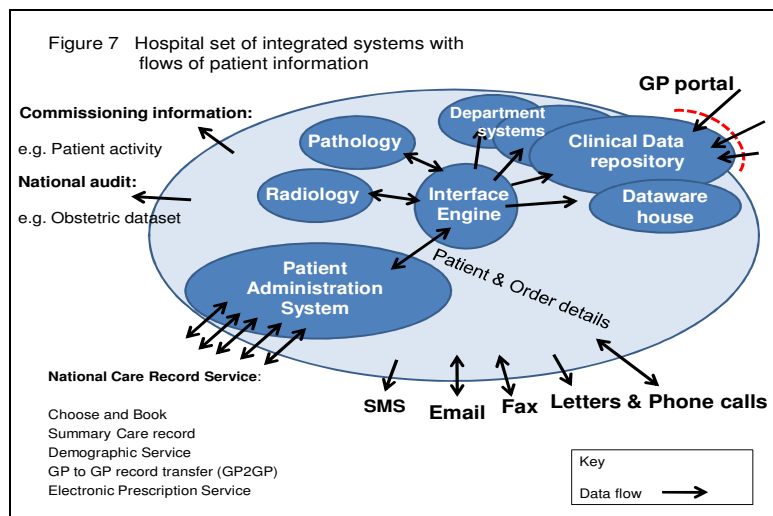
4.1.6. Hospitals have a set of integrated systems from many suppliers built over a 30 year period, integrated to varying extents. Figure 6, illustrates information flows of patient information. An NHS data model defines common outputs from systems [DHd10]. These outputs include a shared activity statement for payment and national audit datasets. The main system for recording patient activity is the Patient Administration System (PAS). A local patient index is maintained integrated with the national index dynamically or through overnight batch interface. Scheduling, admissions, discharge and transfer information is passed across from PAS to department systems. Ordering, results reporting, a clinical repository and automated

Stephen Elgar

Developments in confidentiality and consent functions to support wider sharing of electronic health records in the UK

discharge summary functions are typically available. Electronic prescription services are expected to be available shortly [DHC10]. Communication outward of patient information takes a number of forms from automated structured messages for results to GPs, letters, SMS, phone calls. There is often a portal for GPs and clinicians outside the Hospital to allow the Hospital EHR to be viewed and to pick up documents e.g. discharge summaries.

- 4.1.7. Few of these integrated set of systems have sophisticated security functions. If a patient requests for their care to be provided without an electronic records or for a constraint to be placed on movement of their information this is not usually possible. Some organisations state that an electronic record will be held and shared within the organisation, an inference being patients should go elsewhere if they do not want one. This is not yet a general position and a Court Order can be sought to have a record removed if distress can be proven.



- 4.1.8. Health record fragmentation can be seen to support confidentiality for some services, e.g. sexual health. A number of local approaches are used to provide confidentiality for such specific services. Mental Health services are provided by 76 separate organisations in England (March 2010). When care is provided to staff common practice is for attendance at a different provider organisation. Emphasis is placed in staff training on maintaining confidentiality of records. Local pseudonym procedures are sometimes present. This is not possible with CRS where the national index is shared. Sexual Health services can be based in the Community or in Hospital and are often in separate locations. Use of bogus identities and pseudonyms by patients are encouraged to foster uptake of services. Communication with GPs is a choice offered to patients. Pathology services use for sexual health clinics is often based on a unique system registration from which identity cannot be inferred.

4.2. NHS Policy on consent and confidentiality

- 4.2.1. The Care Record Guarantee (CRG) is a commitment to patients on how health records are handled and applies to all patient records for NHS funded work, the majority of which, at the start of 2010, is recorded on non-CRS systems. Significant issues in compliance with the CRG are identified as lack of understanding and commitment of the executive team. There is also weakness in capacity of specialised information security skills associated with networks, firewalls, and malware management and use of audit trails. As stated previously (4.1.4.), there is an absence of flexibility in handling electronic health records based on the security

functions of existing set of integrated system. In addition, there is excessive use of primary information for secondary purposes with insufficient de-identification [CQ09].

4.3. Conclusion

- 4.3.1. Most health service providers are limited in their capacity to support the wishes of a patient who does not want their information to be shared. Design functions of most existing systems are limited to access control based on username and password and audit. Use of audit system logs often requires outside skills. Integrity and provenance of information is assumed and rests on its location and context in locally controlled systems with reference to audit trails if there are disputes. For both GPs and Hospitals, notwithstanding the simplicity of consent and confidentiality functions, patient information is both imported and exported. For the most part this precedes and follows the carepathway of the individual. In addition considerable anonymised secondary use of GP information is made outside the GP Practice as this is a rich source of clinical information. The largest single transfer of primary patient information for secondary purposes is the export of activity dataset from Hospitals to the commissioning organisations. This Secondary Use Service (SUS) has a Section 251 exemption from the DPA 1998 due to be closed in 2011.

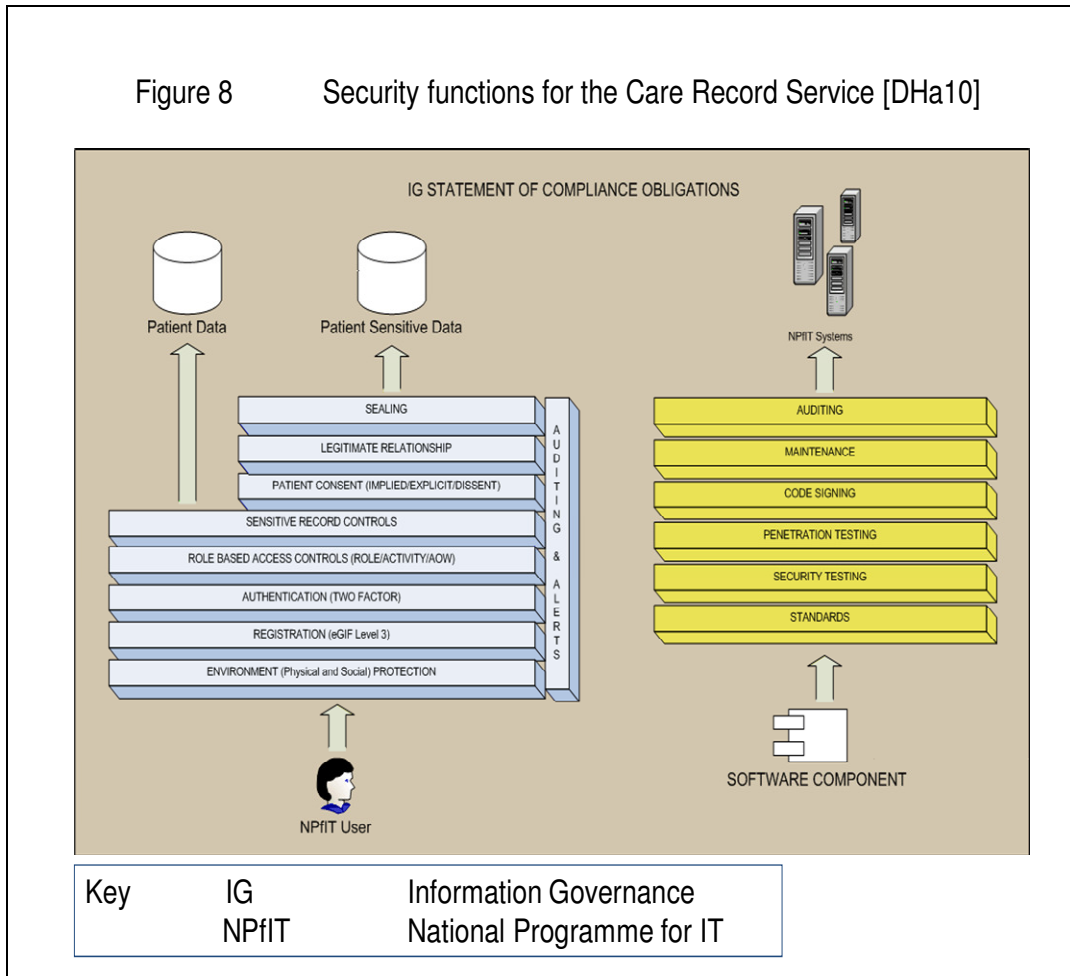
5. Consent and confidentiality functions for NHS Care Record Service and other examples of shared records

In this Section, based on published materials and interviews, consent functionally for CRS is considered. The English NHS CRS is intended to provide access to health records whenever and wherever required. Requirements for functions to support consent and confidentiality were designed to address this challenge. There is now widespread use of the CRS in parts of England. Plans for further development are available. In the second part of the Section a review is made of other EHRs in UK.

5.1. NHS Care Record Service

- 5.1.1. A national programme was launched in 2002 to specify, procure and implement a set of systems to support service modernisation. Two levels of system were to be developed: a national spine and a set of local systems linked by messages within a single security domain. Spine services a upgraded national patient index with a clinical summary care record and include authentication and other services such as as Choose and Book to support referrals, Electronic Prescription Service and a patient portal HealthSpace. Each NHS workplace has a local system to provide direct support for care. Provision of Picture Archiving and Communications System (PACS) was included.

Figure 8 Security functions for the Care Record Service [DH10]



5.1.2. Security measures of CRS applications are illustrated in figure 8. A set of software controls include code signing, security testing and controlled maintenance, penetration testing and security audit. Application features include user registration and strong authentication, role-based access control with an additional attribute of area of work, legitimate relations which allow a differentiation of staff in terms of the care relationship with the patient. There are consent choices for patients, sealing of particularly sensitive information and alerting from audit trails.

5.1.3. All access to CRS application is on the basis of two-factor authentication and digital signatures are used for some data items (e.g. prescription). A distributed Registration Authority was set up in each NHS organisation. 800k users are currently registered as of March 2010. An interface between the electronic staff record and the smartcard software is due to be implemented shortly.

5.1.4. A national definition for role-based access with 50 options has been put into use with the intention of unified business functions across all clinical areas.

5.1.5. Legitimate relation functionality was developed to allow certainty to be given to the team that provides care to a patient. This is based on a configuration of work groups created for, and potentially, across organisations. All users of the system are given membership of one or more work group. Once authenticated, when a CRS user seeks access to a patient record, a check is made of whether the group attribution signifies this as appropriate. A dynamic relationship between application workflow and group membership supports the relationships of staff and patient records.

Stephen Elgar

Associations between patients and legitimate relation groups would age and cease at some time after discharge. A GP Practice might have a single work group with all staff members able to access all records. A Hospital might have a work group for each department with other cross-organisations work groups. As a patient attends the A&E department the CRS workflow creates an association between the patient record and the A&E work group. In this instance if the patient only visited A&E no other staff apart from on call teams, pathology, radiology and other investigation services (who belong to the all-hospital group) would be able to see the record. If the patient is referred to a clinical team, referral would create a relationship for members of the group associated with the team. Details of use of the system by individuals would be noted in an audit trails with alerting functions available to warn of inappropriate access.

5.1.6. Consent options began as a simple choice across all CRS systems:

- explicit consent
- implied consent – for any patient who did not express a view
- dissent to share

In prospect of launch of the Summary Care Record further choices were added for this application:

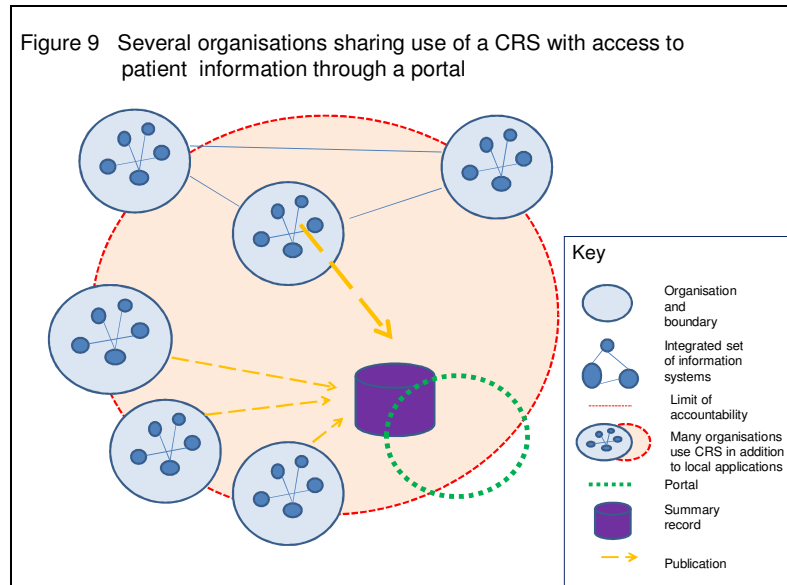
- store and don't ask
- store but always ask to view
- don't store,

Following review of initial use a simplification was made to use of a “permission to view” question to patients at the point of care [GRa08].

5.1.7. Sealed envelopes were to be developed for sensitive records. These were intended to allow parts of the record to be sealed by clinicians on behalf of patients. Seals could then be opened by a small number of clinicians. Final specification of this concept has never been agreed. Some of the problems in gaining agreement include the override. If there is indication of the presence of a sealed envelope there follows an argument that access will always be sought in emergency and if there is no indicator that this can be seen as creating clinical risk.

5.1.8. In summary, a single set of application-level controls support consent and confidentiality across the set of CRS applications. All participating organisations use patient record systems in addition to CRS. The single patient index holding demographic records and a unified code set for the NHS in England are all within CRS. (This index is linked to Scotland, Wales and Ireland). Some English NHS organisations have CRS as the main patient record system. See Figure 9, all participating organisations are obliged to share a commitment to the rules of the CRS security domain.

Developments in confidentiality and consent functions to support wider sharing of electronic health records in the UK



5.2. Experience of use

- 5.2.1. Since 2006 CRS systems have gradually gone into use. In London for example (March 2010), 6 of the 30 hospitals, 28 of the 31 Primary Care, 8 of the 10 Mental Health providers and all GPs have enabled system following upgrade of the existing 1500 Practices. The Summary Care Record is going into use within 18 months. The SCR in England currently holds 1.25 records of 50M patients registered with GPs. Some 60% of referrals to hospital are now placed using the Choose and Book application and 40% of GP prescriptions by the Electronic Prescription Service.
- 5.2.2. Strong authentication is standard across CRS but the original concept of a unified service for legitimate relations, role-based access, alerts and audit has not been achieved. Instead use is made of the functions of the applications that make up the CRS set. Consent functions have grown in complexity without offering greater granularity of control of access to the record. For example, in London there are 4 consent function that could be set for a patient illustrated in Table 6.

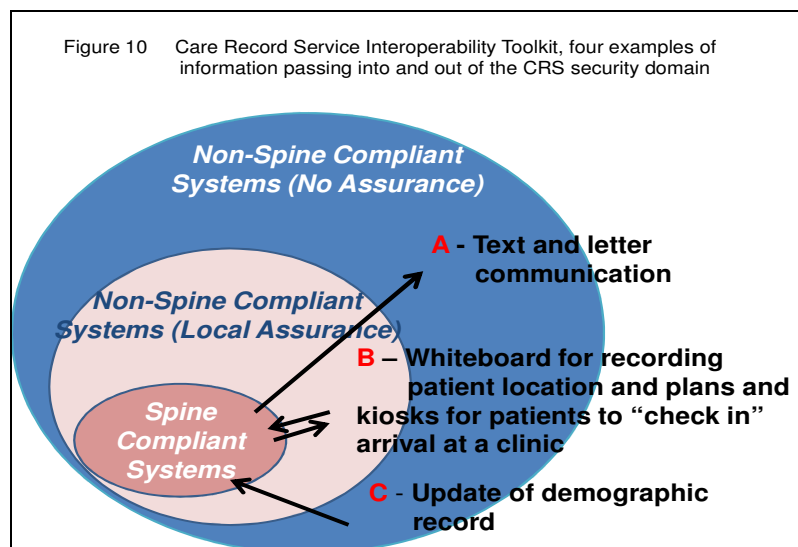
Table 5 Care Record Service consent functions in London			
National demographic record	National summary care record	National summary care record	Local Care Record Service
A flag can be set by GPs to limit response to query to index (NHS number) and name and excluding address	Permission to view asked at contact with the out-of hours service or attendance at emergency department	Store or don't store the summary, this flag is set by GP Practice staff and enables load of the summary record (active medications, contraindications, allergies & documents such as care plans) ; default position is store	Share or don't share flag will be set by clinical or administrative staff and will enable viewing of records between Local Care Record Service instances (not yet in use) In addition, in London an application to support a Single Assessment for Older People is used on the basis that a record is not created unless the client consents.

Developments in confidentiality and consent functions to support wider sharing of electronic health records in the UK

- 5.2.3. There is now active, limited use of the Summary Care Record in some parts of England. These are problems with usability, availability and integrity. The system prompts for the patient to be asked “permission to view” whenever the application is used which could be several times on one visit to A&E; staff are reluctant to ask the patient the same question repeatedly. As a result, the consent functions act as a barrier to use. SCR is currently used as a standalone system. It will soon be integrated with the A&E and Out-of-hours systems which will make use more attractive. Currently, any update from the GP systems has to be actively initiated by Practice staff rather than being automated.
- 5.2.4. HealthSpace, the patient portal is limited in functionality at present allowing the patient to record health facts and also acting as a signpost to NHS services.
- 5.2.5. Although all CRS local applications are linked with the national demographic service, local registration is permitted for sexual health services. This means that the former practice of pseudonyms can continue. If this option is selected for a patient, consolidation of this episode of care with the long term record (e.g. GP-held) is not possible.

5.3. Further developments

- 5.3.1. CRS Suppliers have been slow to develop compliant applications and to respond to changes in business and clinical practice. Many NHS organisations have chosen to stay with existing applications which are tuned for their particular needs. Although there is a process for any supplier to gain CRS accreditation, there has been little uptake of this option. CRS is perceived to be a monolithic security architecture and a consequent isolated island of patient information. In response to this, an Interoperability Toolkit (ITK) has been developed. This enables applications to be linked to CRS to support rapidly changing business requirements – see Figure 10. Extended CRS use through ITK is based on application to application security with a varied approach to identity management. New applications coexist with CRS in a private NHS network with a controlled and relatively static application landscape. The concept is that organisations make local decision about each extended use of CRS. Risk of leakage of patient information and corruption of that held within CRS will be managing through risk assessment and the detail of implementation.



- 5.3.2. Figure 10 – illustrates four examples: use of SMS messages, discharge letters, a whiteboard for staff to mark patient movements and an edit of the demographic record.
- (A) Text and letter communication applications draw information for individual patients from the local CRS application. This development is seen as low risk.
 - (B) Whiteboards are placed at Nurse Stations in A&E, departments or wards and hold a note of patient location and plan. These boards have been developed as a user interface with applications. The board presents patient information from the detailed record, staff update the status of patients and these changes are written back to the CRS. Once the device is authenticated to CRS, usage is without any form of authentication. Data entry of the status of admission, discharge and transfer is a by-product of manual recording of location on the Board. In this case there are risks of patient information error, integrity and confidentiality; these are managed by the responsible clinical team in the moment and the application is approved by the local organisation that may have to deal with problems of data quality.
 - (B) Use of kiosks for the patient to record arrival are becoming common. The patient confirms identity, queries CRS for appointment and confirms arrival.
 - (C) Another projected use of ITK is to enable patients to edit their address on the national demographic record. Provenance and integrity of the record would be supported by staff reviewing the requested change before it is uploaded. Similar arrangements could be used for clinical records.
- 5.3.3. Other features of ITK include support for user authentication mechanisms in each application joined with CRS. System to system authentication will replace use of CRS smartcards where access is through an ITK-enabled system. Audit trails are available within each application.
- 5.3.4. Developments are also planned for the patient portal HealthSpace (Advanced), it is assumed that this application will be attractive to patients once services are available which replace phone or letter communication (e.g. booking of appointments, order of repeat prescription). Some patients also may wish to have an active participation in management of conditions and to communicate with the clinical team. Interest for this is likely to be patients or carers with dependents with long term conditions, e.g. the parent of a child with diabetes. There are active trials of such communication with clinicians. Patient authentication is required for use of HealthSpace (Advanced). Current arrangement for registration of patients involves special attendance at an NHS location with documents. A risk assessment and business case has been prepared on an option of online Registration with the patient providing multiple identifiers, e.g. passport number, National Insurance number, NHS number, date of birth, address. Although it is possible to steal one identifier it is very difficult to gain all.
- 5.3.5. Extended use of CRS through ITK is a significant change of approach and echoes other proposals for management of information crossing boundaries [CR07]. As decisions on extension are to be made locally mistakes will be made. When this is

Developments in confidentiality and consent functions to support wider sharing of electronic health records in the UK

recognised the particular applications can be unhooked from CRS or additional security mechanisms could be added to address the problem.

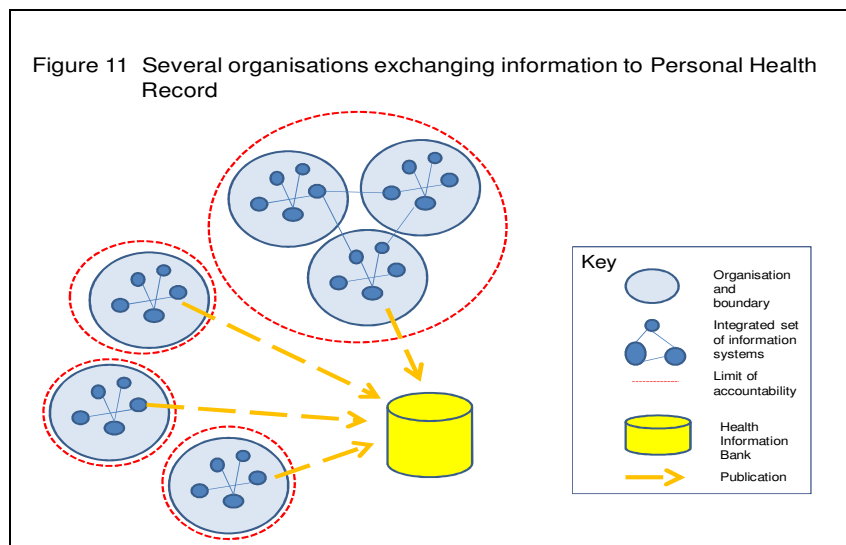
5.4. Other UK shared systems

A number of other EHRs have been developed in the UK, these are considered in turn:

- Hampshire Health Record
- Emergency Care Summary Scotland
- Individual Health Record Wales
- European Union EHR and Summary Care Record
- Personal Health Record
- Extending use of GP systems
- A single set of integrated systems for a facility shared between health care providers – Polyclinic
- London Ambulance Service use of information for Patients with chronic disease

- 5.4.1. Hampshire Health Record [HH10]; Implementation started in this local SCR in 2006. The system holds structured content from the GP record which is loaded daily and includes information about allergies, medication, diagnosis, tests and treatments. Documents and reports are added by local hospital and community care teams. The summary excludes reference to sexual health, terminations, abuse and complaints. There are currently 1.2/1.9 M population records. Username and password access are used with “permission to view” mechanism and patient opt out (0.1% of patients took this decision). Audit trail is available through the host organisation.
- 5.4.2. Emergency Care Summary Scotland [SC10]; The Scottish equivalent to the English SCR has been in use in Scotland since 2006. It presently has 2.5 records / 5M population with a twice daily update form the GP application. A “permission to view” mechanism is in use with patient opt out. As with the Hampshire, username and password access is used. The audit trail is available to patient on request from the GP practice. Implementation was based on local joint working on integration with Clinical leadership. There seems to have been little public controversy or professional criticism and widespread acceptance of benefits.
- 5.4.3. Individual Health Record Wales [WA10]; Similar content and approach as for SCR Scotland; currently available for 1M patients / 3 M population. It is available for Out of hour’s services and will be extended to A&E. Use is only within a local area. A “permission to view” mechanism is in use with patient opt out. Authentication is based on username and password access and an audit trail is available to patient on request.
- 5.4.4. European Union EHR and Summary Care Record; [CE10] Work has progressed on preparation of standards of interoperability but to date there appears to have been little use of these standards. Instead local summary records are being developed at provincial and national levels. The proposed EU SCR is to be based on enabling these summaries to be viewed across national borders. Implementation is at an early stage and there is no detail of proposals for interoperability of consent and confidentiality functions. There are also initial political discussions on interoperability of healthcare between EU and the US in the context of the US Government plan to digitise all healthcare records within five years as a consequence of the American Recovery and Reinvestment Act 2009.

- 5.4.5. Personal Health Record: [TA06], [GO10], [MI10] Personal Health Record (PHR) is a variation of the EH. Content and access to it is directly controlled by the patient. EHR is a legally mandated set of notes on the care provided by clinicians to patients as provided by an organisation. There is no legal mandate that compels a consumer or patient to store her personal health information in a PHR. Major investment is taking place by Google (Google Health) and Microsoft (HealthVault), and these suppliers currently offer use of PHR to patients without charge. Both companies have developed pilots with health service providers to feed elements of the EHR into the PHR, patients can also add information from other providers manually – see Figure 11. Consent and confidentiality functions for PHR are controlled by patients within the constraints of the provider. Should PHR usage become significant the feature that allows the patient to control and edit the record may prove problematic for clinical teams as the patient can delete or withhold information.



- 5.4.6. Extending use of GP systems: In the UK, there are specialised systems for GPs (Section 4.1.4). A recent development has been to extend access to GP systems to other clinical settings, particularly for the support of patients with chronic diseases (e.g. for Diabetes). Such patients receive care from GP, the Community and Hospital clinicians. Consent is gained from each patient for this extended use (e.g. the EMISweb product). Access to the record is unitary. Single factor authentication is used and there are plans to integrate the CRS smartcard authentication. This approach supports integration of care and record keeping centred on the patient with the GP Practice as the custodian. It is unclear whether this model of system use will grow to be significant. It could become universal.
- 5.4.7. A single set of integrated systems for a facility shared between health care providers – Polyclinic. A recent policy development in the NHS in London is to relocate services from hospitals in one location shared with health, social care, public sector and voluntary provider organisations. 100 are planned for the city by 2013. An assumption is that Polyclinics will provide a uniform experience to the patient whatever the service sought and irrespective of the organisation concerned. The plans are that following self-check in, reception staff will be able to register, book and prepare care plan for the patient using integrated systems. This presents a number of challenges not least those concerning consent and confidentiality. One planned approach includes a check-in kiosk, dynamically linked with multiple care systems, use of the SCR to support the out-of-hours provider and access to the extended GP

record. Clients, patients and staff will be briefed on how information is handled. Patients will be asked for permission to view their record and consent will be included in discussion of referral. It is planned to use the CRS ITK to link to the Community and Hospital applications. There will be a mixture of use of strong authentication and username / password. Single sign and context management will not initially be part of the solution. Formal information sharing agreements will lay out the obligations between organisations. It is not yet clear whether the vision of integrated workflows and care pathways across different systems can be achieved or whether the user experience will be intrusive.

- 5.4.8. London Ambulance Service use of information for Patients with chronic disease: Current arrangements for the London Ambulance Service are based on consent for care including hand-on to A&E. Patients may not wish for their GP to be informed or for their care to be diverted to other agencies. For children, vulnerable adults and repeat users routine efforts are made to contact other care providers (e.g. GP and Social Care). There are plans for call handlers to be enabled to view the SCR and locally derived detailed care plans for patients identified with chronic disease. Detail from these systems will be passed to the Paramedic teams and messages noting patient contact sent to agencies noted in the patient plan. It is assumed that such information will at some point be available directly to the Paramedic once mobile network coverage is complete and appropriate end user applications are available. The SCR has security and consent mechanisms, but there may be issues with use of care plans unless consent has already been gained for this specific use.

5.5. Conclusion

- 5.5.1. The CRS can be seen as a single security domain with use of strong authentication with a national patient index and emerging SCR for England contained within it. Common consent and confidentiality features were intended but vary between applications within the set of systems. Implementation of consent functions has resulted in complicated and ineffective controls without selective item granularity of the record. Implied consent within the organisation boundary has re-emerged as significant in the absence of strong legitimate relation functions. The ITK offers opportunities for extending use of information held within CRS and may enable organisations to tune use of information systems for local purposes as see in Section 4.
- 5.5.2. The provincial SCR systems considered show consistent use of patient opt out, withholding of sensitive parts of the record, use permission to view, username and password and audit trail. Extending access to GP applications, Polyclinics and the Ambulance example also show pragmatic and local solutions being found to extend use of current systems. Both CRS and these other examples of share health records provide a confused picture for patients who may not want their information to be shared.

6. Analysis of threats, security services, policy and a proposed use of the Clark-Wilson security model

In section 3, a definition of consent and confidentiality was developed. In Section 6, this definition is used to define the security policy and CW model for the EHR. An analysis of threats to the electronic health record is developed based on ISO7498-2. Relevant security services and technical controls are identified. A security policy is presented to support design. The function of the Clark-Wilson model is introduced and relevant entities discussed. A discussion follows of application of the security policy in design of a system. The section concludes with presentation of how the policy and model can be used in comparison with the examples of EHR in Section 5.

6.1. Analysis of threats to the electronic health record

6.1.1. The following is a list of potential security threats based on ISO 7498-2 [IS88]:

- Breach of message confidentiality
- Breach of message integrity
- Message spoofing
- Message replaying
- Denial of service
- Physical theft of appliance
- Unauthorised service access

These are discussed in the table 7: -

Threat	Assessment
Breach of message confidentiality	Messages contain confidential information and are moving over potentially insecure network. Confidentiality must be maintained at every level of the OSI model. Discussion to date has focused on the application layer.
Breach of message integrity	Messages transiting potentially insecure network. Message integrity is essential as it is used to support clinical care.
Message spoofing	The application traffic is exposed on potentially insecure network and must be protected against interception and reuse.
Message replaying	The application traffic is exposed on potentially insecure network and must be protected against interception and reuse. At OSI layers beneath application, the expectation is that the messages contain a unique identifier and timestamp.
Denial of service	There is a risk of denial of service which could significantly disrupt clinical practice.
Physical theft of appliance	It is assumed all hardware and software is located in a non secure area and that network components are made as secure as possible.
Unauthorised service access	It is assumed that authorisation of access is required at a number of layers of OSI including the user.

6.1.2. The most significant threat is intentional improper disclosures by insiders. Although technical security mechanisms are required at all levels, to address the threats in Table 6, focus for control must be placed on the user of the system.

6.2. Relevant security services and technical controls are identified

6.2.1. In terms of security services, the list in Table 7 are identified as necessary and are assumed as being present in the system.

Table 7 Summary of Technical Controls for electronic health records	
Digital certificates	Digital certificates provide the basis of security in untrusted environments. Use of digital signatures against content of the EHR ensures integrity.
User identification, authorisation, and audit	Strong authentication for staff and potentially patients if they are to have direct access to records. Registration process to ensure identification. All transactions recorded in audit trails.
Application authentication, plus message integrity and confidentiality	Messages to be secured in transit (including protection against man-in-the-middle attacks), and also to perform strong authentication of the application to guard against spoofing.

6.3. A security policy for an EHR

6.3.1. The legal and policy context (Section 3) can be summarised as the need to provide the patient with active choice on whether to allow the record to be viewed or used outside the location and team where it was created. The requirement for a direct relationship of the care team to the patient was identified. In the policy a lead clinician is made responsible for each record (Caldicott Guardian 3.3.2) and there should be a separation of authorisation for access. An emergency override is present (2.1.3). The identity of staff that access the record should be available through an audit trail (3.3.1) A note of the provenance of the record and the capacity to mask parts of the record and audit trail from the patient are also available. This policy is a variation of that presented by Anderson [RA96] with roles-based access rather than access control list on the record. This policy is stated in a sequence of design principles in Table 8.

Table 8 Security Policy for an electronic health record
<ol style="list-style-type: none"> 1. Lead clinician; when a record is created a clinician is designated as lead for granting access rights for other staff and oversight of consent for information sharing 2. Patient decides availability of record; the patient decides what part of their health record is available for use by others outside of the team providing care 3. Staff must be authorised to access a record; a patient's information will be accessed by staff with authorisation and with clear accountability of actions to view, create, edit and blind write 4. Emergency override; Except in an emergency, or otherwise permitted by law, the patients wishes for sharing their information will be followed (whole or part of record) 5. Provenance; the integrity, provenance, author and timeliness of information within the patient record will be clear to the reader 6. Accountable staff; the identity of any staff that have viewed, created, edited, blind written to and deleted any part of a record is available including a note of consent violation <p style="text-align: center;">(continued)</p>

Developments in confidentiality and consent functions to support wider sharing of electronic health records in the UK

Table 8 Security Policy for an electronic health record (continued)

- | |
|--|
| <p>7. Mask third party information from patient; the designated lead clinician can mask third party information in the record and that which may cause harm to the patient (i.e. electronic or paper output)</p> <p>8. Mask audit trail from patient; the designated lead clinician can stop an entry in the audit trail available to patients when available to the patient record is made for purposes of public good or safety; this would not effect other copies of the audit trail which would remain complete</p> |
|--|

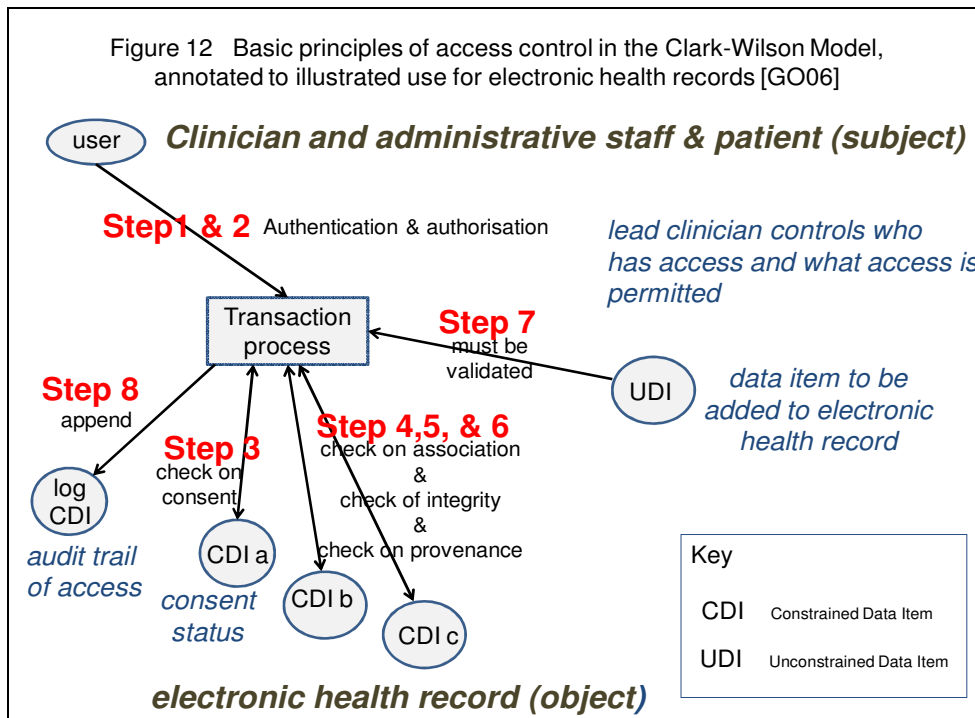
6.4. The Clark-Wilson model

- 6.4.1. The CW security model is concerned with preventing unauthorised modification of data, fraud and errors in commercial applications [CW89]. An important aspect of health records is availability to view and readability. So this is an extended use of the Clark-Wilson (CW) security model to include confidentiality and consent as well as integrity.
- 6.4.2. Two aspects of integrity are considered by the CW model, internal and external. Internal integrity refers to properties and operation of the internal state of the system. External integrity concerns the rules of operation of the model in terms of the outside world. If a health organisation or possibly a patient wishes to join the model – i.e. have a shared electronic health record – the rules that have to be followed and enforced through audit.
- 6.4.3. If the record is defined as only existing within one organisation and potentially a single or linked set of systems, the CW model can be stated in terms of that singular system. For a set of collaborating organisations the rules concern shared use of systems across those organisations. Health records may, for the most part, reside within a particular location and organisation.
- 6.4.4. To maintain external consistency if the health record is used across a number of participating organisations the organisations would need to follow a single set of rules for the model to hold. Any organisation seeking to participate in using the shared health record would need to follow the rules and as part of that use an approved IT system. All individual members of staff and participating organisations are open to audit.
- 6.4.5. In this application of the CW model subjects are the staff, objects are the electronic health records and use of programs (Transaction Programs) link subjects with objects.
- 6.4.6. In CW well formed transactions and separation of duties are general mechanisms for enforcing integrity. Data items can only be manipulated by a specific set of programs and users have to collaborate to manipulate data and to collude to circumvent. This includes development, certification and operation of the system.

Developments in confidentiality and consent functions to support wider sharing of electronic health records in the UK

6.4.7. Figure 12 provides an illustration of the function of the model, in this scenario the user views the record and makes an update.

- Step 1 the user authenticates to access the system;
- Step 2 access rights are specific to the user (previously authorised);
- Step 3 a check is made on the permission to view the record;
- Step 4 a check is made of the association of the patient with the user, Is there a direct care relationship? If so, access is enabled;
- Step 5 & 6 the system checks the digital certificates to confirm data integrity and the origin and timeliness of information
- Step 7 the user updates the record
- Step 8 a note of access is entered onto the audit trail



6.5. Model entities for the electronic health record

6.5.1. In CW models objects can be manipulated only by a restricted set of programs. In the model for consent for health records the following transactions are defined:

TP1 <i>Read part or whole of record dependent on consent status of record</i>	The most important function for the health record
TP2 <i>Read whole of record irrespective of consent status of record</i>	This function is available in emergency situations and is intended to circumvent the consent flags attributed by the patient
TP3 <i>Write to record</i>	
TP4 <i>Blind write to record</i>	This could be an automatic update for example for a biometric reading, i.e. blood pressure

Developments in confidentiality and consent functions to support wider sharing of electronic health records in the UK

Table 9 Clark-Wilson Transaction Processes for an EHR (continued)	
Control Transaction Processes	
TP5 <i>Write to consent configuration of record for a patient</i>	The model allows the consent flags to be set as a default, by the patient directly and by clinical staff.
TP6 <i>Able to authorise a TP to a member of staff</i>	This is an important operational control for the model. This will be undertaken by authorised parties within the organisations or sets of organisations.

- 6.5.2. To simplify selection of TPs for staff, a role-based access control mechanism is applied in this consent application – see table 11.

Table 10 Clark-Wilson; the association of Transformation Procedures (TP) with Role-Based Access Control (RBAC)		
RBAC	TP	comment
Clinician	TP1, TP3, TP4	Clinician is able to use the health record dependent on consent decisions of the patient
Emergency clinician	TP1, TP2, TP3, TP4	This role has the “break the glass” function of access to the health record irrespective of consent decisions of the patient. Such an action would result in an alert being generated to the GP of the patient and the Medical Director of the organisation under which care is delivered.
Administrative staff member	TP1, TP3, TP4	Same functions as a clinician
GP of patient	TP1, TP3, TP4, TP5	Capability to set the consent flags of the health record, otherwise same functions as a clinician
Medical Director of team / organisation	TP6	Capability to set the RBAC for staff and thus select the associated TPs with staff

- 6.5.3. In CW models, data items are Constrained Data Items (CDIs); for this consent application of the model, these are given as:

Table 11 Clark-Wilson; Constrained Data Items for an EHR
Patient index number 1 Patient index number 2 Patient name, Sex, Date of birth, Title Address 1 (A1), residence A1 change date Address 2 (A2), for correspondence A2 change date Registered General Practice (RGP) 1 RGP 1 change date Registered General Practice (RGP) 2 RGP 2 change date Fixed things – blood, allergies and contra-indications, DNA status etc... Useful changing things – medication, care plan & who is providing care Medical history summary Medical history episodic summary / detail Past scans and metrics

Developments in confidentiality and consent functions to support wider sharing of electronic health records in the UK

- 6.5.4. A patient's health record a pattern of consent flags are set for both read and write. These could be at granular level for each data item or at a more general level, in this example model they are set at a granular level and an aggregation that could be adjusted as experience is gained: -

Table 12 Clark-Wilson; Consent flag for view and edit functions for Constrained Data Items for an EHR			
	View	Edit	Aggregation / simplification of consent
Patient index no 1	Yes / No	Yes / No	It may be thought necessary to make some patients invisible to most staff members. This could be done by defining a TP with complete search function with allocation to staff carefully limited and with all others using a limited search function
Patient index no 2	Yes / No	Yes / No	
Patient name	Yes / No	Yes / No	
Sex	Yes / No	Yes / No	
Date of birth	Yes / No	Yes / No	
Title	Yes / No	Yes / No	
Address 1 (A1), residence	Yes / No	Yes / No	An aggregation could be made at demographic detail level – i.e. all such data items could be made searchable and viewable with all with consent operation at the level of clinical information
A1 change date	Yes / No	Yes / No	
Registered General Practice (RGP) 1	Yes / No	Yes / No	
Fixed things – blood, allergies and contra-indications, DNA status etc...	Yes / No	Yes / No	These data items could be grouped together for consent purposes
Useful changing things – medication, care plan & who is providing care	Yes / No	Yes / No	
Medical history summary	Yes / No	Yes / No	
Medical history episodic summary / detail	Yes / No	Yes / No	Access to this level could be constrained by team / organisation association
Past scans and metrics	Yes / No	Yes / No	

- 6.5.5. In addition to the consent status for each data item or group of items, in the model for consent, digital signatures are added. For this to be possible a Public Key Infrastructure (PKI) would need to be deployed across the health care record entity.

Developments in confidentiality and consent functions to support wider sharing of electronic health records in the UK

Table 13 Clark-Wilson; Digital certificate for Constrained Data Items within an EHR		
	Valid digital signature	
Patient index no 1	Yes / No	<p>On each occasion that a CDI is created from a UDI a digital signature is created for each data item or group of data items – i.e. the clinical summary or an episode of care.</p> <p>When a TP reads the CDI, checks can be made on the digital signature.</p> <p>This function allows the provenance of each data item to be confirmed.</p>
Patient index no 2	Yes / No	
Patient name	Yes / No	
Sex	Yes / No	
Date of birth	Yes / No	
Title	Yes / No	
Address 1 (A1), residence	Yes / No	
A1 change date	Yes / No	
Registered General Practice (RGP) 1	Yes / No	
Fixed things – blood, allergies and contra-indications, DNA status etc...	Yes / No	
Useful changing things – medication, care plan & who is providing care	Yes / No	
Medical history summary	Yes / No	
Medical history episodic summary / detail	Yes / No	
Past scans and metrics	Yes / No	

6.5.6. Inputs into the health record are considered as Unconstrained Data Items (UDIs – see Step 7 Figure 11). The programs, (TPs) have to be used to change UDIs to CDIs. At this point of transformation, the integrity of a state is checked by integrity verification (IVPs) – see later discussion.

6.5.7. In this application of the CW model an association of staff member to a team / organisation is included (see Step 4 Figure 11). This allows the IVPs to examine whether there is a relationship between the staff member and the patient. A coding of team and organisation is present in the consent model: -

Table 14 Clark-Wilson; Team and organisation codes for an EHR	
Team 1 Organisation 1 Team 2 Organisation 1 Team 3 Organisation 1 Team 1 Organisation 2 Team 2 Organisation 2 Team 3 Organisation 2	An association is created between staff members and also separately with patients health records. A great number of concurrent associations are possible with patient's records, whilst the staff association is only possible contemporaneously with the organisation and team for which the staff member is working.

6.5.8. When a health record is created a team and organisation in which care has been provided is set an association. Should other services be provided within the organisation, additional team associations are added. Some associations age and cease whilst others remain permanent, e.g. GP. It is possible for an organisation to set a unitary team / organisation code. As a result a patient record will have at least one team / organisation associated with it and may have several at any one time.

Developments in confidentiality and consent functions to support wider sharing of electronic health records in the UK

- 6.5.9. At the time of a Transformation Procedure a series of integrity verification procedures (IVPs) are run. In this consent use of the CW model the following IVPs examples are offered to illustrate function:

Table 15 Clark-Wilson; integrity verification procedures for an EHR	
IVP1 - Is the staff member authenticated?	<i>(see Step 1 Figure 11)</i>
If authentication fails the operation fails	
IVP2 - Is the patient record authenticated? This may not be present.	
IVP3 – Is consent present for the staff request for view of a data item? <i>(see Step 3 Figure 11)</i>	
A check is made as to whether the consent flag relevant to the data item and TP is set to allow use (edit or view). If no, then the operation fails. The message back to user must not allow the user to infer the presence of information.	
IVP4 – Is there an organisational association for the staff request for view of a data item?	<i>(see Step 4 Figure 11)</i>
A check is made as to whether the organisational association for the staff and the patient allows access. If no, then the operation fails. If the health record exists across a number of organisations then there needs to be a translation table to capture the association between organisations (and teams) which is references during the TP. A positive association could link organisations involved with an episode of care such as treatment for cancer or a chronic disease such as diabetes. The operation may be designed to partially fail, for example data items associated with demographic details or summary details such as active medications may always be visible but the more detailed information concerning an episode of care may not be available. When a TP is launched with no organisation associated with the members of staff (for example following an accident abroad) a constrained and limited access may be enabled, e.g. a high level summary of key clinical facts (a consent selection agreed in discussion between the patient and their GP).	
IVP5 – Are the digital certificates associated with data items valid?	<i>(see Step 6 Figure 11)</i>
A check is made on the certificates associated with each data item (CDI). The certificates allow the provenance of each data item to be established and this	

- 6.5.10. A series of integrity verification rules are present, this are illustrated in Table 15.

Table 16 Clark-Wilson; Certification Rules for an EHR	
Certification Rules	
CR1 <i>IVPs must ensure that all CDIs are in a valid state at the time the IVP is run (integrity check on CDIs)</i>	This could include many aspects of checking of data including format, relationship of one to another and the presence of digital certificates that indicate data origin.
CR2 <i>TPs must be certified to be valid, i.e. valid CDIs must always be transformed into valid CDIs. Each TPI is certified to access a specific set of CDIs</i>	This is relevant to the situation where the record is only kept within one organisation; a more distributed environment could mean access from multiple organisations required each the TP set to be tested as part of an approval process. The wider and more universal the record the more complicated this could become.

Table 16 Clark-Wilson; Certification Rules for an EHR (continued)	
CR3 <i>The access rules must satisfy any separation of duties requirements.</i>	The elements to be separated have been identified in this model as allocation of TPs to individual staff members through selection of RBAC and the setting and editing of the consent flags on the patient record. The association of team and organisation attribute to the staff member (or TP in use) and the record could be manual or handles within the computer system. Again this model is more plausible in this respect (CR3) when developed and used within one organisation, more distributed systems would require agreement to a set of rules and use of associated system functions across organisations. The record is required outside of this constrained set and it is possible to conceive of simple functions being available in those cases – i.e. read only constrained by consent flags with no possibility of alternative TPs or changing consent flags.
CR4 <i>All TPs must write to an append log</i>	This places an audit log as a key element of the model.
CR5 <i>Any TP that takes a UDI as input must either convert the UDI into a CDI or reject the UDI and perform no transformation at all</i>	Checking of digital certificates is relevant here.

6.6. An application of the security policy using the Clark-Wilson model

6.6.1. We have looked at the entities of this application of the CW model, further detail is now given of how the policy would work in design of a system for electronic health records. A record can be created in many locations across a range of organisation. The first element of the policy requires a clinician to be responsible for granting access and setting the rules for sharing, this establishes clarity of control and accountability. As records are managed by a clinician then trust in exchange of information is maintained on the basis of clinician to clinician communication. Clinicians may be the minority of direct users of the record with the majority being administrative staff supporting clinicians. The record will stay under the control of the lead clinician even if information is passed to other clinicians.

1. **Lead clinician**; when a record is created a clinician is designated as lead for granting access rights for other staff and oversight of consent for information sharing

6.6.2. The lead clinician has two control decisions, granting the business function or role of other members of staff and how consent for sharing is managed. This could be directly setting the flags, enabling the patient to do this themselves or granting that function to other staff (see Step 2 Figure 11).

6.6.3. One complication to this arrangement is when reference in the record is made to others, e.g. parent relationships, and also 3rd parties. In some circumstances it would not be considered appropriate for the patient to be aware of this information (e.g. allegations of criminality). Arrangements for this circumstance would need to be reflected in local practices and can be seen to militate against full control of the record by the patient. The organisation providing care has obligations to other parties, in this instance, in addition to the direct relationship with the patient.

Developments in confidentiality and consent functions to support wider sharing of electronic health records in the UK

- 6.6.4. Use could be made of digital certificates as the basis for establishing identity and strong authentication of access as well as digital signature for assurance of content of the record; more of this later.
- 6.6.5. Given the scale of record creation various simplifications could be adopted such as having a single clinician responsible for all record creation in an organisation or team and this would fit with other clinical management approaches based on a Director and Consultant. Clinical relationships are characterised as hierarchical in terms of accountability for the care of an individual patient but also collegiate in terms of the provision of care as a team. There would need to be strong local ownership of this principle of clinical accountability of electronic record creation for this to be acceptable and practical and considerable local flexibility to reflect practice. This principle is likely to prove easier in small organisations or departments compared to larger ones. Composite entities (e.g. current set of Pathology results for an episode) may be problematic.

2. Patient decides availability of record; the patient decides what part of their health record is available for use by others outside of the team providing care

- 6.6.6. The electronic health record is assumed to have a granularity that can support consent for sharing all of it, a summary, an episode, or any parts of it – see Table 12 and 6.5.3.
- 6.6.7. The assumption is that all within the team currently providing care can view the record. This is open to further refinement if necessary; for particular circumstances such as sexual health, if electronic records are not viewed as sufficiently secure, then there may be a procedure to hold some information only on paper and in a secure location. This is an occasional arrangement at present – see
- 6.6.8. The patient may be able to set consent rules themselves through use of a portal to the organisations systems or through a Personal Health Records (5.4.5). The funding mechanism for healthcare is likely to dictate whether control is directly available to the patient or is administered through staff employed by the health care organisation.
- 6.6.9. There could be disadvantages to the patient setting consent themselves. The patient may not appreciate the significance of their decisions. The patient may, following an emergency, wish that they had not made a decision not to share. Given the litigious nature of Medicine, health organisations may not accept the risk of being accused of not protecting the patient. The approach taken has to be carefully communicated to patients and staff must be trained in this context. Complexity of consent functions can cause problems – see [GRa08], 5.1.6.

3. Staff must be authorised to access a record; a patient's information will be accessed by staff with authorisation and with accountability of any actions

- 6.6.10. A set of roles for accessing health records is designated (see Table 11, 6.5.2). Control of attribution of roles rests with the designated clinical lead and is delivered by the access control function of relevant systems. Access will vary from blind write (e.g. for a process for storing a result) to view and write. Accountability for access by clinical and administrative staff rests on use of strong authentication and a audit trails. These audit trails will reside in the local application, but could be copied to the

Developments in confidentiality and consent functions to support wider sharing of electronic health records in the UK

GP or directly to the patient (e.g. storage in the Personal Health Records). Alerts could be set up, e.g. to tell the patient someone had accessed their record. Additionally, the audit trail could be hosted by a professional body and could be used to monitor standards [RA96].

4. **Emergency override**; except in an emergency or otherwise permitted by law, the patients wishes for sharing their information will be followed

6.6.11. The consent status for record sharing will be followed by the system. In emergency, an override to this element of access control is available to some staff, e.g. A&E departments and Out of Hours teams. ...

5. **Provenance**; the integrity, provenance, author and timeliness of information within the patient record will be clear to the reader

6.6.12. Digital signatures on parts or the whole record can deliver this function. Checking of associated certificates would be automated within the viewer. ...

6. **Accountable staff**; the identity of any staff that have viewed, created, edited, blind written to and deleted any part of a record is available including a note of consent violation

6.6.13. Audit functions of the system are crucial to the model. Use of audit trails will allow tracking and alerting of remote access and, through authentication, accountability of any given access.

7. **Mask third party information from patient**; the designated lead clinician can mask third party information in the record and that which may cause harm to the patient (i.e. electronic or paper output)

6.6.14. Clinicians and their employing organisations have obligations to protect any third parties whose information is recorded as part of a record. In addition there are some situations in which information within the record could be judged as potentially causing harm to the patient. An example of this could be a prognosis when the patient has stated that they prefer ignorance. Mechanisms to deliver this function could require masking of information as resident on the system or in any outputs – e.g. a print out of the record. This is a difficult area and is likely to vary greatly between clinical environments.

8. **Mask audit trail from patient**; the designated lead clinician can stop an entry in the audit trail available to patients when available to the patient record is made for purposes of public good or safety; this would not effect other copies of the audit trail which would remain complete

6.6.15. There will be occasions when access to the record and disclosures of patient information may be required without the consent of the patient. Examples of this include notification of infectious diseases, review of clinical quality, competence of individual practitioners and public interest in the context of a violent patient. The model is set up to alert patients or to create an entry in the audit log. In most situations a patient would be told of disclosure. In an unusual case where there is a public interest in protecting others there may be a requirement not to tell the patient. In this instance the lead clinician could prevent entry in the patient copy of the audit

Developments in confidentiality and consent functions to support wider sharing of electronic health records in the UK

trail and any associated alerts. There would be at least one copy of the complete audit log held, possibly by the GP or by the organisation.

6.7. Conclusion

6.7.1. A security policy has been developed with the following features which will be used in the Section 7 to support comparison and analysis of EHRs:

- Lead clinician;
- Patient decides
- Staff must be authorised to access a record
- Emergency override
- Provenance
- Accountable staff
- Mask third party information from patient
- Mask audit trail from patient;

6.7.2. A security model for electronic health records has also been prepared based on Clark-Wilson because there are many more objects (records) than subjects (Clinicians), records are distributed across many organisations and there is little benefit in the concept of a hierarchy of security levels (all records are confidential). Focus is on an access control of each record. Clark-Wilson provides a framework including formed transactions, authorisation with a separation of function, a shared set of rules and internal audit. The security policy places control of access to the record with a lead clinician with a particular emphasis on the audit trail. In the next section, comparisons are made using this model and policy. Table 16 illustrates how the features of Clark-Wilson are related to health records.

6.7.3. The policy and model address weakness in compliance identified in Sections 4 (existing systems) and Section 5 (shared systems), namely reliance on implied consent rather than demonstrable and direct relationship of care between the team member and the patient, lack of granularity of control of access to the record and diffuse audit trails of access as these are held in each application rather than in brought together in one place.

Table 17 Summarised features of Clark-Wilson Model <i>(distinctive to electronic health records in italics)</i>	
Feature	Comment
Authentication of staff Authentication of patient	Controlled use of the electronic health record requires certainty as to who uses it (identity) and control of functions available to them (authorisation) and then a note of actions
<i>Organisational / team association of staff request</i>	
Constrained actions on data items	Data items and transactions that can act upon them are controlled to ensure a stable system within the system and security policy definitions
<i>Emergency over ride "break the glass"</i>	<i>In an emergency the clinical team has a duty of care which, in general, overrides considerations of privacy; this is open to abuse and attention to active monitoring is recommended</i>

Table 17 Summarised features of Clark-Wilson Model (continued)	
Feature	Comment
Separation of function – authorisation of access and action	This is a standard control feature for security, specific to this application for electronic health records separation concerns authorisation of business function for access (role-based access control), association with the patient and setting of the consent status if this is undertaken for the patient.
Consent status for access to patient record	Reference is made to this consent status as part of the logic of transactions to ensure the system follows the intentions of the patient.
Digital certificates associated with patient record data items	Digital signatures are used to prove integrity, origin and timeliness of items held within the electronic health record.
Shared set of rules for organisations with single agency managing them	Consistent rules ensure that secure of the electronic health record is maintained wherever it is held or accessed in multiple organisations.
Audit of use of system	Audit trails allow active monitoring of use of the system.

7. Comparison of the security policy and model with examples of shared use of electronic health records

In sections 4 we looked at practical issues for consent and confidentiality in use of electronic health records and in Section 5 we looked at the CRS and other shared records. In Section 6 we considered an ideal for these functions, prepared a policy and built an appropriate model. In Section 7 we will look again at existing and shared systems using the policy and model.

7.1. Comparison of CRS with the model

- 7.1.1. In Tables 18 on the following page the different character of example systems are compared with the model. In terms of a lead clinician controlling access to the record, there is a different approach for each example. For existing health records, the Caldicott Guardian provides nominal oversight, for SCRs the GP is in control, sponsorship based on the Caldicott Guardian is used and PHRs are patient controlled. In terms of consent, existing systems are limited in this respect, SCRs have an opt out available through the GP, CRS function is complicated and obtuse and PHRs are patient controlled. All have a process for authorisation of Staff for access, for PHRs, again, the patient is in control. All have an emergency override, apart from small parts of the CRS, provenance is established through system context with audit trail being available for reference. Accountability of staff for access is through authentication of access and reference to application specific audit trails. Masking of records is relevant to existing health records and CRS only and is done manually.

Developments in confidentiality and consent functions to support wider sharing of electronic health records in the UK

Table 18 Comparison of shared electronic health records against the policy					
	Existing health record	Example Provincial Summary Care Record (e.g. Wales)	NHS England Care Record Service	Personal Health Records Google Health and MS HealthVault	Proposed EU Summary Care Record
Lead clinician	Caldicott Guardian for Organisation provides formal oversight, unclear what practical effect this arrangement has on record ownership and access control which are largely by convention	GP as custodian	Staff are sponsored for registration / smartcard, for RBAC. Legitimate relations are controlled through system configuration	Patient is in control of record	Based on provincial or national arrangements
Patient decides	Few possibilities for controlling movement of patient record	Opt out through GP Practice and "permission to view"	For SCR, Opt out through GP Practice and "permission to view", for detailed local record a complex set of options	Patient is in control of record	Based on provincial or national arrangements
Staff must be authorised to access a record;	Yes but great variety of control functions	Yes	Yes	Patient control when and who sees the record	Unclear, presumed will include "permission to view",
Emergency override	Yes	Yes	Yes	Not available unless the patient indicates how record can be accessed if patient is unconscious	Unclear
Provenance	Yes through system context with audit trail available	Yes through system context with audit trail available	Yes through system context with audit trail available. Digital signature is available and used for some data items (e.g. prescription)	Content is controlled by the patient	Unclear
Accountable staff	Yes, through 1-factor authentication and audit trail in each application	Yes, through 1-factor authentication and audit trail; access is local only	Yes, through 2-factor authentication and audit trail in each application;	Access is controlled by the patient	Unclear
Mask third party information from patient	Yes	Content is limited so not necessary	Yes	Not relevant or possible	Unclear
Mask audit trail from patient	Yes	Content is limited so not necessary	SCR content is limited so not necessary, for detailed local record - Yes	Not relevant or possible	Unclear

Developments in confidentiality and consent functions to support wider sharing of electronic health records in the UK

	Existing health record	Example Provincial Summary Care Record (e.g. Wales)	NHS England Care Record Service	Personal Health Records Google Health and MS HealthVault	Proposed EU Summary Care Record
Authentication of staff	Username and password (1 factor authentication)	Username and password (1 factor authentication)	2 factor authentication	Information released directly by patient	Varied by nation, minimum as Username and password
Authentication of patient	No, undertaken by staff	No, undertaken by staff	No, undertaken by staff	Yes, undertaken by patient	No, undertaken by staff
Organisational / team association of staff request	Organisational – yes, team association will vary by application (probably not formalised)	Access from local location (Out of hours service)	Yes, managed by organisation for local record and also for summary record	Patient decision	managed by national organisation
Constrained actions on data items	Yes – will vary between applications	Yes – will vary between applications	Yes, constrained within applications and by a messages set between applications	Yes - receive information from health organisations	Yes read only with controlled update by national government
Emergency over ride “break the glass”	Yes	Yes	Yes	Yes as long as the patient is conscious (or if instructions are present), otherwise no	Yes
Separation of function – authorisation of access and action	Yes	Yes	Yes	Patient decision	Yes
Consent status for access to patient record	No	Opt out and “permission to view	Complex consent functions within application, for summary care record - Opt out and “permission to view”	Access is Patient decision	Yes with additional request to view
Digital certificates associated with patient record data items	No	No	Yes	No, patient controls updates	No
Shared set of rules for organisations with single agency managing them	Yes	Yes	Yes	Patient controlled, provided by a supplier	Yes
Audit of use of system	Yes	Yes	Yes	Unclear	Yes

7.1.2. See Tables 19 two pages forward – the different character of existing systems are compared with the Model. With the exception of PHR, all have a mechanism for authentication of staff. Authentication of patient is absent and is not relevant to PHR. A different approach is taken to organisational and team association of staff request with the patient for each example. All have constraining mechanisms actions on data items, an emergency over ride and separation of function. Consistent consent functions exist for SCRs. Digital certificates are only available in CRS. Audit and a shared set of rules for use of the shared system are available in all examples.

7.2. Conclusion

7.2.1. Comparison of the policy and model with existing and shared systems show the distance between an ideal and the real world. In UK examples, a series of simple approaches are adopted to deal with legal compliance, such as appointing a clinician as Caldicott Guardian, providing nominal oversight of access to health records. The consent aspect and confidentiality functions of CRS are considerably more limited than that established in the model security policy with weakness in legitimate relations and consent at the record level. There is no clear accountability of clinicians for control or visibility of access to the patient. The Summary Care Record can be seen to provide a way of sharing information, again with simple methods of securing and limiting access. Personal Health Records contrast strongly with an alternative approach based on direct control of the record by the patient. Patient authentication is absent; staff of custodian organisations are responsible for this step and this is consistent with the absence of a capacity for the patient to author the record with the exception of PHR.

7.2.2. This is a first generation of system for sharing health records. Great improvements could be made to features such as legitimate relations and consent functions which appear trivial and complicated in CRS. Audit trails could be consolidation and access given to the GP and directly to the patient through HealthSpace or PHRs. Extending use of the established Public Key Infrastructure (PKI) from strong authentication to digital signature for key data items and events (e.g. prescription) and then to signature of larger parts of the record could form the basis of confirming integrity and provenance of the record as it is more widely shared. The portal offers possibility of a co-authored health record with modes and speeds of communication comparable with the expectations for a patient as a consumer.

8. Conclusions

- 8.1.1. In the absence of standards, current examples of shared electronic health records show a pragmatic and incremental approach. There are a number of Summary Care Record taken from the General Practitioner system available for a tenth of population of the UK. These hold information on active medications, allergies and contra-indications. There are common consent and confidentiality functions from these different examples based on a patient opt out managed by the General Practitioner and a “permission to view” question at the point of care. Current experience is that 0.1% of the population wish to opt out. Single factor authentication is in use and an audit trail available. Some of the Summaries include selective withholding of parts of the record (e.g. for sexual health) and some also hold documents posted from Hospital and the Community services.
- 8.1.2. There are also many implementation of extended use of existing systems across organisation boundaries, the most common being provision of wider access to the General Practitioner system by the clinical team based in the Community and Hospital setting. This may become general for patients with long term conditions such as Diabetes. Patient consent is gained and access to the record is unitary. Again single factor authentication is in use and an audit trail is available.
- 8.1.3. Use of a more complex set of systems is planned for Polyclinics – an integrated set of services delivered by multiple organisations in one building. Management of consent functions rest on informing patients on how their information will be handled, inter-organisation agreements and staff procedures with limited possibilities for opt out.
- 8.1.4. In addition, the Care Record Service is in widespread in England. It has a single security infrastructure based on two-factor authentication of access, limited use of digital signature and a compliance regime for the layered technical components that underpin its application set. A central spine holding demographic patient details, a Summary Care Record and other services is connected through messaging with a validated set of patient record systems. Embedded consent functions have proven difficult to develop, hard to use and confusing for the patient. For the Care Record Service version of the Summary Care Record, again, a “permission to view” function is in use. Functions to control access to the patient record based on a direct care relationship (legitimate relations) are delivered within each of the applications of the Care Record Service rather than through the central architecture. Again, audit trails are not consolidated for patient or organisations and are held within each application. Sealed envelopes for selective information have not yet gone into use but are also likely to be application specific.

- 8.1.5. The Interoperability Toolkit may go into widespread use with the Care Record Service. If so, the Care Record Service may be considered to have a strong security domain at its' centre with risk-based sharing of information at its edge. This would reflect current system integration within organisations where, once patient data is collected, it is repeatedly used. Also, if a simple way of managing registration for patient authentication to the HealthSpace portal is achieved and NHS services are enabled for communication, then this may become a popular tool for patients to book appointments, reorder prescriptions and communicate with the clinical team. There is currently no evidence of widespread use of Personal Health Records in the UK (Google Health and Microsoft HealthVault). If HealthSpace is successful then this may be more attractive because of its authentication, potential upload of the record from custodian organisations from NHS systems and for communication with the clinical team.
- 8.1.6. Of the examples considered, the Care Record Service is closest to the policy and model developed in this dissertation. Public Key Infrastructures, strong authentication and digital signatures are expensive and inflexible, so perhaps it is not surprising that the only example of use is national. Some improvements are available such as providing a single place of reference for audit trails of access. Should standards for electronic records be implemented then perhaps such technologies will also go into mass use providing additional services such as supporting integrity and provenance.

Appendix – Interviews

Clive Thomas	Information Governance Manager, NHS South Central SHA
Paul Richards	Information Governance Manager, UCLH
Remi Ogbe	Information Governance Manager, Barts and The London NHS Trust
Lech Bogdanowicz	Information Governance Manager, St. George's Healthcare NHS Trust
Nick Murphy O'Kane	Information Governance Manager, NHS Shared Business Service
Chris Kitchener	Information Governance Manager, East London NHS Foundation Trust
Ray Hill	Information Management Project Manager, NHS London SHA
Paul Evans	Connecting for Health, Technical Architect
Nick Schlanker	Connecting for Health, Technical Architect
Janice Sorrell	Information Governance Manager, Kingston Hospital NHS Trust
Peter Singleton	Connecting for Health, Information Governance Subject Matter Expert
Dr Gillian Braunold	Connecting for Health Clinical Lead
Paul Everson	Department of Health

1. Is consent for information sharing an important function for electronic health records?
2. How is it handled in the current systems / recent developments / Care Record Service?
3. Have mechanisms for consent changed?
4. Do you think current arrangements are practical?
5. Would you do anything different if you knew then what you know now?
6. How about the wider sharing context of EU, Google Health and Microsoft HealthVault?
7. Do you have any thoughts about the future of consent? (i.e. shared identity management for commercial and public sector services and use of Public Key Infrastructure by Professional bodies and health care providers?)

Appendix – References

[BN89]	DFC Brewer, MJ Nash, The Chinese Wall Security Policy, Proceedings of the IEEE Symposium, 1989
[BE96]	DE Bell, LJ LaPadula, Secure Computer Systems: Mathematical Foundations, Electronics Systems Division 1973, reproduced Journal of Computer Security 1996
[CE10]	European Committee for Standardisation, http://www.cen.eu/cen/
[CO02]	A Cornwall, Electronic health records: an international perspective, Health Issues 2002 number 73, 2002
[CO04]	E Coiera, R Clarke, e Consent: The Design And Implementation of Consumer Consent Mechanisms in an Electronic Environment, Journal of the American Medical Informatics, 2004 2004;11:129
[CQ09]	Care Quality Commission, National Study; the right information in the right place, at the right time – a study of how healthcare organisations manage personal data, http://www.cqc.org.uk/
[CR07]	PCh Cheng, P Rohatgi, C Keser, Fuzzy MLS: An Experiment on Quantified Risk–Adaptive Access Control, IBM Thomas J. Watson Research Center, IEEE Symposium, January 3, 2007
[CW89]	Clark DD, Wilson DR, A comparison of commercial and military computer security policies, NIST special publication, 1989
[DA08]	M Davies, S Eccles, G Braunold, M Winfield, M Thick, Giving control to patients, Br J Gen Pract. 2008 March 1; 58(548): 148–149.
[DH01]	Department of Health, UK. Building the information core: Protecting and using confidential patient information, 2001
[DHa02]	Department of Health, UK, Legal and policy constraints on electronic records 2002, http://www.connectingforhealth.nhs.uk
[DHb02]	Department of Health. Delivering 21st century IT support for the NHS: national specification for integrated care records service consultation draft. Version 1.22 (26 July 2002), http://www.connectingforhealth.nhs.uk
[DH03]	NHS Confidentiality Code of Practice, 2003, www.dh.gov.uk/
[DH07]	Department of Health, NHS information governance – guidance on legal and professional obligations, 2007, http://www.dh.gov.uk/
[DH08]	Department of Health, High quality care for all: NHS Next Stage Review final report, http://www.dh.gov.uk/
[DHa10]	Department of Health, Systems & Services, 2010, http://www.connectingforhealth.nhs.uk/
[DHb10]	Guidance for the Classification Marking of NHS Information www.connectingforhealth.nhs.uk
[DHc10]	Department of Health, Informatics Planning 2010/11 guidance, http://www.dh.gov.uk/
[DHe10]	Department of Health, Caldicott Guardian Manual, http://www.dh.gov.uk/
[DHd10]	Department of Health, NHS Data Model and Dictionary, http://www.dh.gov.uk/
[DHf10]	Department of Health, Information Governance Toolkit, https://www.igt.connectingforhealth.nhs.uk/
[GM09]	GMC, Confidentiality 2009, www.gmc-uk.org
[GO06]	D Gollmann, Computer Security, Wiley, 2006
[GO10]	About Google Health, http://www.google.com/intl/en-GB/health/about/
[GRa08]	T Greenhalgh, GW Wood, T Bratan, K Stramer, S Hinder, Patients’ attitudes to the summary care record and HealthSpace: qualitative study, BMJ 2008;336:1290-1295 (7 June), doi:10.1136/bmj.a114
[GRb08]	T Greenhalgh, K Stramer, T Bratan, E Byrne, J Russell, Y Mohammed, G Wood, S Hinder, Summary care record early adopter programme: an independent evaluation by University College, London, (2008) http://eprints.ucl.ac.uk/6602/

Developments in confidentiality and consent functions to support wider sharing of electronic health records in the UK

[HGJ99]	JG Hodge, LO Gostin, PD Jacobson, Legal Issues Concerning Electronic Health Information: Privacy, Quality, and Liability, JAMA. 1999;282:1466-1471.
[HH10]	What is the Hampshire Health Record? http://www.hantshealthrecord.nhs.uk/
[HL10]	Health Level Seven http://www.hl7.org.uk
[HO10]	Hippocratic Oath, National Library of Medicine, www.nlm.nih.gov
[ICa10]	NHS staff numbers, NHS Information Centre http://www.hesonline.nhs.uk
[ICb10]	Hospital Episode Statistics, NHS Information Centre http://www.hesonline.nhs.uk
[ICO10]	Information Commissioner, View of the changes to how health records are maintained, http://www.ico.gov.uk
[IS10]	ISO/TC 215, 2010, The Joint Initiative on SDO Global Health Informatics Standardization, http://www.global-e-health-standards.org/
[IS88]	"Information Processing Systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture", ISO 7498-2, ISO/IEC, 1988
[Ka06]	D Kalra, Electronic health record standards, IMIA Yearbook of Medical Informatics 2006. International Medical Informatics Association and Schattauer, Stuttgart, Germany, pp. 136-144.
[LE05]	B Lewis, B Chang, C Friedman, Section 1 Consumer Health Informatics, 2005, Consumer Health Informatics: Informing consumers and improving health care, New York, USA, Springer
[MA01]	KD Mandl, P Szolovits, IS Kohane, Public standards and patients' control: how to keep electronic medical records accessible but private, BMJ 2001; 322:283-287
[MI10]	Welcome to Microsoft HealthVault, http://www.healthvault.com/Industry/index.html
[NA06]	National Audit Office, The National Programme for IT in the NHS: NAO report 2006, http://web.nao.org.uk/
[NE10]	DICOM, 2010, http://medical.nema.org/
[NI09]	National Information Governance Board, NHS Care Record Guarantee, 2009, http://www.nigb.nhs.uk/guarantee
[PO99]	R Porter, The greatest benefit to mankind: a medical history of mankind, ISBN: 9780393319804, 1999
[RA96]	RJ Anderson, A Security Policy Model for Clinical Information Systems, 1996 IEEE Symposium on Security and Privacy, ISBN: 0-8186-7417-2
[RI97]	DM Rind, IS Kohane P Szolovits, C Safran, H Chueh GO Barnett, Maintaining the Confidentiality of Medical Records Shared over the Internet and the World Wide Web, Medicine and Public Issues, July 15, 1997 vol. 127 no. 2 138-141,
[SC10]	Your Emergency Care Summary: What does it mean for you? http://www.scotland.gov.uk
[SN10]	Online SNOMED CT Browser http://semfinder-snomed.ch
[TA06]	PC Tang, JS Ash, DW Bates, JM Overhage, DZ Sands, Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption, Journal of the American Medical Informatics Association, Volume 13, Issue 2, March-April 2006, Pages 121-126,
[TF97]	T Ferguson, Health online and the empowered medical consumer. Jt Comm. J Quality Improvement 1997; 23: 251-257, Medline
[WA10]	Individual Health Record http://www.wales.nhs.uk/