Report

South Staffordshire Health Community

EHR Security Policy

Working Draft Version 2.4

October 2001

Secta
PARTNERS FOR CHANGE

South Staffordshire Health Community

EHR Security Policy

1 INTRODUCTION

1.1 Background

1.1.1 Following its initial Electronic Health Record (EHR) pilot, the Electronic Health Record has become one of the four national pan-community ERDIP demonstrator sites. The ultimate concept of an EHR is that summary patient information can be accessed from anywhere in the country at any time of day by a clinician with a legitimate reason for viewing it.

1.1.2 As a pan-community initiative, the EHR raises concerns about protecting the confidentiality of patient identifiable data and raises issues about the sharing of clinical data within the NHS family and with partner agencies.

1.1.3 It is normal practice within the NHS to share information about patients. There is, however, concern that the Data Protection Act, the Human Rights Act and Caldicott principles are correctly applied to sharing information via the EHR.

1.1.4 In order for the EHR to function effectively, it is essential to have a security policy (based on a realistic risk analysis) to be used by the organisations maintaining the EHR and the individuals accessing it. If necessary, this policy can be tested against national policy guidelines and the appropriate Acts.

1.2 Purpose of this Document

1.2.1 This document represents the security policy to be applied to the EHR within South Staffordshire. Its primary purpose is to protect the data transmitted from local feeder systems and held on the central EHR server but, as part of that remit, also contains requirements for the security of such data when held on the various remote servers in organisations using EHR information for operational purposes.

1.2.2 The document is a national deliverable to the Electronic Records Development and Implementation Programme (ERDIP), comprising I1: Security and Confidentiality Policy, I2: User Guidance, I3: Inter-organisational data sharing protocol. [Deliverable I4 on consent procedures will be added later.]

1.3 Target Audience

1.3.1 The policy is drafted to:

- Obtain the agreement of the South Staffordshire EHR Programme Board.
- Inform the South Staffordshire EHR Information Security Officer.
- Inform local Information Security Officers and System Owners in South Staffordshire.

1.4 Terminology

1.4.1 Throughout this paper, the following terms will apply:

- 'Clinician' will be used generically to encompass all healthcare and healthcare related professionals, i.e. doctors, nurses, paramedics, therapists, approved social workers and pharmacists etc., engaged in the care of the patient.

- 'NHS Family' will be used to denote NHS organisations, including GPs.

- 'Extended NHS Family' will be used to denote NHS organizations and GPs plus Social Services and NHS related organizations such as opticians, nursing homes, charities, dentists etc. who are not part of the NHS but who contribute to patient care or well being.

- 'Third Party' is an organisation that is neither NHS or extended NHS family.

1.5 Sources

1.5.1 The following documents were referenced as part of this review:

- South Staffordshire EHR Threat Analysis, March 2001.

- South Staffordshire EHR User Requirement Version 1.2 dated August 2001.

- South Staffordshire Initial Draft EHR Security Policy Version 0.3.

- Walsall ERDIP Security and Confidentiality Policy.

- Gloucestershire NHS Information Security Policy.

- North and Mid Hampshire Central Hampshire Electronic Health Record Demonstrator, January 2001, Product T9: *Information Sharing Protocol*.

- Longstaff et al *A model for accountability, confidentiality and override for healthcare and other applications* ERDIP Paper 2001

- Thick, M et al *An authorisation model based on accountability and consent*. ERDIP Paper 2001

- South Staffordshire Technical Report: *EHR Confidentiality Model Review*, CSW, Version 0.2 April 2001.

2 MANAGEMENT OF SECURITY FOR THE EHR

2.1 Introduction

2.1.1 The nature of the EHR makes the management of security rather complex. In order for this security to be effective, it is necessary to understand:

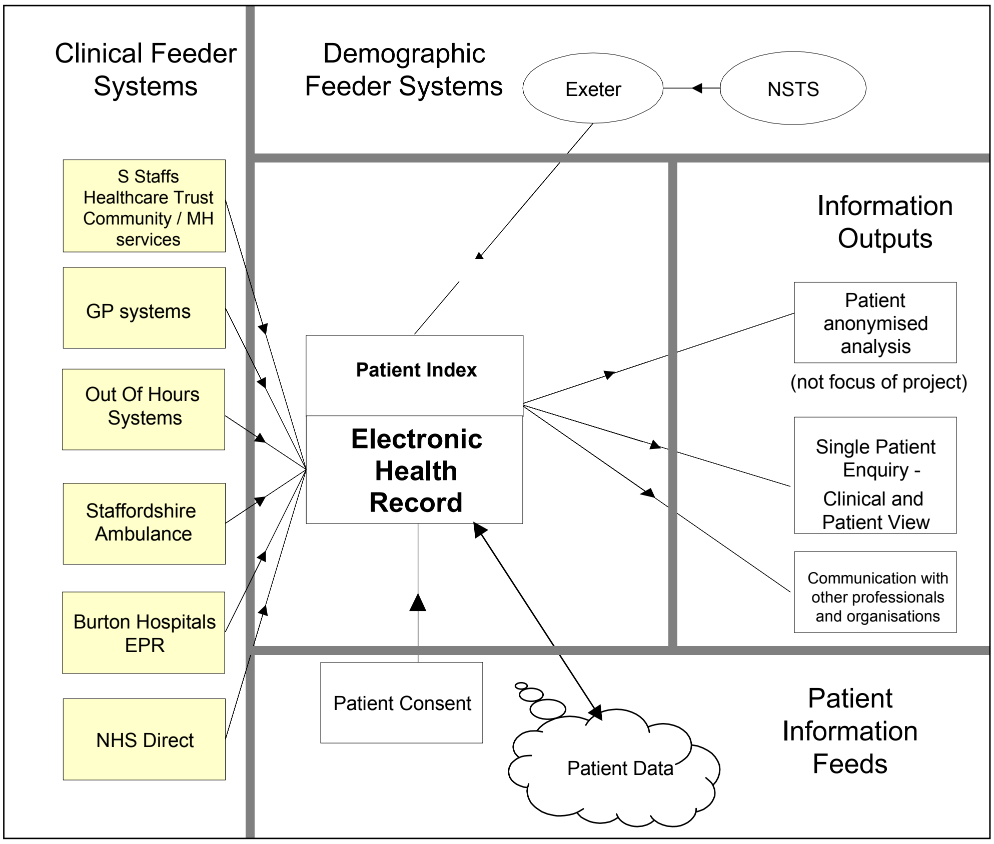
- The concept of the EHR.
- The scope of the EHR security policy and information sharing protocol.
- The technical implementation of the EHR concept.
- The responsibilities for security and the management framework.
- The relationship between the security policy for the EHR main server and the security policies operated at organisations within the NHS extended family.

2.2 The Concept of the EHR

2.2.1 The concept of the EHR is defined in the EHR User Requirement and is illustrated in **Figure 2-1**. The EHR receives data feeds from the 'Exeter' system for demographics and from a variety of clinical systems throughout the South Staffordshire Community. Patients will also add information to the EHR and procedures will be put in place to gain their informed consent to their information being shared.

2.2.2 The EHR will provide single patient views of the information for clinical professionals with a need to know, and for patients to review. The EHR provides integrated e-mail facilities for clinical professionals to contact one another in relation to information found in the EHR in support of patient care. Anonymised aggregate analyses will also be available.

Figure 2-1: The EHR Concept


Clinical Feeder Systems
Demographic Feeder Systems
Exeter
NSTS
S Staffs Healthcare Trust Community / MH services
GP systems
Out Of Hours Systems
Staffordshire Ambulance
Burton Hospitals EPR
NHS Direct
Patient Index
Electronic Health Record
Information Outputs
Patient anonymised analysis
(not focus of project)
Single Patient Enquiry - Clinical and Patient View
Communication with other professionals and organisations
Patient Consent
Patient Data
Patient Information Feeds

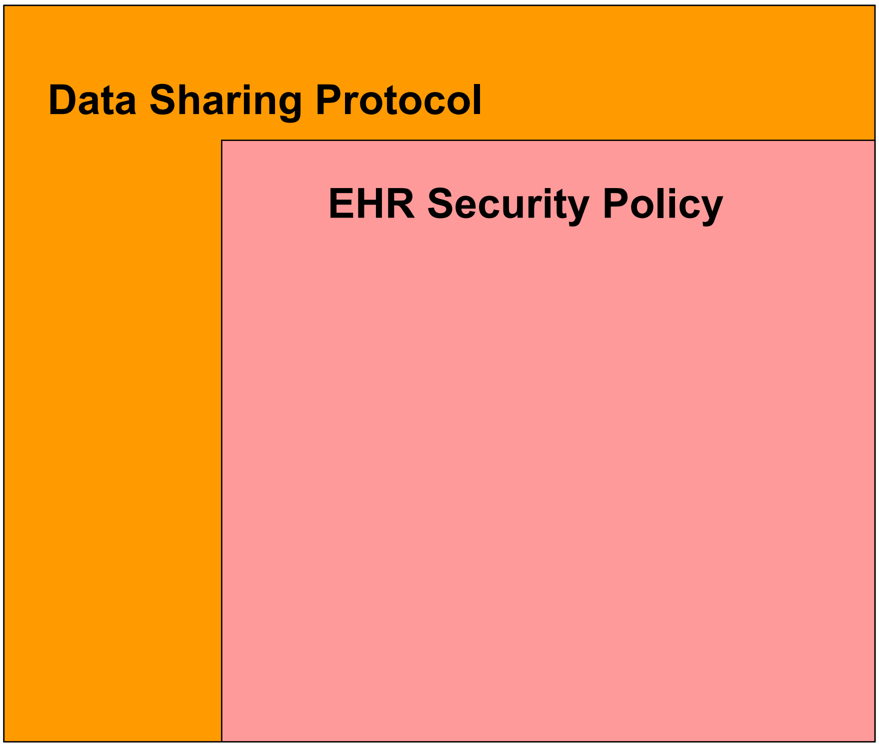
2.3 The Scope of the EHR Security Policy and Data Sharing Protocol

2.3.1 This **information security policy** is concerned with EHR information held primarily on automated systems comprising servers, workstations and networks, although it also covers the handling of physical media such as printed paper versions of the EHR. It sets out the measures that South Staffordshire is committed to putting in place in order to protect its EHR information assets covering technical measures and associated manual procedures.

2.3.2 The **data sharing protocol** attached as **Appendix D** to this policy represents an agreement between two or more organisations about the standards for handling data that will apply when one organisation passes its information to another, e.g. when an EPR system passes data to the EHR. It seeks to establish a level of trust between the participants and is concerned primarily with information control between organisations.

2.3.3 **Figure 2-2** shows the scope of the EHR security policy and the data sharing protocol with respect to the EHR concept.

Figure 2-2



2.4 Security and The Technical Implementation of the EHR Concept

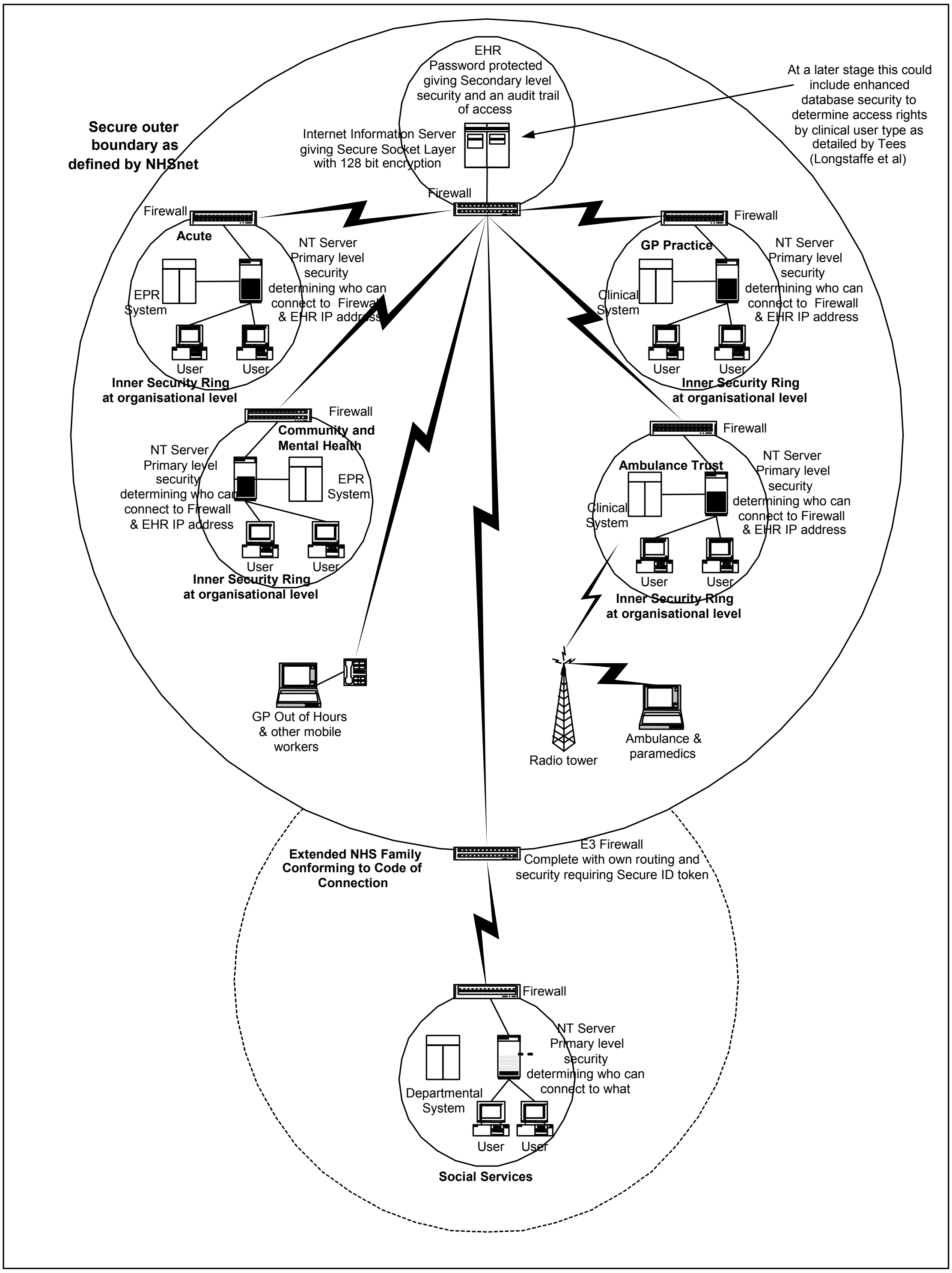
2.4.1 The technical infrastructure to implement the EHR concept is shown in **Figure 2-3**. In essence this shows that the EHR within South Staffordshire comprises a central EHR server (maintained by InfoSys, South Staffordshire's IM&T Agency) networked to a number of remote systems which feed information into the central server on a regular basis. The organisations that feed the central server also use the network to draw down summary information about patients in order to assist with their care.

2.4.2 This configuration raises a number of issues for the management of EHR security, since attacks can be made directly on the main EHR server and the information it contains or indirectly through security weaknesses at the sites using EHR information

2.4.3 The scope of this policy is restricted to protecting the information held on the main server. However, as one of the threats identified by the risk analysis was unauthorised access to patient data, it does lay down a series of requirements which NHS organisations and other members of the extended NHS family must reflect in their local security policies and adhere to. This ensures a set of minimum standards to protect EHR data whether on the main server or at remote locations.

2.4.4 The philosophy behind the security policy is therefore the establishment of a "web of trust" across all organisations using the EHR. This relies upon each organisation having in place security policies that either match or exceed the requirements set out in this policy.

Figure 2-3: EHR Physical Security Model

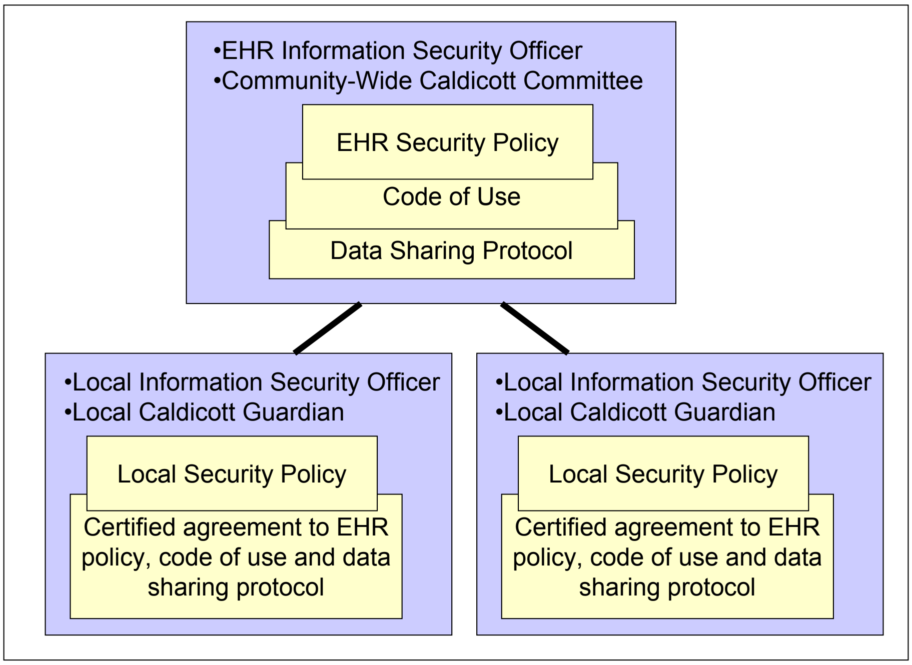


2.5 Security Responsibilities and Management

2.5.1 For EHR information to be properly controlled and protected, it is important that individuals and organisations are clear about who owns specific items of information and/or information systems. Within the South Staffordshire health community, the security of EHR information will be managed professionally and to the highest standards, including BS7799. Owners will be identified for specific information systems and, where appropriate, specific datasets. These owners will work with Caldicott Guardians to determine appropriate data sharing protocols, access protocols and appropriate security practices and procedures.

2.5.2 The broad relationships are illustrated in the Figure.

Figure 2-4


•EHR Information Security Officer
•Community-Wide Caldicott Committee
EHR Security Policy
Code of Use
Data Sharing Protocol
•Local Information Security Officer
•Local Caldicott Guardian
Local Security Policy
Certified agreement to EHR policy, code of use and data sharing protocol
•Local Information Security Officer
•Local Caldicott Guardian
Local Security Policy
Certified agreement to EHR policy, code of use and data sharing protocol

Responsibility of Security Managers

2.5.3 The Director of the South Staffordshire ERDIP Programme is responsible for the overall security of the EHR project within South Staffordshire. He will ensure that all organisations meet the standards set out in this policy, complete a certificate of compliance and sign the agreed data sharing protocol.

2.5.4 Each organisation participating in the South Staffordshire EHR pilot is responsible for any information it holds, including local EPR information and any information that is accessed from the EHR. The Information Security Officers within these organisations (who are responsible for the implementation and enforcement of their individual Information Security Policies) will have organisational security management responsibilities for:

- Monitoring and reporting on the state of information security within their own organisation.
- Ensuring that an Information Security Policy is implemented throughout their own organisation that contains all of the provisions of this EHR security policy.
- Developing and enforcing detailed procedures to maintain security.
- Ensuring compliance with relevant legislation.

- Ensuring that staff are aware of their responsibilities and accountability for information security.

- Monitoring for actual or potential information security breaches.

2.5.5 Detailed responsibility for particular systems will be delegated to the relevant systems managers.

Responsibilities of Caldicott Guardians

2.5.6 Caldicott Guardians will have responsibility for ensuring that everyone in their organisation conforms to the Caldicott Principles regarding the protection and use of patient identifiable information within the EHR. This will include the following responsibilities:

- Ensuring the organisation has policies in place to ensure the confidentiality and security of person identifiable information.

- Maintaining criteria for staff to use when deciding whether to share information against a patient's wishes.

- Acting as a point of appeal to a person whose information is to be used or disclosed against their wishes.

- Convening an Appeal Panel when a person appeals.

- Offering advice to Staff and Clinical Leads where use or disclosure of information is needed and consent has been refused.

Staff Responsibilities

2.5.7 All staff and all those carrying out work on behalf of the NHS have a legal duty of confidence to patients. It is each individual's responsibility to comply with the EHR security policy and to ensure that local practice reflects its requirements as laid out in the example 'Code of Conduct for using the EHR' in **Appendix B** to this document. Specifically:

- Access to EHR information is restricted to those staff who have a justifiable need to know in order to carry out their job effectively.

- All staff must ensure that they comply with security awareness programmes provided by the EHR Management.

- Staff must not share their passwords.

- All staff should report any breaches in information confidentiality and security through the incident reporting process (see **Figure 4-1**).

- All staff should inform patients and obtain consent that the information may be shared with others that need the information to provide the best care possible.

- Any intention to use or disclose information against a persons wishes must be notified to that person.

- All staff must be aware of the severe consequences of breaching confidentiality of person based information. It may result in disciplinary action, legal action and health professionals may be subjected to action from their regulatory bodies.

System Ownership

2.5.8 Each of the systems using the Electronic Health Record will be the responsibility of a specified "data owner". S/He will work in close liaison with the EHR Security Officer from the individual organisation's IM&T Department. The data owner will be responsible for ensuring compliance with the local security policy, ensuring the appropriate use of the equipment, and being responsible for troubleshooting and maintenance.

Patient Responsibilities

2.5.9 Patients also need to use the EHR in a responsible manner. A code of conduct for patients when reviewing their EHR or adding information to it is described in **Appendix C**. [#DN Need to check – 'placeholder' there at present]

2.5.10 The responsibility for ensuring that patients only access their own records in a secure setting and abide by the code of conduct rests with the organisational setting in which patients access the record. Thus the relevant local Information Security Officer will be responsible for ensuring compliance. Where access is outside an organisational setting, e.g. remote access from the patient's home, the overall EHR Information Security Officer will be responsible for ensuring compliance.

3 RISK ANALYSIS

3.1 Introduction

3.1.1 As part of the work to develop this security policy, a risk analysis was conducted to determine the threats to the EHR, the impact upon the EHR project should they occur, the likelihood of them occurring and the EHR's vulnerability to them. The results from that analysis are shown in the following tables.

3.2 Confidentiality

Threat	Impact	Manifestation	Likeli-hood	Vulner-ability
Public Disclosure	Embarrassment: ▪ Patient ▪ Organisation ▪ Political Patient Harm Legal Action	Absence of agreed sharing protocols across organisations Insecure data destruction procedures Staff Browsing Illegal staff access and theft (deliberate misuse of privileges) Carelessness by staff (open terminals etc) Unauthorised access to server by outsiders (hacking) Theft of Server Infiltration of EHR and/or its communication systems Patient with certain conditions may be driven to harm themselves should information be revealed	M M M L M L L L L	H H H H L L L L L
Disclosure to Patients/Family/Carers	Embarrassment Possible Legal Action Possible Patient Harm	Lack of agreed protocols across organisations Lack of clear policies Carelessness by staff Patient with certain conditions may be driven to harm themselves should information be revealed	H M L L	M M M L

Threat	Impact	Manifestation	Likeli-hood	Vulner-ability
Disclosure to Staff	Embarrassment Possible patient harm	Staff browsing Inappropriate access to subsets of data Patient with certain conditions may be driven to harm themselves should information be revealed	M H L	H M L
Misuse of Information by Organisation	Professional/ Caldicott action	Use of information for statistical and other management purposes leading to disclosure of clinical details to administrative staff Lack of clear policies	L M	M M
Legal Action	Financial Loss Detrimental effect on organisation's activities Embarrassment	Patient/Carer sues for breach of privacy/confidentiality Information Commissioner issues warning/order to cease processing	L L	M L
Public Confidence	Loss of esteem Loss of income? Professional embarrassment	Adverse publicity in local press regarding any breach Local networks/"Chinese whispers Patients refuse to attend a particular unit Any service contracts are revoked Any service contracts lose revenue	L M L L L	M L L L L

3.3 Integrity

Threat	Impact	Manifestation	Like-lihood	Vulner-ability
Adverse Effect on Clinical Decisions	Incorrect Diagnosis Patient Harm Legal Action	Currency of data is suspect Provenance of data is suspect Increased reliance on the EHR leads to clinical	M L L	M M L

Threat	Impact	Manifestation	Like-lihood	Vulner-ability
	Regulatory Action	decisions being taken on the basis of inaccurate data Clinical/Professional staff are subject to disciplinary action Patient sues the organisation for damages	L L	L L
Adverse Effect on Professional Confidence	Collapse of EHR Project/System Adverse Effect on NHS Information Authority credibility	Clinical staff refuse to use the system Professional bodies instruct members not to use the system Professional and Computing Journals run critical articles	M M M	H H H
Effect on Public Confidence	Loss of esteem Loss of income? Professional embarrassment	"Scare" stories in local press Local networks/"Chinese whispers Patients refuse to attend a particular unit	M M L	M L L
Legal Implications	Financial Loss Detrimental effect on organisation's activities Embarrassment	Patient sues for damages as a result of incorrect treatment Information Commissioner issues warning/order to cease processing	L L	M L
Business Disruption	System is taken out of operation Organisation has to revert to "old" manual procedures	Reliability of the information is such that, in the face of growing criticism, the organisation has to take the system off-line Increased reliance on the system means that the organisation may have withdrawn its manual procedures Management and statistical information is lost	L L L	L L L

3.4 Availability

Impact	Threat	Manifestation	Likelihood	Vulnerability
Adverse Effect on Clinical Decisions	Vital social information missed Incorrect Diagnosis Patient Harm Legal Action Regulatory Action	Failure of feeder system leads to out of date records Possibility of violent attack on clinical staff Treatment delayed through absence of quick clinical summary (eg allergies) Clinical staff unable to gain access to vital clinical information Incorrect treatment given due to unavailability of system Patient sues Action taken by professional regulatory bodies Action taken by Information Commissioner	L L M M L L L L	M M M L L L L L
Adverse Effect on Professional Confidence	Collapse of EHR Project/System Adverse Effect on NHS Information Authority credibility	Clinical staff reject use of the system Patient complaints arise due to obvious problems with the system Failure of pilot leads to adverse public criticism	M L L	M L L
Effect on Public Confidence	Loss of esteem Loss of income? Professional embarrassment	Patients lose trust in the system through adverse publicity Regular failures of the system create an overall bad image	L L	M M
Business Disruption	System is taken out of operation Organisation has to revert to "old" manual procedures	Regular failures require detailed investigation Difficulties in starting up old procedures if they have not been used for some time		
Legal Liability	Financial Loss Detrimental effect on	Patient sues for damages as a result of incorrect treatment	L	M

Impact	Threat	Manifestation	Like-lihood	Vulner-ability
	organisation's activities Embarrassment	Information Commissioner issues warning/order to cease processing	L	L
Financial Implications	Cost of rebuilding the system Cost of reconstructing data	Physical destruction of the system requires an expensive rebuild Inadequate backup leads to additional costs in rebuilding the record database		

3.5 Wider Risks and Issues

3.5.1 The planned implementation of the EHR envisages the creation of a structured summary of identifiable clinical and relevant social information. Unauthorised access to this data would therefore reveal a very detailed and potentially damaging insight into the health and lifestyle of an individual. Apart from the ethical considerations associated with such a disclosure, the potential for an expensive lawsuit, professional disciplinary action and unwelcome publicity is very large indeed.

3.5.2 Unauthorised access to the system through technical infiltration ie hacking, is a relatively minor threat giving the balance between technical complexity and any reward to be gained from such an exercise. However, the theft of the server is much more likely and, while likely to be driven by motives other than access to patient data still results in the same outcome: patient data released into the public domain in a readable and structured form.

3.5.3 Apart from ensuring that physical protection of the EHR server is as strong as possible, the only way of protecting the confidentiality of the data is through encryption of the data. The combination of clinical information and, in some cases, highly sensitive social data eg history of violence, child abuse etc., probably merits this level of protection particularly given other considerations such as wide geographical access across the network.

3.5.4 However, there is a danger that the EHR pilot in South Staffordshire may implement a solution, which is out of step with the wider encryption policy and associated trials currently being initiated by the NHS Information Authority. The EHR pilot recognises the sensitivity of the data and the need for encryption but is seeking advice from the NHSIA regarding its options in this area.

3.5.5 Another risk associated with the implementation of the EHR is the issue of seeking explicit patient consent to put information onto the system. This is a significant issue in that the Information Commissioner is quite clear that the current Act requires all patients to be informed of the purposes to which their information will be put. The Commissioner also requires that they should give explicit consent for their data to be used for these purposes. The risk is that if these procedures are not followed the possibility of a complaint and subsequent legal action by the Commissioner is very real.

3.5.6 This is not in itself an EHR issue. The EHR will be comprised of subsets of data "harvested" from a variety of feeder systems and, almost without exception, explicit consent is not currently obtained from the patient. Patient consent for data processing and sharing to support immediate patient care and treatment is generally assumed within the NHS.

3.5.7 South Staffordshire have agreed with the NHS Executive IPU and NHS IA that the pilot should test the extent to which implied consent can be used to protect the confidentiality of data in the EHR[1]. This assumption is only likely to be valid for the pilot (rather than for any operational system) and may be superseded by work from other ERDIP demonstrators or new national guidance. Work is currently being carried out by the NHS Executive into the options and costs for obtaining patient consent for information sharing within the acute sector for electronic patient records. **It is recommended that the EHR pilot continues to take advice from the NHS Executive regarding its position in relation to patient consent**.

[1] Meeting 4 October 2000 with NHS Executive IPU and NHS IA.

4 THE SECURITY POLICY

4.1 Introduction

4.1.1 This section contains the detailed security policy to be applied to the South Staffordshire EHR project. The countermeasures and associated procedures represent the minimum required to protect EHR data from the threats identified in the Risk Analysis section.

4.1.2 The countermeasures are described under the following headings:

- Feeding the right information to the EHR.
- Gaining consent to sharing the information.
- Using patient identifiable information in a secure way.
- Maintaining physical security.
- Controlling access to the EHR.
- Ensuring secure communications.
- Maintaining personnel security.
- Ensuring proper housekeeping.
- Maintaining a continuous service.
- Managing security incidents.
- Keeping the security policy up to date.

4.2 Feeding the Right Information to the EHR.

4.2.1 Purpose: This section of the policy outlines the measures required to ensure that only appropriate information is sent to the EHR.

Caldicott Principles

4.2.2 Information for patient care routinely flows within the NHS community and between NHS organisations and other bodies concerned with patient care or an individual's medical condition. The routine use of patient identifiable information for non-clinical purposes could have an adverse effect on the doctor/patient relationship. It could also infringe individuals' rights to have confidential information about them used properly. With this in mind, the organisations using the EHR have considered the recommendations of the Caldicott Committee and have established Caldicott Guardians to ensure that the flow of patient identifiable information is appropriately controlled. All data sharing will be strictly undertaken against the principle that "only those who are involved with the direct provision of care or with broader work concerned with the treatment or prevention of disease in a population should normally have access to patient identifiable information". This is not restricted to clinical staff but may include other staff, where they need access to clinical information systems (manual and electronic).

4.2.3 All organisations using the Electronic Health Record are fully committed to the Caldicott Principles regarding the protection and use of patient-identifiable information, namely:

- Only data relevant to the purpose of the EHR will be collected.
- Use and transfer of such information will only take place where the purpose is fully justified.
- Use and transfer will only occur when absolutely necessary.
- The minimum of patient identifiable information will be used – where possible, data will be anonymised.
- Access to information will be on a strictly "need to know" basis.
- Everyone must understand their responsibilities.
- The law must be understood and complied with.

Data Sharing Protocol

4.2.4 All organisations using the Electronic Health Record will be expected to sign an agreed data sharing protocol in addition to the certificate of compliance described previously. A copy of the protocol for use within the South Staffordshire health community is attached at **Appendix D**.

4.3 Gaining Consent to Sharing the Information

4.3.1 Purpose: To ensure that patients agree to the sharing of their information and to respect the views of those patients who do not wish their information to be shared.

4.3.2 The EHR project is fully committed to the principles of informed consent and will do everything in its power to ensure that all patients have the opportunity to give their consent to the use of their information within an EHR.

4.3.3 In order to achieve this, the existence of the EHR will be publicised through a co-ordinated awareness campaign involving posters, leaflets, radio and television advertising. This work is part of a national pilot on behalf of the Department of Health Information Policy Unit and the NHS Information Authority. This security policy will be updated in the light of the findings of the pilot and emerging national guidance. An inter-organisational data sharing protocol has been developed which reflects present thinking but may require amendment after the completion of the consent pilot (**Appendix D**).

4.3.4 As part of the informed consent process, individual patients will be given the opportunity to opt out of participation in the EHR scheme.

4.4 Using Patient Identifiable Information in a Secure Way.

4.4.1 Staff accessing the EHR will adhere to appropriate procedures to preserve the confidentiality of patient information. Such procedures will cover:

- On line interrogation of the EHR.
- Paper or facsimile copies of the EHR.
- Verbal communications relating to the EHR.
- Electronic mail.

Staff Access to Patient Information.

4.4.2 In order to protect patient confidentiality and prevent inappropriate use of sensitive personal data, staff must not:

- Access any EHR record (in either electronic or manual form) when they have no proper reason to do so in the course of their duties.
- Access records for their personal interest. This includes their own records.

4.4.3 EHR Management will:

- Decide what level of access staff have to any computer system and ensure that access is appropriate to the post and that necessary training is provided.
- Ensure necessary access to EHR information when authorised users are on annual or sick leave.
- Ensure that an audit trail of all access is provided.

4.5 Maintaining Physical Security of the EHR

4.5.1 Purpose: to guard against the physical denial of service, e.g. theft (one of the highest risks in the threat analysis), loss of power, fire, physical damage, etc.

Physical Access Control

4.5.2 All central processors, networked file servers and central network equipment associated with the EHR will always be located in secure areas with restricted access.

4.5.3 Local network equipment, file servers and NHSNet terminating equipment will always be located in secure areas and/or lockable cabinets.

4.5.4 Where appropriate, unrestricted access to EHR computer facilities will be confined to designated staff, whose job function requires access to that particular area or equipment. Restricted access may be given to other staff by the IT Department where there is a specific job function need for such access.

4.5.5 An appropriate EHR representative must accompany visitors to restricted areas at all times.

4.5.6 Authenticated representatives of third party support agencies will only be given access through specific authorisation from the EHR IT Department.

Equipment Siting and Protection

4.5.7 IM&T equipment will always be installed and sited in accordance with the manufacturer's specification. Equipment will always be installed by, or with the permission of, the EHR IT Department (this includes the attachment of PCs to the network).

- Where appropriate, environmental controls will be installed to protect EHR equipment. Such controls will trigger alarms if environmental problems occur. In such cases, where equipment is sited in a secure area, only authorised entry will be permitted.
- Smoking, drinking and eating will not be allowed in areas housing the central EHR computer equipment.

Power Supplies

4.5.8 The EHR main server will have generator backup power to the mains electricity supply.

4.5.9 Critical computer equipment will be fitted with adequate battery back-up to ensure that it does not fail during switchovers between mains and generator.

Cable Routing

4.5.10 All cabling (electricity or communications) between buildings will, where possible, be via underground conduit not accessible to unauthorised people.

4.5.11 All cabling associated with the EHR within buildings will be in conduits if surface mounted otherwise, within the framework of the building.

Equipment Maintenance

4.5.12 All central processing equipment, including file servers, will be covered by third party maintenance agreements.

4.5.13 All personal computers, terminals, printers and network components will be covered by maintenance agreements with third parties for repair of out of warranty equipment provided it is cost effective (each case will be judged on its merits).

4.5.14 All such repairs will only be made on approval by the EHR IT Department.

4.5.15 All such third parties will be required to sign confidentiality agreements.

4.5.16 Records of all faults or suspected faults will be maintained by the organisation's support department.

Security of Hard Disks

4.5.17 Hard disks on any machine associated with the EHR may contain sensitive or confidential data. Removal off site of such disks represents a potential threat to the confidentiality of patient data. Each such case will be judged on its merits balancing the need versus the risk of breach of confidentiality and then only to approved repairers who will have signed confidentiality agreements. Data and information will be overwritten, the equipment de-gaussed or media destroyed by the EHR team or approved repairers following documented procedures.

Security of Equipment Off Premises

4.5.18 Equipment and data will not be taken off site without formal signed approval, other than to transport it from one of Electronic Health Record's sites to another.

4.5.19 Lap top computers should have no downloaded EHR data contained in them and should not be left in open view in cars.

4.5.20 Portable PCs are very vulnerable to theft, loss or unauthorised access. Users should refer to the guidelines on the use of portable PCs.

4.5.21 To preserve the integrity of data, frequent transfers should be made from portable to system computers. They should be maintained regularly and batteries kept charged to preserve their availability.

Disposal of Equipment

4.5.22 EHR hardware disposal can only be authorised by the EHR IT Department. They will ensure that data storage devices are purged of sensitive data before disposal, or securely destroyed.

4.5.23 Unusable computer media should be destroyed (e.g. floppy disks, magnetic tapes, CD-ROMS).

4.5.24 Users should contact their local IT department for advice on disposal of media and equipment.

Disposal of Information.

4.5.25 All media containing patient information must be destroyed in a manner that ensures that data is not disclosed to an unauthorised person.

4.5.26 Paper Records. Paper and facsimile copies of EHR records must be destroyed once they are no longer required

4.5.27 Other waste must not be mixed with confidential waste.

4.5.28 The retention of personal health records is covered by the guidance in HC(99)053.

4.5.29 **Other Media.** Prior to the disposal of any processor or hard disk, the data will be erased or the disk totally destroyed. The EHR IT Department will ensure that hard disks are not handed over to suppliers in part exchange for new disks.

4.5.30 All removable media associated with EHR central systems e.g. tapes and floppy disks will be burnt. Sacks containing such media must be stored securely until collected.

Storage

4.5.31 The following procedures apply to the storage of EHR records:

- All paper based EHR information should be stored within locked rooms and only authorised staff are permitted access.
- Unless in active use such information will be stored in designated stores or libraries.
- EHR hard copy must not be left unattended in unlocked rooms.
- No written document containing patient data must be left visible where it can be read by anyone without authority to do so. This includes telephone messages, computer prints, letters and other documents.
- Patient data must not be stored on the hard disk of a laptop. Security precautions must be taken in accordance with the Organisation's I.M.&T. Policy & Procedures.
- Diskettes must be kept in proper storage boxes and locked away when not in use.
- The principles above apply to patient records at all times whether they are being used for clinical or other purposes e.g. teaching or research.

Transporting Information.

4.5.32 All users of the EHR must ensure patient information is always be transported in a manner that ensures that information is not accidentally disclosed to unauthorised people.

4.6 Controlling Access to the EHR – Logical Access Control

4.6.1 Purpose: to ensure that only those staff with an agreed right to access the EHR can do so. Access control also determines which parts of the EHR users can gain access to. The granularity of access control is still being considered by the EHR pilot.

Access to the EHR

4.6.2 For the purposes of the ERDIP project, clinicians within the NHS Family within South Staffordshire will be allowed access to the EHR providing they, through their organisations, comply with the EHR certificate of security compliance and the NHSNet Code of Connection.

4.6.3 At a later date, the same rights are expected to be able to be applied to social workers within the Extended NHS Family.

NHSnet requirements

4.6.4 All external connections to EHR systems must be via NHSnet. Where third parties are still in the process of gaining NHSnet accreditation, strong authentication procedures and technology must be introduced for all dial up connections to Electronic Health Record's IT systems where concurrent connection to the NHSnet is possible.

4.6.5 Electronic Health Record requires that third parties providing remote support do so over NHSnet.

Remote diagnostic services

4.6.6 The following provisions will apply to all access for remote diagnosis:

- Suppliers of EHR systems and software expect to have dial up access to such systems on request to investigate or fix faults. Electronic Health Record will permit such access subject to it being initiated by the EHR computer system and all activity monitored.

- Each supplier requiring remote access will be required to commit to maintaining confidentiality of data and information and only using qualified representatives.

- Each request for dial up access will be authorised by the EHR IT Department, who will only make the connection when satisfied of the need. The connection will be physically broken when the fault is fixed or the supplier ends the session.

- Modem links for diagnostic services will not be connected except in response to an authenticated supplier request, to prevent the possibility of unauthorised access.

- Enhanced modem security incorporating strong authentication measures will be introduced as soon as practicable for additional security.

Users' Access Control

4.6.7 The need for carefully controlled access to the information held on the EHR computerised information systems or in manual files, reports and other written communications is a central tenet of information security. The Caldicott report on the protection and use of patient-identifiable information recognises this, and a core responsibility of the Caldicott Guardians is define and assign access privileges to systems and their users. Guardians will be assisted in this task by individual system owners.

Registering Users for Access to Systems

4.6.8 Each organisation using the EHR will identify those systems, manual files, applications and networks which contain information to which access should be restricted, and will apply appropriate authentication controls commensurate with the sensitivity of the data held within or transmitted across them.

4.6.9 Formal procedures will be used to control access to EHR systems. Each application for access should be countersigned by an authorised manager, against the rules determined by the relevant Caldicott Guardian.

4.6.10 Access privileges will be modified or removed - as appropriate - when an individual changes job or leaves.

User Password Management

4.6.11 No individual will be given access to a live system unless properly trained and made aware of their security responsibilities.

4.6.12 Users must keep their passwords secret. Sharing passwords may be a disciplinary offence.

4.6.13 Passwords will be changed regularly – the main EHR systems will include password ageing to force users to change their password periodically.

Removal or Change of Access.

4.6.14 When a member of staff leaves or changes job within their organisation his/her manager must ensure that rights of access to EHR systems are rescinded or changed to meet the needs of the employee's new post,

4.7 Ensuring Secure Communications

4.7.1 Purpose: to protect the information flowing to the EHR from feeder system, the transmission of EHR information to local user sites, and the communication of EHR related information by users.

4.7.2 The following procedures will be adhered to for the transmission of EHR information.

Network Security

4.7.3 The organisations participating in the EHR project will manage their network services to at least the level of the NHSnet Data Networking Security Policy and its associated Code of Connection.

Postal Communications

4.7.4 The organisations using the Electronic Health Record will ensure that their staff adhere to any locally designated arrangements for sending and receiving information through the post.

Facsimile Security

4.7.5 The Electronic Health Record pilot will implement controls to ensure that fax communications are protected at all times. Patient information must only be sent by facsimile transmission as a last resort i.e. in a clinical emergency. As little information as possible should be included in any facsimile transmission . Only that which is essential at the time should be sent.

4.7.6 All facsimile transmission headers must include the name and telephone number of a contact person.

4.7.7 The following statement must appear on the facsimile transmission header:

> *'This facsimile transmission is strictly confidential and intended solely for the person or organisation to whom it is addressed. It may contain privileged and confidential information and if you are not the intended recipient you must not copy, distribute or take any action in reliance on it. If you have received this facsimile transmission in error, please notify us as soon as possible and return the facsimile transmission to us by post. The Organisation will reimburse you for the postage.'*

4.7.8 Before sending a facsimile transmission, staff must be satisfied that the receiving facsimile transmission machine is sited in a secure area. Staff must telephone in advance to ensure that it is manned.

4.7.9 Facsimile transmission must not be used for any patient attributable data concerning termination of pregnancy, fertility treatment, sexually transmitted diseases or HIV and AIDS.

4.7.10 When sending facsimile transmissions great care will be taken in entering the receiving facsimile number to minimise the risk of error. Where possible frequently used numbers will be programmed into the facsimile transmission machine memory.

Electronic Mail

4.7.11 All criteria applied to facsimile transmission apply to electronic mail.

Verbal Communications

The Electronic Health Record will ensure that all staff are advised and regularly reminded of their obligation, under the Caldicott guidelines, to respect the privacy of individual patients. This means holding conversations about patients discreetly and with due regard to the sensitivity of the subject under discussion.

4.8 Maintaining Personnel Security

4.8.1 Purpose: to ensure that information security is recognised as a shared responsibility and to protect the confidentiality, integrity and availability of EHR information from being compromised due to a breach of security (which could be accidental or malicious) occurring at any point in the information flow cycle.

Management Responsibilities

4.8.2 It is the responsibility of managers to ensure the following, with respect to their staff:

- All staff must sign confidentiality (non-disclosure) undertakings as part of their contract of employment.
- All current and future staff should be instructed in their security responsibilities.
- Staff using EHR systems will be trained in their use (See Appendix B for the proper use of the EHR).
- Managers will determine which individuals are to be given authority to access the EHR systems. The level of access to specific systems will be on a job function need, independent of status.
- Managers should ensure that the relevant EHR system managers are advised immediately about staff changes affecting computer access (e.g., job function changes, leaving department or organisation) so that passwords may be withdrawn or deleted.
- Managers must ensure that all contractors undertaking work for or on behalf of organisations within the Electronic Health Record pilot have signed confidentiality (non-disclosure) undertakings.

Staff Responsibilities

Each employee is personally responsible for ensuring that no breaches of information security result from their actions.

System Managers

4.8.3 Job descriptions for system managers will include specific reference to the security role and responsibility of the post.

Security Officer

4.8.4 The Security Officer will be responsible for ensuring these personnel security measures are complied with.

4.9 Ensuring Proper Housekeeping

4.9.1 Purpose: to protect the confidentiality, integrity and availability of information in the EHR through proper management of the large volumes of data in the EHR and the management of the regular updates to it.

Operational Controls & Housekeeping

4.9.2 Housekeeping is an integral part of the security equation. Lost or destroyed information could have a detrimental effect on the service provided or on the treatment of individuals. Effective operational controls and housekeeping mean that the availability of the EHR information base will be preserved. The housekeeping principle applies to both manual information, e.g. records management, manual filing systems, and to electronically held information.

Data Backup

4.9.3 The EHR will have an appropriate backup regime which reflects the importance of the data and which have been subjected to a proper risk assessment. This will consist of daily and weekly backups.

4.9.4 All backed up data will be stored securely at an off-site location.

4.9.5 Data owners should liase with their organisation's IT Department and system supplier to ensure that archiving of data is consistent with the legal requirements associated with the EHR.

Virus Control

4.9.6 The EHR project seeks to minimise the risks of computer viruses through user education, good practice and anti-virus software positioned in the most vulnerable areas.

4.9.7 Users should report any virii detected or suspected on their machines immediately to their IT Department.

4.9.8 Users need to be aware that no newly acquired disks from whatever source, are to be loaded unless they have previously been virus checked according to their organisation's policy on protection of data. This includes shrink wrapped software and disks used by support organisations for error detection.

4.10 Maintaining a Continuous Service.

4.10.1 Purpose: to ensure that the EHR remains available in the face of protracted loss of key systems.

Disaster Recovery & Business Continuity Planning

4.10.2 The EHR project recognises that IM&T systems are critical to the successful delivery of a comprehensive Electronic Health Record and that the protracted loss of key systems or user areas could be highly damaging to the pilot, particularly given the concept of an emergency care system available 24 hours per day, 7 days per week.

4.10.3 However, because of the EHR's experimental nature, a business continuity plan will not be prepared. In the event of a major loss of service, the options for recovery will be reviewed at the time depending on the level of findings already drawn from the pilot. [In the event of the EHR becoming an operational system core to healthcare delivery, a business continuity plan will be prepared.]

4.11 Managing Security Incidents

4.11.1 Purpose: To identify any breaches, or near-breaches, in security rapidly, to take appropriate action and to record how incidents were resolved to inform the audit and development of the security policy.

Security Incident Management

4.11.2 Part of the effective management of security risks involves the logging and resolution of incidents. Incidents may be reported locally or to the NHS Information Authority's Incident Reporting Scheme. The latter is not mandatory, though incidents shared through this agency will result in the sort of benefits associated with access to a larger knowledge base.

Security Incidents

4.11.3 A security incident is an event which may result in:

- degraded system integrity;
- loss of system availability;
- disclosure of confidential information;
- disruption of activity;
- financial loss;
- legal action;
- unauthorised access to applications.

Incident Reporting

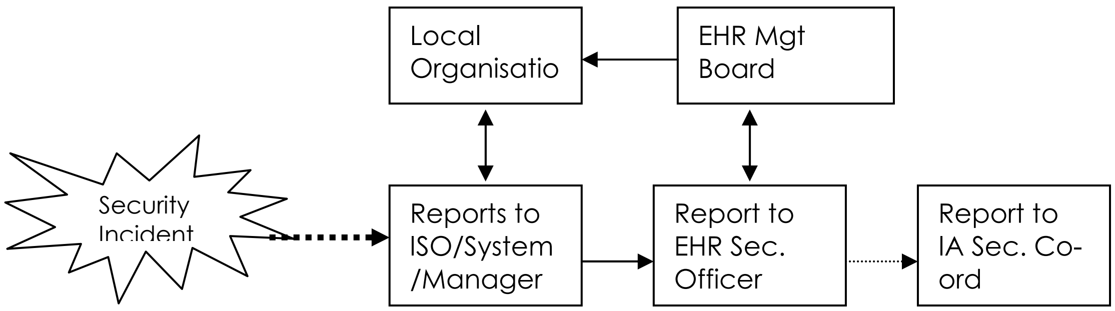
4.11.4 A formal incident recording and escalation procedure will be developed for the EHR. Information Security Officers in organisations using the EHR will report serious incidents to the NHS Executive's Security and Data Protection Programme via the EHR Information Security Officer. All security incidents that may have an impact on NHSnet will be reported immediately, by the EHR Information Security Officer to the NHSIA Security Co-ordinator or NHSnet Security Manager.

4.11.5 Incident recording will be used to log all unusual events. This mechanism will include what happened, what was done and final resolution.

4.11.6 Users will immediately report security incidents to their line manager, the relevant system manager and/or the Information Security Officer, as appropriate.

4.11.7 Actions and resolutions will be recorded by the relevant system manager and Information Security Officer. A collated set of incidents, covering both EPR feeder systems and the EHR will be maintained by the EHR Information Security Officer. The reporting chain is shown in the **Figure 4-1** below.

Figure 4-1



4.11.8 [Applicable when EHR moves from pilot to operational system] Major incident control procedures will be used to manage serious problems e.g., inability to recover critical live systems.

4.12 Keeping the Security Policy Up To Date

4.12.1 To update the security policy in line with changing threats, changing user requirements and the changing development status of the EHR.

Auditors

4.12.2 This policy, its implementation and systems will be subject to periodic review by both internal and external auditors, the recommendations from which will normally be implemented unless specific dispensation is given at executive management level. Any major security incident is liable to be referred to the auditors for investigation.

Method

4.12.3 The EHR will be subject to a security review by the system manager at least once every three years. Review of the policy is likely to be driven by development events rather than fixed time periods given the developing nature of the EHR and the changing range of threats as different organisations are granted access to the EHR.

4.12.4 The Review will include:-

- identification of assets of the system;
- evaluation of potential threats;
- assessment of likelihood of threats occurring;
- identification of practical cost effective countermeasures;
- implementation programme for countermeasures;
- Systems are liable to independent reviews by internal and external auditors.

Reporting

4.12.5 Each system review will include a formal report to the EHR Programme Board containing findings and recommendations.

Appendix

Certificate of Security Compliance

A

South Staffordshire Health Community

Electronic Health Record

Certificate of Security Compliance

This is to certify that ________________________________ (Organisation) has undertaken a formal review of its current information security arrangements and procedure against existing NHS standards, and that:

1. It has a formal IT security policy in place which meets, or exceeds the requirements of the main EHR Security Policy
2. All staff have read and understood the IT security policy
3. Appropriate training/briefing has been given to staff and that they fully understand their responsibilities in relation to the security of the Electronic Health Record
4. All staff have signed a confidentiality agreement as part of their contract of employment
5. Procedures are in place to notify the EHR central team in the event of a breach of security

Signed ____(Caldicott Guardian)

Date: ____

Appendix

B

Use of the Electronic Health Record A Good Practice Guide for Care Professionals

Use of the EHR

A Good Practice Guide

1. Purpose of the EHR

The purpose of the EHR is to provide a cradle to grave care record for an individual. It will contain significant health events, medications and information provided by the patient about their personal care preferences.

Its prime usage is in immediate and emergency care settings, allowing professionals access to pertinent details of the patient's history. This will speed assessment and facilitate patient care.

2. Legal Position with regard to EHR

The legal position of the EHR is no different to any other paper or electronic patient record and is subject to just the same legislation and constraints.

Patients give consent to the use of these records in their treatment and access to the records on a "need to know" basis only and it is your duty to respect their wishes.

For a complete legal position, this Good Practice Guide must be read in conjunction with your organisation's Security and Confidentiality Policy and the "Information Sharing Protocol".

3. Management of Access to EHR

The ERDIP technical team manage access to the EHR under the supervision of a Clinical Guardian. Access rights are granted to staff based on their clinical role, allowing different views of the record which pertain to their role. Staff have the ability to "override" their levels of access, in extenuating circumstances, in order to see the whole EHR for their patient.

However, **all** access to the EHR is audited. The audit trail provides details of who accessed what record, which part of the record, when and where. If you "override" your access level the incident is recorded and passed to your local Caldicott Guardian of patient information.

This management tool is for the protection of both patients and staff. It ensures that staff cannot "browse" records and that when an "override" takes place, the member of staff has a clear opportunity to justify their actions.

Organisational reviews of the audit trail occur on a routine basis.

- You are a healthcare professional with a legal and ethical code of conduct.

- The EHR is a tool to help you in your role.

- Please ensure that:

  - You **never** share your password with another member of staff.

  - You never access a patient record when you have no need.

  - You do not access records for personal interest.

  - *You only 'override your access level after making every reasonable attempt to gain patient consent.*

  - You always log out of the EHR when leaving a terminal or have a password protected screensaver installed.

  - You close each patient's EHR screen promptly when you have finished using it.

  - You only disclose information from the EHR under permitted circumstances – see the "Protocol for Inter-Organisational Sharing of Person Identifiable Information".

  - You treat all patient information with the strictest confidence.

4. Illegal use of the EHR

Existing contracts of employment and your organisation's Security and Confidentiality Policy outline the need to act lawfully and ethically.

Any breach of those standards without a clear and valid justification will result in disciplinary proceedings in line with your organisation's policy.

Such breaches may well leave the individual subject to civil action by the aggrieved individual under Data Protection and Human Rights legislation.

Appendix

C

Use of the Electronic Health Record A Good Practice Guide for Patients (Draft)

Use of the EHR

A Good Practice Guide for Patients

[NB. This is draft and requires further work]

Purpose of the EHR

The purpose of the EHR is to provide a cradle to grave care record for an individual. It contains significant health events, medications and information provided by the patient about their personal care preferences.

Its prime usage is in immediate and emergency care settings, allowing professionals access to pertinent details of the patient's history. This will speed assessment and facilitate patient care.

Legal Position with regard to EHR

The legal position of the EHR is no different to any other paper or electronic patient record and is subject to just the same legislation and constraints.

Patients give consent to the use of the EHR in their treatment and access by clinicians to the record is on a "need to know" basis only. It is their duty to respect your wishes.

Staff have the ability to "override" their levels of access, in extenuating circumstances, in order to see the whole EHR for their patient.

However, **all** access to the EHR is audited. The audit trail provides details of who accessed what record, which part of the record, when and where. If you "override" your access level the incident is recorded and passed to your local Caldicott Guardian of patient information.

This management tool is for the protection of both patients and staff. It ensures that staff cannot "browse" records and that when an "override" takes place, the member of staff has a clear opportunity to justify their actions.

Organisational reviews of the audit trail occur on a routine basis.

Your responsibilities when using the EHR

- You are a patient responsible for working in partnership with health professionals to maintain your health.
- The EHR is a tool to help you in your role.
- Please ensure that:
  - You **never** share your password with another member of staff.

- You only access your own record and immediately notify a member of staff if the record is not yours.
- You add information truthfully.
- You avoid any obscenities or libellous opinions.
- You always log out of the EHR when leaving a terminal and close your EHR screen promptly when you have finished using it.

Illegal use of the EHR

Any breach of these standards without a clear and valid justification may result in legal proceedings under the Data Protection Act and Human Rights legislation.

Appendix

D

Information Sharing Protocol

Version 1.0

September 2001

5 INTRODUCTION

5.1.1 The objective of the South Staffordshire Electronic Healthcare Record Demonstrator to develop an electronic healthcare record which supports 24 hour emergency health and social care for residents of South Staffordshire. Achieving this objective is dependent on information being exchanged between participating organisations in a seamless and consistent manner.

5.1.2 The endorsement of this agreement demonstrates this organisation's commitment to work in an information-sharing partnership, to govern the sharing of information, satisfy the requirements of the law and guidance, regulate working practices, and provide operational guidelines in both the disclosing and receiving organisations.

5.1.3 For ethical and legal reasons the primary concerns in sharing are about the appropriateness of the information content, and ensuring the security of that information. In summary, this means:

- Information to be shared must be purposeful and justified.
- Information should be specifically geared to the task it is intended to serve.
- The information should be sufficient and sharing should exclude unnecessary information.
- Information should normally be only shared with the informed consent of the subject.
- Information should be shared as part of appropriately planned and managed procedures.
- There should be designated accountability for shared information.
- Information should only be shared with 'agreed' information communities .
- Personal identifiers should be removed wherever possible.
- Agencies should take responsibility for ensuring proper procedures for compliance.
- Standards must be established to ensure that technologies used in information sharing are fully fit for the purpose.

6 PURPOSE

6.1.1 The purpose of this protocol is to provide a policy framework for the secure and confidential sharing of information between organisations developing the South Staffordshire EHR to enable them to meet the needs of the public for care, support and protection in accordance with government expectations as specified in the following documents:

- The New NHS Plan.
- Working in Partnership.
- National Service Frameworks.
- Information Sharing between the NHS and Local Authorities.
- Draft General Protocol for Sharing Information Between Agencies.
- South Staffordshire Health Community Local Implementation Strategy for *Information for Health* and *Building the Information Core*.

6.1.2 Its secondary purpose is to inform patients and clients of the organisations who are party to this protocol of the reasons why information about them may need to be shared and how this sharing will be managed.

7 SCOPE

7.1.1 The stakeholders in the EHR project are as follows:

- South Staffordshire Health Authority
- Etc
- Etc

8 GENERAL PRINCIPLES

8.1 The Sharing of Information for the South Staffordshire EHR

8.1.1 In seeking to share information to improve services and support to the population of South Staffordshire, the parties to this protocol will adhere to the following principles:

Commitment to necessary sharing of health information

- Organisations and agencies in South Staffordshire recognise that healthcare requiring a multi-agency approach cannot be achieved without the exchange of information about individual service users, levels of activity, the level and nature of resources and about their approach to addressing the issues. Their adoption of a multi-agency approach to address issues, therefore, includes **a commitment to enable such information to be shared**, albeit in a manner which is compliant with their statutory responsibilities.

General constraints on sharing information

- Where it is agreed to be necessary for information to be shared, information will be shared on a **need-to-know basis** only.

- **Non-NHS organisations recognise the requirements that Caldicott imposes on NHS organisations** and will ensure that requests for information from NHS organisations are dealt with in a manner compatible with these requirements.

- Information shared between organisations for a specific purpose will **not be regarded by the receiving organisation as intelligence for the general use of the organisation**.

- Organisations/agencies are fully committed to ensuring that they **share information in accordance with their statutory duties**. They will seek to put in place procedures which ensure that the principles of the Data Protection Act 1998 and other relevant legislation are adhered to and underpin the sharing of information between their agencies.

- When disclosing information about an individual, **professionals will clearly state whether the information being supplied is fact, opinion, or a combination of the two**.

- Personal information will only be disclosed where the purpose for which it has been agreed to share clearly requires that this is necessary. **For all other purposes, information about individual cases will be anonymised**, e.g. for:

  – assuring and monitoring the quality of care and treatment (e.g. through clinical audit);

  – monitoring and protecting public health;

  – co-ordinating NHS care with that of other agencies ;

  – effective health care administration, in particular;

  – - managing and planning services,

  – - contracting for NHS services,

  – - auditing NHS accounts and accounting for NHS performance,

  – - risk management,

  – - investigating complaints and notified or potential legal claims;

  – teaching;

  – statistical analysis and medical or health services research.

- Careful consideration will be given to the **disclosure of information concerning a deceased person** and if necessary, legal advice will be sought on each individual case.

- Organisations/agencies are committed to putting in place efficient and effective **procedures to address complaints** relating to the disclosure of information, and service users will be provided with information about these procedures.

Instances where disclosure will not occur.

- Patient information must not be disclosed under any circumstances for the purposes of **fund-raising or commercial marketing**.

- Disclosure of information on **HIV, AIDS, sexually transmitted diseases, assisted conception and abortion** is restricted by law. Information must only be disclosed by one of the very limited number of people authorised to do so and in accordance with the relevant statutes.

Consent to sharing information

- All organisations which are party to this protocol recognise their **duty of confidentiality.** Where they have obtained information in the special categories of the Data Protection Act about an individual, in the course of their direct contact with that person, they will seek to obtain the **explicit consent of that person to disclose that information to another organisation**. They will not disclose information without the consent of the person concerned, unless there are statutory grounds and an overriding justification for so doing.

- In seeking consent to disclose information, **an individual will be made fully aware of the information that will be shared** and the purposes for which it will be used. Individuals will be given every opportunity to gain access to information held about them and to correct any factual errors that have been made. Where professionals request that information supplied by them be kept confidential from the service user, the outcome of this request and the reasons for taking the decision will be recorded. Such decisions will only be taken on statutory grounds.

Ensuring staff implement the procedures

- Organisations will ensure that **all relevant staff are aware of, and comply with, their responsibilities** in regard both to the confidentiality of information about people who are in contact with their organisation/agency and to the commitment of the organisations to share information.

- Procedures will be put in place to ensure that **decisions to disclose personal information without consent** have been fully considered relevant to applicable legislation and Schedules 2 or, in the case of sensitive information, Schedule 3 of the DP Act 1998, and that these decisions can be audited and defended. All relevant staff will be provided with training in these procedures.

- Staff will be made aware that **disclosure of personal information which cannot be justified on statutory grounds** and under Schedules 2 or, in the case of sensitive information, Schedule 3 of the DP Act 1998, whether inadvertent or intentional **will be subject to disciplinary action**.

9 DISCLOSURE OF PERSONAL INFORMATION PROCEDURES

9.1 Obtaining consent

General

9.1.1 The procedures agreed by the agencies for obtaining consent recognises the need to handle the **seeking of consent in a sensitive manner**.

9.1.2 It is the responsibility of organisations to ensure that **consent is given on an informed basis**. This means that consent should only be given with the full understanding of what information will be shared, with whom and for what purpose.

Consent Materials

9.1.3 A **standard script will be adopted** by all agencies to ensure a consistent approach to consent seeking and, wherever possible, the material used will be common to all agencies. The material will explain:

- The rights of individuals under the Data Protection Act 1998, particularly in relation to sensitive information will be made available as follows:
- Details of the procedures in place to enable clients/patients to access their records.
- Details of the procedures which may have to be initiated when a member of staff suspects that an adult has been or is at risk of abuse. These procedures must include details of who information will be shared with at each stage, what information will be shared and how the information will be used.
- Details of the circumstances under which information may be shared without consent and the procedures which will be followed
- Details of the complaints procedures to follow in the event that the individual concerned believes information about them has been inappropriately disclosed.
- Details of how the information they provide will be recorded, stored and the length of time it will be retained both by the point of contact agency and the agencies to whom they may disclose that information.
- Details of the length of time for which consent to particular disclosures is valid.

9.1.4 Participating organisations will also make available a **copy of the protocol** covering the purpose for which consent to disclose is being requested at that point in time.

9.1.5 The material should be available in a **variety of formats and languages**. Agencies must also have access to appropriate means of communicating that information and ensure that these are made available if required.

Procedure for obtaining consent

9.1.6 **Consent will be sought at the earliest opportunity**. This should be at the first contact with the person concerned unless the individual is unable, at that time, to fully comprehend the implications or make an informed judgement. If, in the professional judgement of the staff member(s) concerned, it would be detrimental to the health of the person concerned to address these issues at that time, then the reason for not doing so should be recorded and arrangements agreed to complete this task at the first available opportunity.

9.1.7 **Consent-seeking will only be carried out by staff who have been trained in the procedures.** Staff will be trained to present and explain the issues to the individual, to request their consent to share personal information with other agencies and to explain the consequences if consent is not given.

9.1.8 **The patient, client or their guardian will be made aware:**

- That **personal information** acquired by an agency, in the course of their direct involvement with that person, **will only be disclosed to another agency with their consent** (unless for the purpose of protecting the vital interests of the client or the public).

- That information about their case may be shared with other agencies in order **to inform planning and development of relevant policies and procedures**. They should be assured that if this happens, under no circumstances will personal information be released. The data will be anonymised or shared in aggregated form.

- Of any **specific records or systems** which are maintained to support the purpose for which they are in contact with the organisation at that point in time and which require them to pass information about the case to staff based in another agency. They must be told the purpose and content of these records, details of how they are stored and who has access to them.

9.1.9 The person concerned **must be given sufficient time** to consider the material provided. There should be no doubt that the person concerned or, in the event that a person is unable to make informed decisions, their legitimate representative, have been given every help to access and understand the facts before being asked to give consent.

The patient or client decision

9.1.10 Where it has been established that a **patient or client is able to make an informed decision** then the member of staff seeking consent will first tell the client that:

- Everyone has a right to prevent the disclosure of information about themselves.

- It is a requirement of the Data Protection Act 1998 that consent to disclosure of information should be on an informed basis.

- The right to prevent disclosure is recognised by the organisation(s) involved. However, the organisation has a responsibility in some cases to take steps to prevent harm to an individual or to protect their vital interests. If, in a particular case, the organisation concludes that they have such a responsibility and this constitutes statutory grounds for disclosing information without consent, then they may exercise their right to do so.

9.1.11 Where a **person does not have the capacity to make an informed decision** but another person has authority to act as their guardian and take decisions on their behalf, then this situation must be explained to that person.

9.2 Recording Consent

9.2.1 **Participating organisations must have a means by which an individual or their guardian can record** whether they give consent to the disclosure of personal information and what limits, if any, they wish placed on that disclosure.

9.2.2 These limitations should be overridden only if there are statutory grounds for doing so and one of the conditions of Schedule 2 of the DP Act 1998 can be demonstrated. For sensitive information, one of the conditions of Schedule 3 of the DP Act 1998 must also exist.

9.2.3 **Individuals should be able to prescribe**, in respect of all information held by the contact organisation:

- Which organisations their information can and cannot be shared with.
- What information known to the contact organisation can be shared and what information should remain confidential.

9.2.4 In addition, in respect of sensitive information (as defined by the DP Act 1998) which is held by the contact organisation, individuals must be able to prescribe the explicit purposes for which they agree to this information being disclosed to another organisation.

9.2.5 This means that an individual must have access to their files in order to comprehend what information an organisation holds about them and must be **given an opportunity to amend and correct any information that is incorrect**.

9.2.6 In an urgent or emergency situation and in many routine referrals, it may be impractical for existing client records to be studied in detail and amended at that point in time. All organisations should therefore have procedures in place to ensure that clients are fully informed at all times of the content of their records (both manual and computerised) and have opportunities to amend the contents if they are wrong.

9.2.7 Under no circumstances will consent be sought, or taken to have been given, unless the individual or their representative has been fully informed of the consequences of giving consent. As such, consent forms will contain a facility for the individual to confirm that such information has been made available to them.

9.2.8 The consent form should be stored in the individual's personal record file and the file marked to indicate that consent forms are present. **A copy of the consent form should be given to the individual**.

9.2.9 If a person **limits the disclosure of information** in any way, then this **must be flagged both on the consent form and on their records** in such a manner that any member of staff subsequently involved with that person, is alerted to this limitation of consent. Information which is held with this limitation should be stored in such a manner that access can be controlled. This limitation of consent should be recorded whether or not a decision is taken to disclose without consent.

9.2.10 **Consent** to disclosure of personal information for a particular purpose, **will be limited to a period to be specified within individual protocols**, unless the individual concerned withdraws consent in the interim period. A record must be kept of the date on which consent was given, the date on which it is due to expire and the date on which it was withdrawn, if applicable. If at any time following the withdrawal or expiry of consent, an organisation wishes to disclose that information for the same or another purpose, then consent will need to sought again.

9.3 Checking for Consent

9.3.1 An individual's personal **paper or electronic case file should always be checked** before personal information is disclosed to another agency. Members of staff without access to an individual's case file must check with case holders before releasing information.

9.3.2 It is essential that the person receiving a request for personal information about a client first checks that a **consent form (electronic or paper) accompanying the request does not contradict** any previous consent agreements held in their organisation's case file. Any contradictions must be resolved before information is released and should be notified to the persons responsible for controlling access to information. Legal advice should be taken if necessary.

9.3.3 Particular care should be taken before sensitive information as defined by the DP Act 1998 is released. Sensitive information should only be released if its disclosure is critical to the case and explicit consent has been given to its release for that purpose.

9.3.4 It is recognised that in particular investigations (e.g. adult protection enquiries) the significance of information is often not apparent at the early stages and agencies may put in place procedures which enable them to share all information they hold about the person(s). In this case individual protocols will clearly state that such an agreement has been made and will set out the specific arrangements they have put in place to limit the access to such information to those with a need to know.

9.4 Disclosing Information with Consent

9.4.1 Patient identifiable information **can be disclosed**:

- With the patient's written consent, for an agreed healthcare purpose, on a need to know basis if the person receiving the information is concerned with the patient's treatment.
- When the information is required by law or under a court order.
- In child protection proceedings if it can be established that the information required is in the public interest.
- Where disclosure can be justified for another purpose. This is usually for the protection of the public or the individual.

9.4.2 The Organisation must be able to justify any decision to pass on information.

9.4.3 When disclosing information about individual clients, organisations must indicate to what extent this information is current, is factual or an expression of opinion and whether it has been confirmed as correct by the individual.

9.4.4 Organisations will be kept fully informed about the disclosure of information originating from their files, whether it is with or without the consent of the person to whom the information pertains. Accurate records must be kept of what information has been disclosed to whom, the source of the data disclosed, and the date on which it was disclosed and protocols must specify who will be responsible for ensuring that this is done.

9.5 Disclosing Information without Consent

9.5.1 The **disclosure of personal information without consent must be justifiable on statutory grounds** and meet one of the conditions of Schedule 2 of the DP Act 1998. In addition, the disclosure of "sensitive" information without consent must meet one of the conditions of Schedule 3 of the DP Act 1998.

9.5.2 Each participating organisation will therefore appoint **a person or persons who has the authority and knowledge to take responsibility for such a decision**. This authority will be available at all times, to enable emergency situations to be dealt with.

9.5.3 The person(s) designated will be provided with clear guidance to enable them to decide whether there are statutory grounds for disclosure without consent and whether any of the conditions in Schedule 2 or 3 of the DP Act can be met. If they are in any doubt, they should **refer the case to the designated legal expert** for advice. It is the responsibility of each organisation to ensure that the responsible staff know how and who to contact for legal advice. Individual protocols will indicate who will provide the legal expertise for the client group covered by the protocol.

9.5.4 If information is disclosed without consent, then **full details will be recorded** about the information disclosed, the reasons why the decision to disclose was taken, the person who authorised the disclosure and the person(s) to whom it was disclosed. Individual protocols will specify the person(s) responsible for ensuring this happens.

9.5.5 Wherever possible **organisations will nominate contacts for the receipt of personal and sensitive information**. These contacts will be responsible for instigating the agreed security procedures to ensure that this information is restricted to those who need to know it for the purposes agreed. Individual protocols will set out the contacts agreed for the purposes integral to that protocol.

9.5.6 Recipients of the information will be made aware that it has been disclosed without consent and will put agreed security procedures in place.

9.5.7 A record of the disclosure will be made in the client's case file and the client must be informed if they have the capacity to understand.

9.6 Avoiding Unintentional Disclosure of Patient Information

9.6.1 All staff must take care to ensure that unintentional breaches of confidence do not occur. Examples of practices to avoid:

- Leaving files, facsimiles, computer prints, terminals, written phone messages etc. lying in places where they can be read by patients, visitors and other staff.
- Discussing patient details in areas where they may be overheard.
- Leaving messages stuck to computer screens.
- Pinning notes on notice boards even in private offices where staff and other visitors to the office may read them.
- Generating excess copies of computer reports.
- Using old/spare computer reports for scrap paper.

9.6.2 Staff must also be aware that people may seek to gain information by deception and must therefore be on their guard to prevent this.

9.6.3 Information must not be passed by telephone unless the recipient has been positively identified and is authorised to receive it.

9.7 Staff Guidance on Consent-Seeking

9.7.1 To support staff, each organisation will put in place procedures which give clear guidance on:

- The need to seek consent and the consequences of not doing so.
- Who is trained to seek consent and how their involvement should be initiated.
- Who is able to take a decision on behalf of another person.

- The circumstances under which information may be disclosed without consent.

- Who can authorise the disclosure of information without consent and how this authority should be requested.

- The records which must be kept of this process.

- The procedures for recording and storing consent to share information.

- The procedures for recording limitations of consent to share.;

- The procedures to be followed when consent is limited.

9.7.2 Where a patient has expressed a wish that information be withheld in total or limited:

- The consequences for their treatment (for example where non-disclosure will affect the Organisation's ability to work with another agency such as the Social Services Department) must be explained to the patient.

- The patient's wishes must be communicated to other staff who need to know particularly to the Reception and Enquiry Office at the organisation.

- The patient's wishes must be respected unless overruled by other circumstances.

9.7.3 Individual protocols will include a date by which all parties to the protocol will have these procedures in place and will set out how progress in implementing these procedures will be monitored.

9.8 Maintaining Contact Details

9.8.1 All organisations will maintain a list of the staff who have been trained to seek consent. Organisations will provide the names and contact details of members of staff:

- To whom requests for information for particular purposes should be directed

- Who can authorise disclosure in respect of individual protocols.

- Who will provide legal advice in respect of the disclosure of information concerning a particular client group.

- Who are authorised to receive confidential information in respect of a particular purpose.

9.8.2 Individual protocols will list or refer to the contacts specific to that particular protocol and specify how this list will be maintained.

9.9 Audit of Consent Procedures

9.9.1 Managers should audit policies and procedures within their organisation and provide a record of the success or failure of the policies and procedures to the department for their action and retention.

10 SPECIFIC ORGANISATIONAL ISSUES RAISED BY INFORMATION SHARING

10.1 Relatives, Friends and Carers.

10.1.1 The “Patient’s Charter” states that “if you agree you can expect your relatives and friends to be kept up to date with the progress of your treatment”. If a patient expresses a wish that relatives etc. should not receive any information, this wish must be respected.

10.1.2 In order to ensure that this occurs, staff must ensure that reception areas are aware of the patient’s wishes.

10.2 The Media.

10.2.1 Information must not be passed to the press or to broadcasters without the written consent of the patient. All requests from the media must be dealt with under the Organisation’s procedure for handling media queries.

10.3 Religious Bodies.

10.3.1 Hospital chaplains are part of the care team and as such have access to appropriate patient information. However the fact that a patient has given his/her religion does not imply consent for disclosure to religious bodies outside the Organisation nor that a patient wishes to see a religious representative whilst in hospital. The patient’s views must be sought about contact from religious representatives either whilst in hospital or after discharge.

10.4 Voluntary Bodies.

10.4.1 Staff must not release information to voluntary bodies without gaining appropriate written consent, either from the patient or consultant under the Organisation’s policy for gaining consent.

10.5 Other Hospitals.

10.5.1 Written consent must be obtained from the patient and the consultant who provided the most recent treatment to the patient. If that consultant is not available the Clinical Director of the appropriate specialty must authorise release. If case notes are requested only copies must be sent. These must be sent in a sealed envelope, registered if by mail.

10.6 Private Hospitals/Clinics/Practices

10.6.1 As for 'Other Hospitals' with the addition that only copies of case notes must be sent. These must be sent in a sealed envelope, registered if by mail. An invoice must then be sent to the requestor to cover the cost of the copies and delivery. The cost per copy must be obtained from the Medical Records Manager or his/her deputy.

10.6.2 Other agencies providing care e.g. Local Authorities, agencies providing care to offenders .

10.6.3 It is important that the duty to maintain confidentiality does not prevent the proper sharing of information in support of good care of the patient.

10.6.4 Policies for clinical departments must state in detail how liaison with other agencies will occur and how the confidentiality of information will be safeguarded. These policies must contain guidance on dealing with emergency requests at any time. The policies must specify the role of the on-call manager.

10.6.5 Only in exceptional circumstance must information be disclosed to a third party without written patient consent. The decision to do so rests with the consultant treating the patient in accordance with Organisation policies. Out of hours or in his/her absence the on-call manager must decide with, if necessary, the advice of the Organisation's solicitor.

10.7 Department of Social Security.

10.7.1 Information will only be passed to the local Benefits Agency by General Office staff if all the following conditions are met and supported by authorised documentation:

- The patient is receiving benefit.
- The patient has been in hospital for six weeks.
- The Organisation has a mandate to handle the patient's financial affairs.
- The patient has agreed to the information being passed on.

10.7.2 Where another person e.g. a friend or relative is looking after a patient's financial affairs, information must not be passed on by Organisation staff.

10.8 The Police.

10.8.1 Information must not be passed to the police without the written consent of the patient except where this is necessary to assist in the investigation of serious crime. The following criteria must be satisfied:

- Without disclosure, the task of preventing, detecting or prosecuting the crime would be seriously prejudiced or delayed.

- Information is strictly relevant to a specific investigation.
- There are satisfactory undertakings that the information will not be passed on or used for any purpose other than the current investigation.

10.8.2 There is no hard and fast definition of a serious crime and this is a grey area. Information must only be released to the police by a senior manager after consultation with the GP/ consultant most recently responsible for the patient's care (or in his/her absence, the on-call consultant for the specialty). The Organisation's solicitors must be consulted if there is any doubt or if clarification is required.

10.9 Teaching and Research.

10.9.1 Patient information must not be used for teaching or research without the written consent of the patient.

10.9.2 Patients must be asked whether they wish to participate in teaching and, if they do not, their wishes must be respected. Patients must be informed of the Organisation's teaching status and information must be contained in the printed information given to patients.

10.9.3 All research and study projects must be approved by the Local Ethical Research Committee. The Committee must be satisfied that:

- Confidentiality will be safeguarded.
- The use of identifiable patient data as opposed to aggregated or anonymised data is justified.
- Patients specifically consent to any research activity which will involve them personally.
- Published findings will not identify patients without their specific consent.

10.10 Clinical Audit

10.10.1 Requests for patient records for audit/research purposes must always be referred to a manager. It is the manager's responsibility to check, confirm and record that the request is bona fide and to obtain permission from the consultant most recently responsible for the patient's care. For requests external to the Organisation copies of records must be sent. Originals must not be removed from Organisation premises.

10.11 Protecting Public Health.

10.11.1 Information may be shared between health professionals on a "need to know" basis without the consent of the patient where this is necessary for the surveillance of communicable disease. Certain diseases are notifiable under the public health legislation. Organisation medical staff must adhere to the provisions of HSG(93) 56.

10.12 Litigation.

10.12.1 Information must be released, by the Appropriate Director, to the Organisation's legal advisors or to a patient's solicitor with the consent of those doctors (including those in support services) involved in the potential litigation. Consent must also be sought from other health care professionals where this is appropriate.

10.12.2 Should these health professionals consider it appropriate consent must also be obtained from others concerned with the patient's care.

10.13 Children and Young People.

10.13.1 Young people aged 16 and above are regarded as adults and must be asked for consent.

10.13.2 Children under 16 who are able to understand can give their consent otherwise the parent or guardian must be asked to consent on the child's behalf.

10.13.3 In child protection cases the interests of the child must be safeguarded. It may be necessary to pass on information without the consent of the parent or guardian. In these cases the information must only be released by the consultant most recently responsible for the child's care or, in his absence, the consultant on call for the specialty.

10.13.4 Parents do not have the automatic right to receive information about their child regardless of age.

Agreement for Participating Organisations

We accept that the protocol set out in this document will provide a secure framework for the sharing of information between partner organisations/agencies in a manner compliant with their statutory and professional responsibilities.

As such we undertake to:

- Implement and adhere to the procedures and structure set out in this protocol.
- Ensure that all policies/procedures established between organisations/agencies for the sharing of information are consistent with this protocol.
- Ensure that where these procedures are adopted then no restriction will be placed on the sharing of information other than those specified in other policies/procedures (detailed at beginning of document).

This document must be agreed to and signed by the following:

Chief Executive

Name:

Signature:

Date:

Caldicott Guardian;

Name:

Signature:

Date: