Information Sharing Protocol

for the secure and confidential sharing of person identifiable information

Produced by Julie Lee-Winsor
Dated: June 2002
Version: 6.a
Document status: DRAFT awaiting SCSC approval
Date effective from: 1 July 2002 (if approved)
Date of review: 1 year from adoption
### Document version control

<table>
<thead>
<tr>
<th>Number</th>
<th>Date issued</th>
<th>Issued to</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1.5</td>
<td>13 March 2001</td>
<td>ISP Sub-group &amp; QA team</td>
<td>First approved version</td>
</tr>
<tr>
<td>V1.6</td>
<td>12 April 2001</td>
<td>ISP Sub-group</td>
<td>7th draft for comment</td>
</tr>
<tr>
<td>V1.7</td>
<td>30 August 2001</td>
<td>Security &amp; Confidentiality Standing Committee</td>
<td>8th draft Updates and changes requested by the Security and Confidentiality Standing Committee at meeting of 17 August 2001</td>
</tr>
<tr>
<td>V2.0</td>
<td>14 September 2001</td>
<td>Security &amp; Confidentiality Standing Committee</td>
<td>Updates and changes requested by the Security and Confidentiality Standing Committee at a meeting on 14 September 2001 and recommended based on principles agreed at that meeting</td>
</tr>
<tr>
<td>V3.0</td>
<td>30 November 2001</td>
<td>Security &amp; Confidentiality Standing Committee</td>
<td>Updates and changes requested by the Security and Confidentiality Standing Committee at a meeting held on 16 November 2001.</td>
</tr>
<tr>
<td>V4.0</td>
<td>18 February 2002</td>
<td>Security &amp; Confidentiality Standing Committee</td>
<td>Updates and changes requested by the Security and Confidentiality Standing Committee at a meeting held on</td>
</tr>
<tr>
<td>Version</td>
<td>Date</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>V5.0</td>
<td>11 April 2002</td>
<td>Updates and changes requested and agreed by the Security and Confidentiality Standing Committee meeting held on 20 March 2002</td>
<td></td>
</tr>
<tr>
<td>V6.0</td>
<td>27 April 2002</td>
<td>Changes requested and agreed by the Security and Confidentiality Standing Committee meeting on 26 April 2002</td>
<td></td>
</tr>
<tr>
<td>V6.a</td>
<td>28 June 2002</td>
<td>Proposed changes to consent section by GPs (approved by SCSC) and minor amendments requested and agreed by the Security and Confidentiality Standing Committee meeting held on 28 June 2002</td>
<td></td>
</tr>
</tbody>
</table>
0. EXECUTIVE SUMMARY

The Electronic Health and Social Care Record Project is proving a concept that an IT system (known to the project as SSHARE\(^1\)) can access and combine information held by the IT systems of participating agencies and then make it available to staff who provide care and/or treatment. This protocol covers all the legal requirements and government guidelines concerning information sharing where this involves sharing personal-identifiable information across primary and secondary healthcare, social services and other health and social care agencies.

0.1 Background

Historically there have been boundaries surrounding the ownership and use of information about individuals that have restricted the ability to share information. Set against this, delivering efficient and effective health and social care for service users requires the different agencies and organisations involved to share information on a need to know basis. Indeed, latest research shows that most service users expect that their information is already shared to a far greater degree than it actually is.

0.2 Scope of the protocol

The Caldicott requirements state that every health and social care organisation must have an agreed, signed procedure in place to cover the sharing of service user identifiable information between themselves and other agencies. This protocol explains the specific requirements needed for approval to use SSHARE, which must be included in each agency’s Caldicott procedure for them to be permitted access to SSHARE.

The protocol relies on the existing and developing legislation and guidance that relate to safe and secure information handling. Each participating organisation will be legally responsible for ownership of the information within their own organisation, and will implement their own internal confidentiality and security procedures which will ensure compliance with this over-arching protocol, as the protocol evolves.

Only those organisations that sign the protocol, and continue to operate procedures that meet the requirements for the secure and confidential handling of person identifiable information are permitted access to the West Surrey Electronic Health and Social Care Record (SSSHARE).

\(^1\) “Social Services and Health Accessing Records Electronically”
0.3 Objectives and principles
Each participating organisation is expected to explain to each service user and/or their representative the proposed uses of their information. Under the Data Protection Act 1998, the Human Rights Act 1998 and the Caldicott requirements the service user is given a leaflet outlining the proposed uses of their information and with whom their information may be shared. Expressed consent is to be sought where this is practically possible. Arrangements must be in place to handle objections to information sharing including reasons for over-riding objections and the practical implications of observing an objection.

0.4 Management of the protocol
The organisations participating in the West Surrey Electronic Health and Social Care Record Project have agreed management arrangements that include the on-going management and maintenance of this protocol to include access, monitoring of actual or anticipated breaches, and dealing with any organisation that fails to comply with the requirements for continued participation.
CONTENTS

0. EXECUTIVE SUMMARY ................................................................. 3
  0.1 Background ............................................................................ 3
  0.2 Scope of the protocol ................................................................. 3
  0.3 Objectives and principles .......................................................... 4
  0.4 Management of the protocol ....................................................... 4
1 Introduction to the Protocol .......................................................... 7
  1.1 Background ............................................................................ 7
  1.2 Scope of the protocol ................................................................. 7
  1.3 Parties (agencies/organisations) to the Protocol ......................... 8
  1.4 What is the West Surrey Electronic Health and Social Care Record 10
  1.5 Legal requirements .................................................................. 11
  1.6 The Data Protection Act 1998 .................................................... 12
  1.7 NHS/LASSL guidelines/requirements ......................................... 14
2 Objectives of the Protocol ............................................................. 15
3 General principles to be applied relating to uses of person identifiable
  information .................................................................................... 16
  3.1 Purposes information can be used for ......................................... 16
  3.2 Consent to use person identifiable information for EHSCR purposes 18
  3.3 Consent to use anonymised information .................................... 18
  3.4 Requirements of user/s of the EHSCR ....................................... 18
  3.5 Consent .................................................................................. 19
  3.6 Where will consent be required .................................................. 19
  3.7 How will consent be recorded .................................................... 20
  3.8 How will consent be kept up to date .......................................... 20
  3.9 What if consent is not available (service user not capable of
    providing) .................................................................................. 20
  3.10 What if consent is not given ..................................................... 21
  3.11 Where consent is not required .................................................. 21
  3.12 Deceased persons .................................................................. 22
4 Management of the protocol .......................................................... 23
5 Defined purposes ........................................................................... 24
6 Access & security .......................................................................... 25
  6.1 Access by users ......................................................................... 25
  6.2 Access by a third party (Supplier) ............................................... 25
  6.3 General Security ....................................................................... 26
  6.4 Audit process ............................................................................ 26
7 Wording included in the agreements for organisations and/or agencies
  using the Electronic Health and Social Care Record ....................... 27
  A The Data Protection Principles, their interpretation and how the Electronic
    Health and Social Care Record complies with them .................... 30
Information Sharing Protocol
for the secure and confidential sharing of person identifiable information

B Legislation to restrict/require, disclosure without consent of the individual ................................................................................................................35
C Other guidance - NHS, Social Services, Professional Bodies.................36
D Definitions........................................................................................................39
E Glossary .........................................................................................................41
F Details of other relevant Acts of Parliament.............................................42
G Guidance for providing information for service users.........................44
H Register of authorised users to the EHSCR.............................................45
I Standing Committee for the EHSCR Security and Confidentiality .......46
J Approval for operational use of the EHSCR.............................................50
1 Introduction to the Protocol

1.1 Background

1.1.1 Agencies/organisations providing health and social care for 'service users' contracted or referred to any organisation covered by this protocol (see definitions) need to work efficiently and effectively to deliver a service to the general public when and where they need it. This is a requirement of Information for Health - Information Strategy for the NHS.

1.1.2 Historically there have been boundaries surrounding ownership and use of information about individuals (service users/staff etc.). This has now been defined within requirements laid down in legislation e.g. the Data Protection Act 1998 ensures data controllers (organisations/agencies) have legal responsibility for person identifiable information within their care - and instils legal requirements concerning the use/s of that information. Hence ownership becomes paramount and information may not be made available to those who need it, when they need it, to provide care to service users. This has restricted the ability to share information.

1.1.3 Different agencies/organisations are collecting and recording identical information about service user’s which is inefficient and a duplication of keying in information. A single point of entry and access to all relevant information would reduce the time wasted on duplication of effort.

1.1.4 Staff (people who are given access by the organisation to the organisation’s information system) from these organisations/agencies have restricted access to systems and information - which could prove detrimental to service user's care and treatment. Again a single point of secure entry and access to all relevant information would increase access to useful information to improve services provided to the service users and all other organisations involved with their care.

1.2 Scope of the protocol

1.2.1 This protocol is an agreement between organisations/agencies detailed in section 1.3. It is designed specifically to establish procedures for the sharing of information between organisations/agencies involved with the care and treatment of 'service users' within the West Surrey Health Community participating in the Electronic Health and Social Care Record.
1.2.2 The NHS and Social Service Caldicott requirements state that where patient information is to be shared between agencies (NHS/Social Services and other) this can only occur where an agreed signed protocol is in place. This protocol is produced to satisfy this requirement.

1.2.3 This is the overarching protocol to cover the sharing of information for all the purposes listed in section 5 and comprises all the legal requirements and government guidelines governing sharing of identifiable information. This protocol also details and cross-refers to other local policies and procedures governing the use and disclosure of person identifiable information.

1.2.4 Organisations/agencies involved with information sharing will sign to agree to the requirements set out in this protocol. All organisations/agencies involved will also abide by their own individual policies and procedures that supplement this protocol and will be fully compliant and consistent with this protocol.

1.2.5 Each organisation will have its own effective procedure to deal with any breaches to this protocol. All incidents will be reported to that organisation through existing incident reporting and management procedures. Any reported incident, with wide consequences on the EHSCR, will be discussed by the Security and Confidentiality Standing Committee of the EHSCR (see section 4.10).

1.3 Parties (agencies/organisations) to the Protocol

The parties to the protocol will be those agencies or organisations that have formally accepted the protocol as laid out in section 7. A register of these parties will be maintained by the Security and Confidentiality Standing Committee on behalf of the Board responsible for the management of the EHSCR.

1st phase
- Woking Area Primary Care Trust
- Surrey County Council (Adult Services)
- North West Surrey Mental Health Partnership Trust

2nd phase
- Ashford & St Peter’s NHS Trust
- General Practitioners
- NHS Direct
- Surrey Ambulance Service NHS Trust
1.3.1 The protocol is the responsibility of the Security and Confidentiality Standing Committee of the EHSCR. The initial project was jointly sponsored by The NHS Information Authority and the West Surrey Health Community via the Information for Health LIS programme.

1.3.2 To ensure the protocol is accurate and up to date it is regularly reviewed by the Standing Committee for Security and Confidentiality. All changes must go through a formal change control process.

1.3.3 Standards required of parties to the Protocol

Each organisation/agency wishing to participate in the project will need to ensure that have mechanisms in place to enable them to address the issues of physical security, security awareness and training, service user access to information, security management, confidentiality management, systems development, site-specific information systems policies and system specific policies (see list below).

The document will need to be read in conjunction with the participating organisation’s own procedures.

To be a user of the EHSCR each organisation will need to provide evidence that they have the following:

<table>
<thead>
<tr>
<th>Required documentation (policies and procedures)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Data Protection registration</td>
</tr>
<tr>
<td>Up to date Information Security Policy</td>
</tr>
<tr>
<td>Up to date System Security Policy for system/s involved with EHSCR.</td>
</tr>
<tr>
<td>A comprehensive training program for staff in the subject of information security and confidentiality</td>
</tr>
<tr>
<td>Current Disciplinary procedures</td>
</tr>
<tr>
<td>Disposal of confidential waste (non-clinical)</td>
</tr>
<tr>
<td>Retention of records policy/procedure to comply with relevant government guidelines</td>
</tr>
</tbody>
</table>
1.4 What is the West Surrey Electronic Health and Social Care Record

1.4.1 The West Surrey Electronic Health and Social Care Record (EHSCR) does not actually hold information within itself. It is a 'virtual' EHSCR created by using a front end to allow access to data items residing on existing systems within each organisation party to the protocol. Access will be provided with strict controls in place concerning the details of service users and healthcare staff and social care staff. Access will normally be available on a 24 hour basis, subject to approval and compliance with this protocol, by health and social care staff and agencies.

1.4.2 The service user details will include data such as: NHS number, name, address, date of birth, sex, registered GP/Contact details, HA /EHSCR identifier.

The following may also be included:

- Biographic details
- Summary of relevant Past History
- On-going medical problems
- Current acute diagnosis
- Assessment summaries
- Assessment needs
- Mental Health Act status
- Care co-ordinator
- Care manager
- Care plan objectives with dates and who is responsible
- Date of next review
- Diary of recent and scheduled care contacts

1.4.3 The EHSCR will provide a facility for a single point of entry to all relevant information sources to enable continuous support and evolution of improving processes of delivering services to service users.
1.4.4 The facility will be a front-end system to ‘push’ and ‘pull’ information from the systems already in existence in partner organisations. All security and access controls will be within the individual systems. The aim is to have a single log-in via the front end which can handle the controls in the underlying system/s.

1.5 Legal requirements

1.5.1 There are legal requirements which must be considered and complied with to ensure individual’s rights are respected and the organisations involved do not breach these legal requirements.

1.5.2 The main pieces of legislation governing individuals rights which must be considered are:

- Human Rights Act 1998
- Freedom of Information Act 2000
- Data Protection Act 1998
- Crime & Disorder Act 1998
- Computer Misuse Act 1990
- Copyright Designs and Patents Act 1988
- Children’s Act 1989
- NHS & Community Care Act 1990
- Mental Health Act 1983
- Carers (Recognition & Service) Act 1995
- Access to Health Records Act 1990 (only for manual records of deceased patients)
- The Adoption Act 1976
- The Health Act 1999 (section 31)
- The Health and Social Care Act 2001

Further information and details of the most relevant of these Acts are in appendix F.
1.5.3 The following Acts relate to security and confidentiality of information:

<table>
<thead>
<tr>
<th>Act of Parliament</th>
<th>Relates to</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Freedom of Information Act 2000</td>
<td>Individuals right of access to information</td>
</tr>
<tr>
<td>The Human Rights Act 1998</td>
<td>Individuals right to privacy for themselves and their family members</td>
</tr>
<tr>
<td>The Data Protection Act 1998</td>
<td>Individuals rights to confidentiality and security for their information and their right to access their own records</td>
</tr>
<tr>
<td>The Computer Misuse Act 1990</td>
<td>Makes it an offence for any user to gain unauthorised access to information on a computer</td>
</tr>
<tr>
<td>The Regulation of Investigatory Powers Act 2000</td>
<td>Allows organisations to monitor automated communications e.g. e-mail</td>
</tr>
</tbody>
</table>

1.5.4 There are other Acts which either: a) make it an offence to disclose information or b) make it a legal requirement to disclose information. These are detailed in Appendix B.

1.6 **The Data Protection Act 1998**

1.6.1 This Act is the key legislation covering all aspects of information processing including security & confidentiality of person identifiable information. This Act relates to manual and automated records of living identifiable individuals from collection of information, use/s and through to disposal. Therefore this Act is detailed to highlight how the protocol and operation of the EHSCR comply with these legal requirements. Other relevant legislation and NHS/LASS guidelines are detailed in appendix C.

1.6.2 The Act is implemented by abiding by 8 principles of good practice known as the 'eight data protection principles’. The principles and their interpretation are outlined below:
1. Personal data shall be processed fairly and lawfully

**Interpretation:**
Individuals have a right to have their information processed within the law and to be made aware of why their information is needed, how it is to be used and to whom it may be disclosed. Information can only be processed if certain conditions are met and individuals have a right to object to their information being used for other purposes. This is a complex issue that is detailed in section 3.

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

**Interpretation:**
Interacts with above and also requires that information processed by automated means (e.g. computer) must be registered with the Information Commissioner.

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

**Interpretation:**
Information collected and held must be for a justified purpose on a need to know basis.

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

**Interpretation:**
Ensure personal information about service users and staff is recorded accurately and kept up to date.

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

**Interpretation:**
Ensure procedures are in place which detail how long information about service users and staff is kept within the front end facility and within the organisations own systems. This will be for as long as deemed useful or defined by government guidelines.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act

**Interpretation:**
*Individuals have rights e.g. to have a copy of information held about themselves, to object to information being processed, to know why information is requested - further details in Appendix A.*

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

**Interpretation:**
*Each organisation must comply with standards and procedures for information security e.g. BS7799. See section 6 and Appendix A.*

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

**Interpretation:**
*If information is processed outside of the EEA certain conditions apply prior to information being exchanges/sent (see www.dataprotection.gov.uk for further information)*

### 1.7 NHS/LASSL guidelines/requirements

1.7.1 There are guidelines issued by government departments which also have to be considered. Some of the guidelines are further information concerning the implementation of legal requirements and some actually state that the NHS/Local Authority Social Services (LASSL) need to do more than the legal requirements. The most relevant guidance is that relating to implementation of the Caldicott requirements. Other relevant circulars are detailed at appendix C.
1.7.2 The NHS Executive has issued Caldicott Guardian Guidelines:

- HSC1999/012 to all Trusts and Health Authorities in January 1999.
- HSC2002/3/LASSL2002/2 Caldicott Guardians & Implementing the Caldicott Standard into Social Care
- GP/PCG guidelines were issued in March 2000 (available on the NHS Caldicott web site under Management Audits & Improvement Plans section called ‘Guidance for Primary Care Groups).

1.7.3 The aim of the Caldicott requirements are to improve the security and confidentiality of service user (patient) information. Most are also requirements of the data protection legislation but some require further action. Service users (patients/clients) with special needs e.g. sight impairment, or those whose first language is not English must also be made aware of their information uses and be given the same rights (e.g. to refuse information to be used for ‘extra’ purposes) the same as all other individuals. See appendix C for further information.

2 Objectives of the Protocol

2.1 The purpose of this document is to provide an overarching framework which will allow the safe and confidential sharing of service user, carers and staff information between agencies/organisations to enable the provision of the most effective and efficient care and support for the needs of service user/s. This framework will be in accordance with and take account of legal and other government agency requirements surrounding the security and confidentiality of person identifiable information.

2.2 Service users of the organisations party to this protocol must be informed of the reasons their information is collected, recorded, used and shared to comply with legal requirements surrounding individual’s rights to privacy and confidentiality of their information. How this will be implemented, managed, monitored and reviewed will also need to be detailed by individual organisations in their procedures to implement the Caldicott requirements.
3 General principles to be applied relating to uses of person identifiable information

3.1 Purposes information can be used for

3.1.1 Personal information about service users and their family/relatives can only be used for specific purposes and shared for specified justified reasons. All other uses of this information can only occur if consent has been gained.

3.1.2 For most cases this means that information can be collected from service users and their relatives if it is to be used for the conditions specified within the data protection principle 1.

Service user conditions

Schedule 2(6)1 of the Data Protection Act 1998 states: ‘The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject’.

Interpretation:
The processing is necessary for the normal purposes of the organisation. Health and social care organisations (and agencies) will require information to allow them to provide care and treatment to that individual and their family members. Health and social care information about individuals cannot be used for any other purposes e.g. law enforcement

And for sensitive information
Schedules 3(8)1 and (8)2 of the Data Protection Act 1998 state: ‘The processing is necessary for medical purposes and is undertaken by a) a health professional, or b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

In this paragraph ‘medical purposes’ includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services’.
Interpretation:
In addition information held and used for the provision of health and social care must be for the primary purpose of care and be recorded by the relevant professional or their support staff. All persons coming into contact with service user information must be bound to their organisation by a confidentiality agreement (normally their contract of employment)

Staff information

Schedule 2(2)
The processing is necessary ‘for the performance of a contract to which the data subject is party, or, for the taking of steps at the request of the data subject with a view to entering into a contract’

Interpretation:
Staff/employee information can be processed if there is a contract between the organisation and their employee to enable this to occur

3.1.3 If the above conditions are met, the organisation processing the information can usually do so for those specific purposes. It will not permit sharing with other organisations e.g. social services unless there is an overriding legal requirement to do so or informed consent has been obtained. This issue is dealt with in other points within this section (see section 3.6).

3.1.4 What is consent?

Taken from the Department of Health publication ‘Building the Information Core – Protecting and Using Confidential Patient Information’ – A Strategy for the NHS (published by the Information Policy Unit December 2001).

<table>
<thead>
<tr>
<th>Consent</th>
<th>Agreement, by someone with the capacity to make a valid decision, either express or implied, to an action based on knowledge of what the action involves, its likely consequences and the option of saying no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Express consent</td>
<td>Consent which is expressed orally or in writing (except where service users (patients) cannot write or speak, when other forms of communication may be sufficient) (GMC)</td>
</tr>
</tbody>
</table>

Consent Agreement, by someone with the capacity to make a valid decision, either express or implied, to an action based on knowledge of what the action involves, its likely consequences and the option of saying no

Express consent Consent which is expressed orally or in writing (except where service users (patients) cannot write or speak, when other forms of communication may be sufficient) (GMC)
Implied consent

Consent which is inferred from a person’s conduct in the light of facts and matters which they are aware of, or ought reasonably to be aware of, including the option of saying no

When the term informed consent is used within the Protocol this is the same as the definition of express consent given above.

3.2 Consent to use person identifiable information for EHSCR purposes

3.2.1 Consent to share information between other organisations will be required from all of those persons whose information will form part of the EHSCR. This will apply to service users, their family/relatives and in some cases employees.

3.2.2 Consent is a complex issue (see section 3.6 for detailed requirements)

3.2.3 The information will be used/processed for the purpose of providing care and treatment to the service user and/or their family/relatives. The organisations using the information will be those defined within section 1.3 which have agreed and signed up to this agreement (see section 7). Other users requiring access to, or those who wish to use the information, will be assessed on a need basis by the Security and Confidentiality Standing Committee.

3.3 Consent to use anonymised information

3.3.1 Some information will be used in an anonymised format and therefore consent may not be applicable.

3.4 Requirements of user/s of the EHSCR

3.4.1 All staff using service user and other organisations employee information are bound by a duty of confidence through their contract of employment and, for a health and social care professional also in the terms of their professional body membership.

3.4.2 Any user of the information who is found to have breached a service user or employee’s confidence by unauthorised use/disclosure of their information will face disciplinary action by their employer.
3.5 Consent

3.5.1 Each participating organisation will have their own policy for Information Confidentiality and Security. This policy will detail the way person identifiable information (service user and staff) is managed and used within their own organisation. It will also include how information will be passed to other organisations and agencies where a need to exchange and share information is identified.

3.5.2 Consent of an individual will be required unless it is deemed by a care professional to be detrimental to the safety of the service user or others. There may be circumstances where consent cannot be sought or should not be sought and these will be detailed within the policies. An outline of the requirements is listed in this protocol and further information can be found within the policies of partner organisations.

3.6 Where will consent be required

3.6.1 Service users will be provided with sufficient information to ensure they are aware of all the uses and potential uses/disclosures of their personal information.

3.6.2 Information leaflets and posters will also be distributed throughout the organisations for service users and their representatives/carers to read. The leaflet will include contact details to seek clarification or additional information.

3.6.3 In addition each service user, or their legal representative, will be provided with an information leaflet at first point of contact e.g. at the start of an episode of care or at the time of registration with a General Practitioner, outlining the uses of their information.

3.6.4 Staff will be trained to ensure they give the service user all the information they require to understand what will happen to their information. Service users may also be given the opportunity to opt out of ‘extra’ uses of their information but will also be made aware that they may not opt out of all uses as it may impact on their care and treatment. This will at the discretion of the care professional and defined by policies of the individual organisations.

3.6.5 In the absence of a referral from a health or social care professional participating in the EHSCR, staff will gain consent from the service user and/or their representative to access their record/s in the EHSCR. This will typically apply to unplanned (emergency) care and self-referral except as in 3.5.2.
3.6.6 In certain circumstances organisational procedures may allow the relevant health or social care professional to disregard a refusal to give consent. This override will only ever be used if considered in the ‘best interest’ of the service user and would need to be justified by the professional/s concerned.

3.7 How will consent be recorded

3.7.1 Each organisation should have a procedure for recording informed consent. The procedure must include the need to record the provision of an information leaflet, how and when it was provided to the service user and/or their representative, if agreement was or was not provided, and evidence of any exceptions.

3.7.2 As a minimum each organisation must have a process for recording that an information leaflet has been provided to the service user and/or their representative, to include date and how provided, e.g. by hand, through the post. This would be required at the start of an episode of care/treatment and/or at first point of contact such as GP registration.

3.8 How will consent be kept up to date

3.8.1 It is the organisations responsibility to keep personal information accurate and up to date. This applies to staff and service user information, in computer records, manual files and all other media. Consent for use/s of service user information should be addressed with the service user at an applicable time e.g. each new episode of care, when circumstances change, or if the service user changes his or her mind.

3.8.2 This will be achieved by asking for the assistance of the service user. Details will be in the ‘service user’ information leaflet.

3.9 What if consent is not available (service user not capable of providing)

3.9.1 If it is not possible to gain consent from the service user or their relatives/carer a judgement must be made by the appropriate healthcare and/or social care professional regarding the use/s of their information. This should be noted in the service user’s record (manual file and/or computer record).
3.10 What if consent is not given

3.10.1 In very rare circumstances an individual or their representative may refuse to give consent for some/all use/s of their information. It should be explained to them the potential problems they may encounter with their, or their relatives, care and/or treatment if they do not allow their information to be shared.

3.10.2 The requirement to deal with times when the service user and/or their relative refuses to give consent to share their information should be addressed in the organisation’s local procedures. The service user’s wishes should be respected and handled in line with the local procedures. There must be a facility for the care professional to elect not to record on the electronic system/s.

3.10.3 The local procedure should identify the following:

- What instructions have been given to staff to deal with times when consent is not given
- What levels of counselling are available
- What circumstances the decision not to share can be over ruled
- What right of appeal does the service user and/or their relative have
- How the process will be implemented

3.10.4 If consent still cannot be obtained the service user information must not be shared and this must be recorded unless 3.6.6 applies.

3.11 Where consent is not required

3.11.1 The legislation below requires the disclosure of personal identifiable information. This means that an individual’s consent is not required as there is an overriding legal requirement to make the disclosure.

3.11.2 However, it must be noted that not all of the service user record would need to be disclosed as only certain data items are covered by the legislation.

- Public Health (Control of Diseases) Act 1984 & Public Health (Infectious Diseases) Regulations 1985
- Education Act 1944 (for immunisations and vaccinations to NHS Trusts from schools)
- Births and Deaths Act 1984
- Police and Criminal Evidence Act 1984
3.11.3 Other disclosures which can occur without informed consent

- With a Court Order
- For the prevention and detection of crime

3.12 Deceased persons

Although the Data Protection Act 1998 does not apply to records of deceased persons the Common Law of Confidentiality does apply. If a service user has requested that their information is not disclosed after their death this must be respected unless an exception occurs.
4 Management of the protocol

4.1 The document is owned by each organisation signed up to the Electronic Health & Social Care Record.

4.2 The responsibility for keeping the document up to date to take account of changes to legislation, guidance issued by the government and professional bodies and as the result of relevant case law will lie with the community wide group the Standing Committee for the EHSCR Security and Confidentiality (see Appendix I for Terms of Reference).

4.3 This document will be reviewed at least annually and changes will be recorded on the version control sheet (at the front of the document).

4.4 Each organisation will need to ensure they have a current up to date version of this document. It will be the responsibility of each organisation’s Caldicott Guardian/Group to monitor that this is occurring.

4.5 There will be a need to monitor compliance with the requirements of this document. This could occur in a variety of ways but an internal audit and/or external audit of the documents requirements and how they are being complied with will probably be undertaken by auditors of one or more of the organisations involved.

4.6 A register must be produced and maintained of the people to whom access to the EHSCR has been granted. This register will include details of the person who will be using the EHSCR, the purpose for which they need access, details of the information they need to access, and for how long access has been granted. The minimum data set for the register is set out at Appendix H.

4.7 The document will need to be agreed to and signed by authorised person/s within each organisation and someone on behalf of the EHSCR. It is must be the Chief Executive or equivalent for each organisation and the Caldicott Guardian (if relevant).

4.8 A section outlining information flows will be inserted into this section when agreed as the EHSCR progresses.

4.9 Service Level Agreements (SLAs) will exist between the organisations using the EHSCR and the organisation responsible to ‘run’ the system.
The ‘front end’ facility will be procured by West Surrey Health Authority on behalf of the Health and Social Care Community. The contract for supply was signed by West Surrey Health Authority. On re-organisation the contract was re-assigned to Woking Area Primary Care Trust. Therefore for the initial ‘pilot stage’ of the EHSCR they will also ‘own’ the facility. This will need to be reviewed once the pilot stage has been signed off and the EHSCR goes ‘live’.

4.10 If a breach of the protocol occurs each organisation must log the incident and investigate.

Each organisation will also inform such regulatory bodies as need to know of any breaches (e.g. NHS Information Authority)

The Standing Committee for the EHSCR Security & Confidentiality will undertake any relevant reporting.

All breaches actual and/or potential should be reported to the next planned meeting of the EHSCR Security and Confidentiality Standing Committee. It is the responsibility of the Caldicott Guardian to ensure reporting occurs. This could be verbal or a written report.

The group will expect to be provided with the following details:

- Particulars of the incident
- Action taken
- When the incident has been closed

Incident reporting will be a standing item on the agenda of all meetings of the group.

5 Defined purposes

5.1 Below is a list of some of the primary purposes for use of the EHSCR

- delivering and managing personal care & treatment
- assuring & improving the quality of care & treatment
- risk management
- investigating complaints & notified or potential legal claims
- supporting multi-agency working to provide integrated services

Details will be defined in ‘view’ and ‘update’ screens containing specific data items contained within specification PSS05 (version 1.0) and any
subsequent updates. This will be signed off by the appropriate Caldicott Guardian (see appendix J).

6 Access & security

6.1 Access by users

(Section 9 of BS7799 has more detail of requirements for each organisation to address in their respective Security Policies). A summary of the main points are listed below. Please note the term ‘user’ may mean an employee or agent of the organisation to include software suppliers.

- All users of the EHSCR will be allocated user access rights on a strict need to know basis.

- This will be achieved by the use of ‘user profiles’ that allow access to information needed by the care professional accessing the information e.g. a profile for GPs, care of the elderly care staff. Details will be defined within specification PSS06 ‘Roles of Users’ version 1.0 and any subsequent updates which will need to be agreed and ‘signed off’ by the relevant Caldicott Guardians (see appendix J).

- All users will have an individual user id and password. They must maintain the secrecy of the password themselves and they will be trained in system security. All users will comply with the security procedures of their own employing organisation.

- Access rights should be agreed by the organisations own Caldicott Guardian as agreeing access is one of the Caldicott recommendations.

- User rights should be documented within each organisation and kept up to date. This should log who has access, which profile they have been allocated, when their access began and, if necessary, when their access will cease.

6.2 Access by a third party (Supplier)

The supplier will be granted rights to allow them to fix bugs, update the software etc. by their NHS Code of Connection and NHSnet facility.
There will also be a back-up facility available to use to cover any problem with NHSnet connection. The back-up access facility will be via a secure modem link.

The supplier must maintain the confidentiality of any information they see whilst performing their responsibilities under the terms of the contract.

6.3 General Security

(Section 10 of BS7799 has more detail that should be included in each organisations relevant security policies)

The EHSCR will be kept secure to those who need to have access to it by abiding by the rules listed above (6.1 Access rights).

6.4 Audit process

The EHSCR will comply with the audit requirements detailed in HSC1998/153 Appendix A ‘The Legality of Electronic Records in Hospitals’.

All access to the EHSCR by all types of user will be auditable. The audit trail will hold who has accessed what and when. The audit trail will be in the EHSCR software. There should also be full audit trails within the individual systems.
7 Wording included in the agreements for organisations and/or agencies using the Electronic Health and Social Care Record.

We accept that the procedures laid down in this document will provide a secure framework for the sharing of information between partner organisations/agencies participating in the EHSCR, 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:
## Required documentation (policies and procedures) and actions

<table>
<thead>
<tr>
<th>Required documentation (policies and procedures) and actions</th>
<th>In place</th>
<th>Dated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Data Protection registration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Up to date Information Security Policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Up to date System Security Policy for system/s involved with EHSCR.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A comprehensive training program for staff in the subject of information security and confidentiality</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Current Disciplinary Procedures</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disposal of confidential waste (non-clinical)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Retention of records policy/procedure to comply with relevant government guidelines</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Procedure for recording informed consent</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Current NHSnet Code of Connection</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
APPENDICES
A The Data Protection Principles, their interpretation and how the Electronic Health and Social Care Record complies with them

A.1 The first principle of the Act is the most important when considering information sharing. The principle states that ‘fair processing’ of information must occur.

Personal data is defined as ‘data which relate to a living individual who can be identified:-
- from those data; or
- from those data and other information which is in the possession of, or likely to come into the possession of, the data controller
- and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual’.

Processing is defined as ‘obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:-
- organisation, adaptation or alteration of the information or data
- retrieval, consultation or use of the information or data
- disclosure of the information or data by transmission, dissemination or otherwise making available, or
- alignment, combination, blocking, erasure or destruction of the information or data

All information must be processed by at least one condition set out in Schedule 2 of the DPA. For service user information the condition which applies is schedule 2(6)1 ‘The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing in unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject’. This has been agreed by the Information Commissioner and the Department of Health.

In addition for sensitive information as defined within the data protection legislation at least one condition in Schedule 3 of the DPA must also apply.

Sensitive personal data is defined as:
- the racial or ethnic origin of the data subject
- their political opinions
their religious beliefs or other beliefs of a similar nature
whether they are a member of a trade union
their physical or mental health or condition
their sexual life
the commission or alleged commission by them of an offence, or
any proceedings for any offence committed or alleged to have been
committed by them, the disposal of such proceedings or the
sentence of any court in such proceedings.

For service user information schedule 3(8)1 and (8)2 apply ‘The
processing is necessary for medical purposes and is undertaken by a)
a health professional, or b) a person who in the circumstances owes a
duty of confidentiality which is equivalent to that which would arise if
that person were a health professional. In this paragraph ‘medical
purposes’ includes the purposes of preventative medicine, medical
diagnosis, medical research, the provision of care and treatment and
the management of healthcare services’.

The key components of ‘fair processing’ are as follows:
how was the data obtained
was the data subject provided with the following information:
the identity of the data controller
the purpose for which the data are to be processed
any further information - e.g. who will have access to the data
and for what purpose/s
was the data subject aware of all the purpose/s their information are
to be processed, the likely consequences of such processing and
whether particular disclosures can be reasonably envisaged

Required action:
Each organisation must ensure they have adequate tested
procedures to ensure consent for use of information is obtained.
(Refer to section 3 on consent and appendix A Acts of
Parliament).

A.2 The second principle concerns the notification of information held on
electronic equipment that can be processed (refer to definition) by
automatic means. The organisation (data controller) who hold the
information is legally bound to notify the Information Commissioner’s
Office (previously Data Protection Commissioner’s Office) of the
purpose for holding the information, details of the type of information
held and to whom (organisation/agency) the information may be
disclosed.
It should be noted that although it is no longer a legal requirement to notify the Information Commissioner of information sources an individual has a right to know from whom an organisation receives information about them.

**Required action:**
Each organisation must ensure the data protection registrations are current and updated to take account of information use/s. The organisation commits a criminal offence if it is not kept up to date and accurate.

A.3 The **third** principle states that information must be adequate, relevant and not excessive. This requires that information collected must be for a justified purpose and this may need to occur on a data item by data item case. Each organisation/agency must be able to justify why they need each data item they request access to (see section 5 purposes).

**Required action:**
Each organisation must be satisfied that they can justify each data item held as part of a service user record (for service user/family and staff). This will be vital if challenged by the service user/staff or as a complaint investigated by the Information Commissioner.

A.4 The **fourth** principle requires that the information must be kept accurate and up to date.

The EHSCR will not hold any data it will only display or receive and route data.

In some cases data will be routed to more than one system ensuring consistency.

Where the same data items contain different information, all versions will be displayed to the system user with additional information such as who recorded when so that they can take an informed view.

It is anticipated that in some cases messages or reports will be generated to draw attention to inconsistencies between the systems feeding the EHSCR.

Data accuracy within the EHSCR is assured through retaining responsibility within the individual organisations where the feeder
systems reside. These systems typically use validation processes within the underlying system at the time of data capture.

Service users to be reminded of their responsibility to provide accurate information and provide information about changes

**Action:**
Each organisation to have tested procedures for recording information accurately and keeping information up to date (service user and staff)

**A.5 The fifth principle** requires that the information must only be kept for as long as is necessary. This will apply to the underlying systems and the ‘virtual’ EHSCR.

The data requirements will be driven by local processes of care delivery across the whole care system. No service user information is kept in the EHSCR for longer than while it is being viewed.

Each individual organisation will take responsibility to meet its legal and policy requirements to archive information but ensure it is available to those who need it when it is needed.

The NHS must abide by the legal requirements under the Public Records Act 1958 which are defined within HSC1999/053 For the Record. This applies to all records regardless of the media they may be held/retained.

Social Services have similar requirements detailed within the Social Services guidelines ‘Retention of Client Records’ procedure P3.

**Each organisation to ensure information kept for as long as required and if needs to be kept for longer the need MUST be justified.**

**A.6 The sixth principle** gives rights to individual’s whose information is held by an organisation in respect of their own person information. These are:

- right of subject access
- right to prevent processing likely to cause harm or distress
- right to prevent processing for the purposes of direct marketing
- right in relation to automated decision taking
- right to take action for compensation if the individual suffers damage
right to take action to rectify, block, erase or destroy inaccurate data
right to make a request to the Information Commissioner for an assessment to be made as to whether any provision of the Act has been contravened

Each organisation must ensure they have up to date procedures to deal with service user and staff requests for access to information held about them and for dealing with complaints for breach of above.

A.7 The **seventh** principle governs security & confidentiality of information. Compliance with BS7799 IT Industry Standards for Information Security apply (see section 6 ‘access and security’)

A.8 The **eighth** principle puts constraints and controls on any electronic person identifiable information which may be or planned to be disclosed to a country outside of the EEA (where the DPA requirements may not be enforced).

If personal information is required to be disclosed in electronic format to countries outside of the EEA advice MUST be sought from the Office of the Information Commissioner.
B Legislation to restrict/require, disclosure without consent of the individual

B.1 Legislation to restrict disclosure of personal identifiable information

Human Fertilisation and Embryology (Disclosure of Information) Act 1992
Venereal Diseases Act 1917 and Venereal Diseases Regulations of 1974 and 1992
Abortion Act 1967
The Adoption Act 1976

B.2 Legislation requiring disclosure of personal identifiable information

Public Health (Control of Diseases) Act 1984 & Public Health (Infectious Diseases) Regulations 1985
Education Act 1944 (for immunisations and vaccinations to NHS Trusts from schools)
Births and Deaths Act 1984
Police and Criminal Evidence Act 1984
C Other guidance - NHS, Social Services, Professional Bodies

C.1 HSC1999/012 Caldicott recommendations
HSC2002/003 Implementing the Caldicott Standard into Social Care
LAC(2002)2 As above

1. Information must be provided to service users (patients), clients and service users (patients) relatives concerning the proposed use/s of information about them.
2. The organisation must have a staff code of conduct in respect of confidentiality.
3. Staff induction programme must include security and confidentiality of information.
4. Confidentiality and security training needs of staff should be assessed.
5. Training must be provided which includes confidentiality and security standards of the organisation and employees individual responsibilities.
6. Contracts of employment should have an up-to-date confidentiality clause.
7. Contracts, agreements and SLAs with other organisations should contain a confidentiality clause.
8. Review information flows containing service users (patients) identifiable information.
9. Internal information/data ownership established.
10. Safe Haven procedures should be in place to safeguard information flowing to and from the organisation.
11. Protocols governing the sharing of service users (patients)-identifiable information with other organisations locally agreed.
13. Security responsibilities Does the organisation have an Information Security officer role in place who has this person been trained?
14. Risk Assessment and Management Programme should be in place and include information (IT and manual records).
15. Security Incidents should be logged, investigated and monitored.
16. Security Monitoring reported to the Board or management team.
17. Users need to be made aware of their responsibilities.
18. Controlling access to confidential service users (patients) information - Is access agreed by Caldicott Guardian?
## C.2 Health and Social Services Circulars

<table>
<thead>
<tr>
<th>Circular</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HSC1998/203</td>
<td>Health records requests for access by patients and their representatives</td>
</tr>
<tr>
<td>HSG(96)18</td>
<td>The protection and use of patient information</td>
</tr>
<tr>
<td>LASSL(99)16</td>
<td>Data Protection Act 1998 draft guidance</td>
</tr>
<tr>
<td>LASSL(98)16</td>
<td>Data Protection Act 1998</td>
</tr>
<tr>
<td>LASSL(96)5</td>
<td>The protection and use of patient information</td>
</tr>
<tr>
<td>MISC(97)52</td>
<td>Faxing of safe haven amendments go live</td>
</tr>
<tr>
<td>HSC1999/053</td>
<td>For the Record (Preservation, retention &amp; destruction of records under the Public Records Act 1958) and records management strategy</td>
</tr>
<tr>
<td>HSC1998/217</td>
<td>Preservation, retention and destruction of GP general medical services records relating to patients</td>
</tr>
<tr>
<td>HSG(91)6</td>
<td>Access to Health Records Act - A guide for the NHS</td>
</tr>
<tr>
<td>IMGE 5498</td>
<td>A guide to implementing an awareness programme (The Information Security Resource pack)</td>
</tr>
<tr>
<td>HSG(96)15</td>
<td>The NHS IM&amp;T Security Manual</td>
</tr>
<tr>
<td>HSG(96)18</td>
<td>The Protection &amp; Use of Patient Information</td>
</tr>
<tr>
<td>HSC2002/3 LASSL2002/2</td>
<td>Implementing the Caldicott Standard into Social Care</td>
</tr>
</tbody>
</table>

## C.3 Useful reference material

<table>
<thead>
<tr>
<th>Reference</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>HSC1998/203</td>
<td>Health records requests for access by patients and their representatives</td>
</tr>
<tr>
<td>HSG(96)18</td>
<td>The protection and use of patient information</td>
</tr>
<tr>
<td>LASSL(99)16</td>
<td>Data Protection Act 1998 draft guidance</td>
</tr>
<tr>
<td>LASSL(98)16</td>
<td>Data Protection Act 1998</td>
</tr>
<tr>
<td>LASSL(96)5</td>
<td>The protection and use of patient information</td>
</tr>
<tr>
<td>MISC(97)52</td>
<td>Faxing of safe haven amendments go live</td>
</tr>
<tr>
<td>HSC1999/053</td>
<td>For the Record (Preservation, retention &amp; destruction of records under the Public Records Act 1958) and records management strategy</td>
</tr>
<tr>
<td>HSC1998/217</td>
<td>Preservation, retention and destruction of GP general medical services records relating to patients</td>
</tr>
<tr>
<td>HSG(91)6</td>
<td>Access to Health Records Act - A guide for the NHS</td>
</tr>
<tr>
<td>IMGE 5498</td>
<td>A guide to implementing an awareness programme (The Information Security Resource pack)</td>
</tr>
<tr>
<td>HSG(96)15</td>
<td>The NHS IM&amp;T Security Manual</td>
</tr>
<tr>
<td>HSG(96)18</td>
<td>The Protection &amp; Use of Patient Information</td>
</tr>
<tr>
<td>HSC2002/3 LASSL2002/2</td>
<td>Implementing the Caldicott Standard into Social Care</td>
</tr>
</tbody>
</table>
Free publications from: General Medical Council, 178 Great Portland Street, London W1N 6JE. Tel:020 7580 7642

Duties of a doctor - guidance from the General Medical Council.
- Confidentiality: Protecting and Providing Information
- Seeking patients’ consent: the ethical considerations
- Good medical practice
- Serious communicable diseases
- Advertising
- HIV & AIDS the ethical considerations
Further information www.gmc-uk.org

PIU project on privacy and datasharing

A project to establish a government-wide framework (or frameworks) for the future of data sharing to take account of privacy requirements of the Data Protection Act 1998 and the Human Rights Act 1998. Project includes: survey of data-sharing within Government; Public attitudes; Legal framework; Technological change and trends and International experience. Key players include both NHS and Social Services. Project due for completion during 2001.
Further information: www.cabinet-office.gov.uk/innovation

BMA Confidentiality and disclosure of health information - 14 October 1999
Consent toolkit
Further information: www.bma.org.uk

Information Commissioner (previously Data Protection Commissioner)
Further information: www.dataprotection.gov.uk
## Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anonymised information/data</td>
<td>Data from which the service users (patients) (employee) cannot be identified by the recipient of the information. The name, address and full postcode must be removed together with any other information (e.g. NHS number) which, in conjunction with other data held by or disclosed to the recipient, could identify the service users (patients) (employee). (GMC)</td>
</tr>
<tr>
<td>BS7799</td>
<td>British Standard for Information Management and Security</td>
</tr>
<tr>
<td>Carer</td>
<td>A recognised person (carer/relative) who provides substantial and regular care for the service user.</td>
</tr>
<tr>
<td>Caldicott</td>
<td>Initially an NHS initiative to improve the security and confidentiality of patient identifiable information. This has now been adopted by Social Services as well</td>
</tr>
<tr>
<td>Consent</td>
<td>Agreement to an action based on knowledge of what the action involves and its likely consequences (GMC)</td>
</tr>
<tr>
<td>Consent (Express consent)</td>
<td>Consent which is expressed orally or in writing (except where service users (patients)s cannot write or speak, when other forms of communication may be sufficient) (GMC)</td>
</tr>
<tr>
<td>EHSCR</td>
<td>Multi-agency Electronic Health Record and Electronic Social Care Record</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Health &amp; Social Care Professional</td>
<td>A doctor, nurse and other care staff who are bound by a professional body e.g. GMC, UKCC</td>
</tr>
<tr>
<td>Person identifiable information</td>
<td>Any information which can identify an individual by name and/or number e.g. date of birth and full postcode or if the recipient has access to the look up tables - the NHS number will make the information identifiable</td>
</tr>
<tr>
<td>Personal information</td>
<td>Information about people which doctors learn in a professional capacity and from which individuals can be identified (GMC)</td>
</tr>
<tr>
<td>Service User</td>
<td>An individual who has contacted, or has been referred to, an organisation that is covered by this protocol.</td>
</tr>
<tr>
<td>Staff/Employee/Agent (including supplier)</td>
<td>People who are given access by the organisation to the organisation’s information system. This will include health professionals and administrative and clerical workers who support the role of the health professional providing care and treatment to the service user and their relatives/carers</td>
</tr>
</tbody>
</table>
### Glossary

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EEA</td>
<td>European Economic Authority (EU countries + other who have adequate protection to use personal information)</td>
</tr>
<tr>
<td>GMC</td>
<td>General Medical Council</td>
</tr>
<tr>
<td>GP</td>
<td>General Practitioner</td>
</tr>
<tr>
<td>HA</td>
<td>Health Authority</td>
</tr>
<tr>
<td>ISP</td>
<td>Information Sharing Protocol</td>
</tr>
<tr>
<td>LASSL</td>
<td>Local Authority Social Services Letter</td>
</tr>
<tr>
<td>NHS</td>
<td>National Health Service</td>
</tr>
<tr>
<td>PCG</td>
<td>Primary Care Group</td>
</tr>
<tr>
<td>PCT</td>
<td>Primary Care Trust</td>
</tr>
<tr>
<td>SLA</td>
<td>Service Level Agreement</td>
</tr>
<tr>
<td>SS</td>
<td>Social Services</td>
</tr>
<tr>
<td>SSP</td>
<td>System Security Policy</td>
</tr>
<tr>
<td>Trust</td>
<td>NHS Hospital, Community, Ambulance or Primary Care Trust</td>
</tr>
<tr>
<td>WSHA</td>
<td>West Surrey Health Authority</td>
</tr>
</tbody>
</table>
Details of other relevant Acts of Parliament

Human Rights Act 2000

This Act became law on 2 October 2000. It binds public authorities including Health Authorities, Trusts, Primary Care Groups and individual doctors treating NHS patients to respect and protect an individual’s human rights. This will include an individual’s right to privacy (under Article 8) and a service user’s right to expect confidentiality of their information at all times.

Article 8 of the Act provides that ‘everyone has the right to respect for his private and family life, his home and his correspondence’. However, this article also states ‘there shall be no interference by a public authority with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention or disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others’.

Each organisation must act in a way consistent with these requirements. It must take an individual’s rights into account when sharing personal information about them.

Freedom of Information Act 2000

This Act came into force in November 2000 and will be fully in force during the coming years. The Information Commissioner (previously the Data Protection Commissioner) will oversee the implementation of this Act. This Act gives individuals rights of access to information held by public authorities. Further information will be available as implementation progresses.


This Act combines rules relating to access to protected electronic information as well as revising the ‘Interception of Communications Act 1985’. The Act aims to modernise the legal regulation of interception of communications in the light of the Human Rights laws and rapidly changing technology.

Crime and Disorder Act 1998
This Act introduces measures to reduce crime and disorder, including the introduction of local crime partnerships around local authority boundaries to formulate and implement strategies for reducing crime and disorder in that local area.

The Act allows disclosure of person identifiable information to the Police, Local Authorities, Probation Service or the Health Service but only if the purposes are defined within the Crime and Disorder Act. The Act does not impose a legal requirement to disclose/exchange person identifiable information and responsibility for disclosure rests with the organisation holding the information. There should be a Crime and Disorder Protocol governing the disclosure/exchange and use of personal information within a local authority boundary agreed and signed by all involved agencies and organisations.

TheComputer Misuse Act 1990

This Act makes it a criminal offence to access any part of a computer system, programs and/or data that a user is not entitled to access. Each organisation will issue each EHSCR user an individual user id and password which will only be known by the individual they relate to and must not be divulged/misused by other staff. This is to protect the employee from the likelihood of their inadvertently contravening this Act.

Each organisation will adhere to the requirements of the Computer Misuse Act 1990 by ensuring staff are made aware of their responsibilities regarding the misuse of computers for personal gain or other fraudulent activities. Any member of staff found to have contravened this Act will be considered to have committed a disciplinary offence and be dealt with accordingly.

The Access to Health Records 1990

This Act gives patient’s representatives right of access to their manually held health records, in respect of information recorded on or after 1 November 1991. This Act is only applicable for access to deceased persons records. All other requests for access to information by living individuals are provided under the access provisions of the Data Protection Act 1998.
G  Guidance for providing information for service users

To comply with the requirements of the Data Protection Act 1998, The Human Rights Act 2000 and the Caldicott requirements service users should be informed of the following when providing personal information as part of the process of providing them with care and/or treatment.

The identity of the organisation

The identity of the person to contact with any queries or for further information

The purpose or purposes their information will be used

To whom the information may be shared with/disclosed to

Any other information deemed to be necessary

This can be achieved by the use of information leaflets and/or posters or by adding to any data collection form the service user will complete. The most common way of addressing this is the use of information leaflets.

The leaflets should provide sufficient information for the service user and/or their representative to know all the details highlighted above.

The organisation collecting the information must (if possible) ensure the service user has understood the information provided to them and if deemed necessary this should be recorded e.g. in the service user record.

The information leaflet, or other written information, should comply with the requirements detailed in the Disability Discrimination Act 1995 and, if possible, the recommendations of the RNIB.

RNIB recommendations:

- Font should be Arial 14pt (no fancy fonts)
- Avoid using all capital letters
- Avoid light type weight
- Line lengths should ideally be between 60-70 letters per line
- Allow plenty of space for the service user to fill in their own information (if they are required to provide any and/or to sign the form)
- Avoid glossy paper
- Ensure leaflets are available in larger print for those who need them (normally upon request – which should be detailed in the information leaflet) e.g. 22 font
H Register of authorised users to the EHSCR

THIS IS A DRAFT ONLY TO LIST WHAT SHOULD BE INCLUDED –

Form to include the following:

Surname
First name
Job title
Department
Organisation
Staff number

Access required to
For what purpose

Access to begin (date)
Access to end (date for those who do not need access all the time)

Signature of employee/system user
Signature of manager (of employee/system user)

For EHSCR staff use only:
Set up on:
Disabled on:
Training provided:
I Standing Committee for the EHSCR Security and Confidentiality

Terms of Reference for the Standing Committee for the Security & Confidentiality of Person Identifiable Information for the West Surrey Electronic Health & Social Care Record

1 Title
Standing Committee for the Security & Confidentiality of Person Identifiable Information.

2 Context
Health and social care organisations in West Surrey wish to improve information sharing across organisational boundaries supported by information technology in the form of the West Surrey Electronic Health and Social Care Record (EHSCR). This EHSCR creates a virtual record combining information held by participating agencies in their computer systems as custodians of information owned by the service user. Access to the record is granted based on the ability to meet and maintain the standards stated in current agreed version of the West Surrey ‘Protocol for the Secure and Confidential Sharing of Person Identifiable Information’.

3 Reporting line
During the project to develop and implement the EHSCR the Standing Committee will report to the EHSCR Project Board.

The representative members of the Standing Committee will be responsible for reporting back to their organisations.

Any issues that cannot be resolved by the Standing Committee will be escalated to the Project Board.

As part of the Project Handover the reporting line of the Standing Committee will be moved to the management structure that takes responsibility for the operation and on-going development of the EHSCR.

4 Membership
Chair to be appointed by the EHSCR Project Board initially, and thereafter the management structure that takes responsibility for the operation and on-going development of the EHSCR.
The management organisation of the EHSCR must be represented by:

- The senior manager/director responsible for developing/implementing/maintaining the EHSCR

Each organisation participating in the EHSCR must be represented on the Standing Committee by people fulfilling the following roles:

- Caldicott Guardian (or equivalent in any organisation not required to identify this role)
- Senior management of information and technology
- Management responsibility for implementing procedures

Meetings may also be attended by personnel co-opted by the Committee or invited by the members of the Committee because of their role in developing, implementing and/or maintaining the EHSCR and the interfaces with the organisations.

5 Aim
To ensure that the operating procedures of organisations who have access to the Electronic Health and Social Care Record comply with the "Protocol for the Secure and Confidential Handling of Person Identifiable Information" and that those procedures are continually monitored and developed.

6 Objectives
A. To be responsible for reviewing, updating and disseminating the information sharing protocol.

B. To control access by organisations to the EHSCR.

C. To ensure the EHSCR is operated in a secure and confidential manner.

7 Meetings
Meetings will be held monthly during the development and implementation. The frequency can be reviewed and agreed by the Standing Committee as it sees fits but should occur at least quarterly.
8 Specific responsibilities

A THE PROTOCOL

1. To ensure that Section 5 of the Protocol reflects the general principles of information flows enabled by the EHSCR and that detailed documentation regarding information flows is maintained by the management of the EHSCR.

2. To ensure that organisations seeking to use the EHSCR understand and meet the requirements for membership. *(NOTE: Appendix A of the protocol includes notes on required actions.)*

3. To keep the information sharing protocol up to date to take account of changes to legislation, guidance issued by the government and professional bodies and as the result of relevant case law.

4. To review the information sharing protocol at least annually and record changes in the version control sheet (at the front of the document).

5. To deliver a current up to date version of the information sharing protocol to each organisation’s Caldicott Guardian, who is also responsible for ensuring that this is occurring.

B CONTROLLING ACCESS

6. To ensure that access by an organisation to the EHSCR only occurs when the information sharing protocol has been signed by the Chief Executive and the Caldicott Guardian (or equivalent) for each organisation in the format set out in the document. This format covers capability and intention to act in accordance with the protocol.

7. To take action to stop access if an organisation continues in serious breach of the requirements.

C OPERATION

8. To agree how to monitor compliance with the requirements of the information sharing protocol. *(It is envisaged that this could occur in a variety of ways but an internal audit and/or external audit of the documents requirements and compliance with those requirements will probably be undertaken by auditors of one or more of the organisations involved.)*

9. To monitor compliance with the requirements of the information sharing protocol.
10. To ensure that a register is produced and maintained of who has been granted access to the EHSCR. It should include details of the person, the purpose for which they need access, what they need access to, and for how long access is granted.

11. To develop and agree categories of incidents of breach of the protocol to be used by each organisation in their log of incidents to highlight why breaches have occurred e.g. 'lack of training', 'misunderstanding of requirements', or 'problems with technology'.

12. To review and monitor incidents recorded and investigated by each organisation as breaches of the protocol with the purpose of ensuring future compliance.

13. To undertake management reporting on breaches of the protocol to the Project Board (and its successor). (It is noted that each organisation will be responsible for informing regulatory bodies that need to know of any breaches.)
J Approval for operational use of the EHSCR