Information Sharing Protocol

<table>
<thead>
<tr>
<th>Author(s)</th>
<th>Neil Taylor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>0.1</td>
</tr>
<tr>
<td>Version Date</td>
<td>23 September 2013</td>
</tr>
<tr>
<td>Implementation/approval Date</td>
<td>25 September 2013</td>
</tr>
<tr>
<td>Review Date</td>
<td>September 2014</td>
</tr>
<tr>
<td>Review Body</td>
<td>Information Governance Steering Group</td>
</tr>
<tr>
<td>Policy Reference Number</td>
<td>030</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Version</th>
<th>Author</th>
<th>Date</th>
<th>Reason for review</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>Neil Taylor</td>
<td>September 2013</td>
<td></td>
</tr>
<tr>
<td>1.0</td>
<td>Neil Taylor</td>
<td>September 2013</td>
<td>Final</td>
</tr>
</tbody>
</table>
1.0 Summary

This document is a combined Tier 1 and Tier 2 information sharing protocol (ISP) recommended to NHS health organisations. It sets out standards that staff in partner organisations must adhere to. It is intended to complement any existing professional Codes of Practice that apply to any relevant professionals working within partner organisations.

Tier 1 is the highest level in the protocol structure and applies to all sharing of personal information. It contains the general key principles of information sharing and the legislative standards that all types of personal information sharing must comply with. This has been provided in the first section of this document.

Tier 2 is a Purpose Specific Information Sharing Agreements (PSISA). PSISAs specify information to be shared, how and with whom information will be given. Responsibility for the production and sign off of PSISAs rests with the Head of Service. PSISAs must comply with the principles set down in this Overarching Protocol.

As the Health and Social Care Information Centre (HSCIC) release further information regarding Information Sharing in relation the Accredited Safe Haven’s (ASH) this document will be reviewed to comply with the HSCIC instructions.

2.0 Introduction

Effective information sharing allows organisations to improve the provision of health and care services, protects the public and identifies and supports meeting statutory requirements. NHS Greenwich Clinical Commissioning Group (CCG) recognise the importance of having clear guidelines to follow, ensuring that information is shared in a secure and confidential manner and in accordance with the law (including the common law of confidentiality, the Data Protection Act 1998, the Human Rights Act 1998 and other related legislation and guidance).

This Overarching Information Sharing Protocol (and its appendices) comprises a set of rules that the CCG will comply with when sharing personal information with another partner agency. It also sets out the standards that staff must follow when sharing personal data.

The sharing of anonymised information for statistical purposes is outside of the remit of this protocol, as the majority of legislation and rules identified concern only the sharing of personal information. However, the Purpose Specific Information Sharing Agreement template created under this protocol can be used to form a basis for the sharing of anonymised information.

Signatories to this protocol are normally the highest level official within the partner organisation (e.g. Authorised Officer or Chief Executive). This high level commitment recognises that information sharing is a key strategic objective of the partnerships within the NHS.
GP and Dental practices within NHS Greenwich CCG catchment are encouraged to implement their own protocol and they are free to model their protocol on this if they wish. In this case NHS Greenwich CCG will waive their copyright on this protocol.

2.01 Objectives

This protocol defines the framework for the legal, secure and confidential sharing of personal information between healthcare organisations.

This Protocol:

- Clarifies the legal background on information sharing
- Outlines the principles that are needed to underpin the process
- Provides practical guidance on how to share information in a series of supporting procedures
- Provides a framework within which organisations can develop Purpose Specific Information Sharing Agreements (PSISA) for specific areas of service.
- Includes arrangements for reviewing the use of this Protocol and for responding to breaches of this protocol or any of the PSISAs.

3.0 Scope of Overarching Information Sharing Protocol

This ISP applies to all staff (Including students, trainees on temporary placements, and volunteers) in the CCG and organisations signed up to this protocol when sharing information with partner organisations.

4.0 Governance

This Protocol will be formally signed off by the Authorised Officer (or relevant senior officer) for each of the partner organisation.

Formal adoption will follow as soon as two or more partners have signed this document. This document then forms the basis for information exchanges between those organisations who have signed up.

Breaches of this protocol and subsequent PSISAs will be managed according to the Procedures set out in the Handling Breaches section.

5.0 Legislation/Guidance to be considered when sharing information

The legal framework within which public sector data sharing takes place is fairly complex it is essential that practitioners sharing information are clearly aware of the legal framework within which they are operating.

Staff should always consult their Information Governance/relevant teams in their organisations if unsure which legal framework they are operating within when sharing information.
More recent detailed guidance on legislation of relevance to information sharing can also be found in NHS Information Governance – Guidance on Legal and Professional Obligations

6.0 Key Principles - Organisation responsibilities

All partners identified in this agreement are responsible for:

- Being committed to sharing person identifiable information to provide effective services to individuals and to the public at large, where this exchange is compliant with their powers and with their statutory responsibilities
- Nominating a Senior Management representative responsible for ensuring security, data protection, data quality and confidentiality within their organisation
- Ensuring that employees, contractors, volunteers and all individuals for whom the organisation is responsible, are competent in handling person identifiable information, including a basic understanding of their responsibilities under the Data Protection Act 1998, Human Rights Act 1998 and common law duty of confidence
- Ensuring that all aspects of information security and confidentiality are considered for all new and existing instances of routine information sharing and/or joint processing, and support compliance with the stated principles.
- Ensuring that all staff with direct or indirect access to PCD, confidential or sensitive information are appropriately trained in information governance and have clear guidance on the processing, sharing and secure transfer of that data

6.01 Justification for sharing

Partners are responsible for:

- Ensuring that when person identifiable information is shared and/or jointly processed it will be in accordance with current legislation and common law duties
- Defining the purpose and justification for information sharing, ensuring alternatives to sharing person identifiable information and the impact of sharing on all the relevant stakeholders are considered
- Ensuring that when sharing person identifiable information only the minimum required for the purpose is shared.

6.02 Fairness and transparency

Partners are responsible for:

- Recognising that the public have rights of privacy and confidentiality and that sharing and/or joint processing of person identifiable information will respect these rights
- Ensuring that:
  - the public are informed of the purposes for processing their information
  - the public are informed which other organisations it may be disclosed to consideration is given to whether consent of the data subject is required, and if so, will be sought (and complied with), unless there is a legal obligation that overrides this requirement
• Developing procedures to address requests for further information, complaints and concerns raised by members of the public or by staff concerning the implementation of this guidance and any resulting information sharing agreements, procedures or guidance.

6.03 Information standards

Partners are responsible for:

• Ensuring processes are in place to check the quality of the person identifiable information before it is shared.
• Ensuring all information flows are documented and secure methods of transfer are in place (e.g. Nhs.net to Nhs.net)
• Ensuring that all information is clearly marked according to organisational classification guidelines, such as CONFIDENTIAL or RESTRICTED

6.04 Retention of shared information

Partners are responsible for:

• Ensuring retention and disposal processes and schedules are agreed for the information being shared in line with statutory and organisational requirements.

6.05 Security of shared information

Partners are responsible for:

• Taking responsibility for restricting access to person identifiable information that they process and the secure exchange of person identifiable information in line with principle 7 of the Data Protection Act.
• Setting out standards for the technical security arrangements that must be in place to protect shared information during transfer and within partner organisations.
• Ensuring that all personal identifiable information is transferred in line with national security guidance and protocols.

6.06 Security of data processed on behalf of other Organisations

Partners are responsible for:

• Taking responsibility for restricting access to person identifiable information that they process and the secure exchange of person identifiable information in line with principle 7 of the Data Protection Act (See appendix 5 and for further guidance)
• Ensuring that person identifiable data is processed to the instructions of the data controller by the providing assurance, details of processes used and being subject to audit
7.0 Handling incidents & breaches

7.01 Reporting incidents and breaches of this Protocol

All incidents & breaches are to be logged, investigated, and the outcome noted as part of the concerned organisations incident handing procedures and DH guidance.

The following types of incidents will be logged:

- Refusals to disclose information
- Conditions being placed on disclosure
- Delays in responding to requests
- System, application or process error resulting in significant delay or failure to comply
- Disclosure of information to members of staff who do not have a legitimate reason for access
- Non-delivery of personal information
- Disregard for procedures
- The use of data/information for purposes other than those agreed in the protocol
- Inadequate security arrangements.

7.02 Breaches noted by members of staff

A member of staff (or other person) working on behalf of any organisation party to this protocol who becomes aware that the procedures and agreements set out in a PSISA are not being adhered to, whether within their own or a partner organisation, should first raise the issue with the line manager responsible for the day-to-day management of the PSISA.

The manager should record the issue and check whether the concern is justified. If the manager concludes that the PSISA is being breached, they should first try to resolve it informally. If the matter can be resolved in this way, the outcome should be noted and forwarded to the designated person for that PSISA.

7.03 Breaches alleged by a member of the public

Any complaint raised by, or on behalf of, a member of the public concerning allegations of inappropriate disclosure of information will be dealt with in the normal way by the internal complaints procedures of the organisation who received the complaint: Any disciplinary action will be an internal matter for the organisation concerned.

In order to monitor adherence to and use of the protocol, procedures should be established within each organisation by which complaints relating to the inappropriate disclosure of information is passed by the officer designated to deal with breaches of the PSISA. The designated officer should report any complaints of this nature to the equivalent officer in each relevant organisation. All alleged breaches of the protocol, whether proven or not, should be analysed as part of the formal review of each PSISA.
8.0 Monitoring Compliance with this Protocol

8.01 Monitoring of compliance

<table>
<thead>
<tr>
<th>Measurable Protocol Objective</th>
<th>Monitoring/Audit Frequency of monitoring</th>
<th>Responsibility for performing the monitoring</th>
<th>Monitoring reported to which groups/committees, including responsibility for reviewing action plans</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Governance Steering Group</td>
<td>Quarterly</td>
<td>Information Governance Lead</td>
<td>Audit Committee</td>
</tr>
</tbody>
</table>

8.02 Non Compliance

Non-compliance with this code of conduct by any person working for the CCG may result in disciplinary action being taken in accordance with the disciplinary procedure.

To obtain a copy of the disciplinary procedures please discuss with your manager or the Human Resources department.

9.0 Implementation and dissemination of document

The Protocol, once approved by the CCG’s governing body, or delegated group, will be shared with all staff through the all staff email, updated on the intranet, and shared with the CCG’s Management Board. A team briefing will be provided to support this dissemination.

10.0 Training Requirements

Training will be carried out for this protocol in line with the Information Governance Training Needs Assessment.

11.0 Latest Version

The audience of this document should be aware that a physical copy may not be the latest version. The latest version, which supersedes all previous versions, is available on the CCG Internet and Intranet.

12.0 Associated Documents

As a new organisation, the CCG is still developing a broad range of policies, protocols and procedures, which will be subject to further updates and additions. Related CCG policies, protocols and procedures currently include:

- Consent to use PCD Policy
- E-mail Policy
- Information Governance Policy
• Internet Policy
• Mobile Device Policy
• Records Management Policy
• Acceptable Use Protocol
• Confidentiality Code of Conduct Protocol
• Freedom of Information Protocol
• Information Sharing Protocol
• Information Lifecycle Protocol
• Pseudonymisation Protocol
• Safe Haven Protocol
• Confidentiality Audit Procedure
• Subject Access to Health Records Procedure

Supporting documentation also includes:

• Information Governance Management Framework
• Information Communication and Technology Framework
• Information Governance Strategy
• Information Governance Acronyms Document
• Information Governance Roles & Responsibilities Document
• Information Governance Steering Group Terms of Reference
• Information Governance Training Needs Assessment

13.0 Appendices

Appendix 1 Equality Impact Assessment Checklist
Appendix 2 Consultation history
Appendix 1  Equality & Equity Impact Assessment Checklist

This is a checklist to ensure relevant equality and equity aspects of proposals have been addressed either in the main body of the document or in a separate equality & equity impact assessment (EEIA)/ equality analysis. It is not a substitute for an EEIA which is required unless it can be shown that a proposal has no capacity to influence equality. The checklist is to enable the policy lead and the relevant committee to see whether an EEIA is required and to give assurance that the proposals will be legal, fair and equitable.

The word proposal is a generic term for any policy, procedure or strategy that requires assessment.

<table>
<thead>
<tr>
<th>Challenge questions</th>
<th>Yes/No</th>
<th>What positive or negative impact do you assess there may be?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Does the proposal affect one group more or less favourably than another on the basis of:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Race</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>• Pregnancy and Maternity</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>• Sex</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>• Gender and Gender Re-Assignment</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>• Marriage or Civil Partnership</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>• Religion or belief</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>• Sexual orientation (including lesbian, gay bisexual and transgender people)</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>• Age</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>• Disability (including learning disabilities, physical disability, sensory impairment and mental health problems)</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>2. Will the proposal have an impact on lifestyle?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(e.g. diet and nutrition, exercise, physical activity, substance use, risk taking behaviour, education and learning)</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>3. Will the proposal have an impact on social environment?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(e.g. social status, employment (whether paid or not), social/family support, stress, income)</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>4. Will the proposal have an impact on physical environment?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(e.g. living conditions, working conditions, pollution or climate change, accidental injury, public safety, transmission of infectious disease)</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>5. Will the proposal affect access to or experience of services?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(e.g. Health Care, Transport, Social Services, Housing Services, Education)</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

**Document Author**  14.8.13  
**Signature:**

**Equalities Lead** (Carol Berry)  16.8.13  
**Signature:**
## Appendix 2  Consultation History

<table>
<thead>
<tr>
<th>Stakeholders Name</th>
<th>Area of expertise</th>
<th>Date sent</th>
<th>Date received</th>
<th>Comments</th>
<th>Changes made</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Appendix 3 – Tier 2 Purpose Specific Information Sharing Agreement

### Details of Information to be shared
This section covers the details of the personal information covered by the agreement, how it will be collected, used, disclosed, stored and kept accurate. Leads of the partners sharing information should complete this section to provide the details.

<table>
<thead>
<tr>
<th>The information/data that will be shared;</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>for example personal identifiers, demographic, sensitive/clinical etc</em> List the items of information to be disclosed and what systems they are derived from.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>The purposes for which the data will be shared;</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>for example clinical care, provision of services, social support etc and the benefit that is to be achieved by sharing the information</em></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>The means by which the data will be shared;</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>for example paper, fax, email, electronically.</em> For regular flows of information give detail on, the process for requesting the information and the roles of the people involved in the information sharing. Also give specific details on the triggers to information sharing that takes place where the disclosures are on a case by case basis.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>The nature of the consent that will be obtained and the information that will be given to the data subjects regarding the uses to which the information collected will be put;</th>
</tr>
</thead>
<tbody>
<tr>
<td>The nature of the consent that will be obtained and the information that will be given to the data subjects regarding the uses to which the information collected will be put. Are you relying on an expressed or implied statutory power to sharing? Are you normally going to rely on consent? How long will consent be valid for under this agreement? If consent is normally required to share information for this purpose provide detail on any specific circumstances where this consent is not required.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Communication to Service Users about this information sharing &amp; how are they notified;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detail the “fair processing notice that individuals are given about data sharing under this agreement. Also outline how and when this notification is provided to individuals. If applicable, outline the circumstances where the Service User will not be told about the information sharing. If the consent is due to last for a lengthy period of time, detail at what points/how often an individual will be reminded of the fair processing information and given a subsequent chance to “opt out” having previously</td>
</tr>
</tbody>
</table>
How shared information will be recorded and held;
How will the information be stored by the receiving partner and what are the physical and technical security arrangements they have in place?

How will access to information be controlled?
Access should be limited to a need to know basis, specify if any internal or external parties have access to the information. For internal staff specify any vetting arrangements in place.

Storage and disposal of Information;
The nature of the information to be shared will have a bearing on how long it should be held. Specify in this section how long the shared information will be held. Refer to your organisations record retention schedule for further guidance or discuss with the organisation(s) that is going to be providing the information. Personal information must be securely disposed of in line with the requirement under the 7th Data Protection Principle (see Appendix b).
Appendix 4 – Declaration to the PSISA  
Information Sharing Agreement

DECLARATION OF ACCEPTANCE

_______________________________________ accepts that this Agreement provides a framework for the safe and secure sharing of personal and person identifying information between: ____________________________________ And NHS Greenwich Clinical Commissioning Group in a manner that complies with statutory and professional responsibilities.

_______________________________________ will:

1. Implement and adhere to this Agreement;
2. Establish appropriate internal systems, raise awareness, inform service users, issue specific guidance, and provide training to staff to ensure compliance with this Agreement and associated protocols;
3. Ensure that no restrictions are placed on information sharing other than those specified in this Agreement or associated information sharing protocols.

**Designated Officer:** (Should be Caldicott Guardian, or Director/nominated lead officer)

<table>
<thead>
<tr>
<th>NHS Greenwich CCG</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Signature:</strong></td>
<td><strong>Signature:</strong></td>
</tr>
<tr>
<td><strong>Name:</strong></td>
<td><strong>Name:</strong></td>
</tr>
<tr>
<td><strong>Position:</strong></td>
<td><strong>Position:</strong></td>
</tr>
<tr>
<td><strong>Date:</strong></td>
<td><strong>Date:</strong></td>
</tr>
</tbody>
</table>
Appendix 5 – Legislation/Guidance to be considered when sharing Information

Legislation that Requires Information to be Shared when requested to do so

Information can be shared without consent if requested to do so by the following public bodies/officials but individuals should be informed that disclosure has been required.

<table>
<thead>
<tr>
<th>Public Body/Official</th>
<th>Reason for Sharing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Courts, including a coroner’s court, tribunals and enquiries</td>
<td>Only give the information requested in the order and no more. Many different Acts give courts the powers to issue court orders.</td>
</tr>
<tr>
<td>General Medical Council (GMC)</td>
<td>Entitled to access confidential patient health records as part of an investigation under the Medical Act 1983. The GMC have indicated that they would always try to obtain consent first – refer to the GMC website at <a href="http://www.gmc-uk.org">http://www.gmc-uk.org</a></td>
</tr>
<tr>
<td>Audit Commission</td>
<td>Entitled to access confidential patient health records as part of an investigation under section 6 of the Audit Commission Act 1998 (refer to the Audit Commission website at <a href="http://www.auditcommission.gov.uk/">http://www.auditcommission.gov.uk/</a>)</td>
</tr>
<tr>
<td>Health Service Ombudsman</td>
<td>The Health Service Ombudsman have the same powers as the courts to require disclosure of person identifiable information. Any request made should be complied with without obtaining a court order.</td>
</tr>
<tr>
<td>Care Quality Commission</td>
<td>The Care Quality Commission is the independent regulator of health and social care in England. Their aim is make sure better care is provided for everyone, whether that’s in hospital, in care homes, in people’s own homes or elsewhere. They regulate health and adult social care services whether provided by the NHS, local authorities, private companies or voluntary organisations and they protect the rights of people detained under the Mental Health Act.</td>
</tr>
<tr>
<td>Immunisations and vaccinations</td>
<td>Under the Education Act 1944 information must be passed to NHS Trusts from schools.</td>
</tr>
<tr>
<td>Births and Deaths</td>
<td>The Births and Deaths Act 1984 provides for the registration of births, stillbirths and deaths.</td>
</tr>
<tr>
<td>National Information Governance Board</td>
<td>The National Information Governance Board for Health and Social Care (NIGB) provides leadership and promotes consistent standards for information governance across health and social care. It considers ethical issues; the interpretation and application of the law and policies; and provides advice on information governance matters at a national level. The Board reports annually to the</td>
</tr>
</tbody>
</table>
Secretary of State for Health and is responsible for the NHS Care Record Guarantee for England. Members of the Board are either members of the public appointed by the Appointments Commission or represent stakeholders in health and social care. The Health & Social Care Act 2008 establishes the NIGB as a statutory body. From January 2009, the NIGB function includes administration of applications under section 251 of the NHS Act 2006 which allows the common law of duty of confidentiality to be set aside in specific circumstances. This function was formerly carried out by the Patient Information Advisory Group (PIAG) which was abolished on 31 December 2008.

Members of Parliament

Information can only be shared with MP’s without consent when they are acting on behalf of the patient e.g. the patient has contacted the MP with a view to them investigating on behalf of the individual. If their constituent is not the patient but is instead a relative or friend, then explicit consent is required before sharing any information.

DWP & Service and Personnel Veterans Agency

The DWP are not required to provide consent to the sharing of information, for the purposes of assessing benefits and monies due to individuals.

Information sharing that requires Explicit Consent

The Department of Health has identified certain situations where Explicit Consent is required for information sharing that does not directly contribute to direct continuing healthcare of an individual. In these instances, Explicit Consent will always be required unless there is a robust public interest in favour of releasing information without consent. For most information sharing issues that are not for the direct continuing care of individual, organisations should consult their Information Governance Lead or Caldicott Guardian. Information sharing for purposes that are not for the direct continuing healthcare of an individual (this list may not be exhaustive) (with the exception of the Single Assessment Process), are as follows:

<table>
<thead>
<tr>
<th>Common Assessment Framework which incorporates Single Assessment Process</th>
<th>Refer to your Common Assessment Framework Information Sharing Protocol for further guidance. This process requires explicit consent even though it is for the direct continuing healthcare of an individual.</th>
</tr>
</thead>
<tbody>
<tr>
<td>NHS Complaints Committees</td>
<td>Complaints committees will invariably need individual’s personal information. However, explicit consent of the complainant, and any other individual whose records may need to be reviewed, is required prior to disclosure</td>
</tr>
<tr>
<td>Management</td>
<td>Commissioning, prescribing advisors, financial audit,</td>
</tr>
<tr>
<td>Purposes</td>
<td>resource allocation etc., - no restrictions are imposed if the data is anonymised. The explicit consent of individuals must be sought for information about them to be disclosed for these purposes in an identifiable form, unless disclosure is exceptionally justified in the public interest, or has temporary support in law under section 251 of the NHS Act 2006.</td>
</tr>
<tr>
<td>Occupational Health Professionals</td>
<td>Information on staff referred to occupational health departments. However, if clinicians are the patients, the powers of professional regulatory bodies for disclosure may apply.</td>
</tr>
<tr>
<td>Researchers</td>
<td>Although research is not incompatible with healthcare purposes the Information Commissioner does not consider it an essential element of providing healthcare, therefore, explicit consent is required. Whilst individuals are generally aware and supportive of research it is not reasonable to assume that they are aware of and consent to each and every research subject or proposal. Before any research project can be undertaken, application must be made to the Local Research Ethics Committee for approval. If the research project is to use anonymised data, (which is preferable) no restrictions are imposed. If there is any doubt about, then refer to National Information Governance Board (NIGB)</td>
</tr>
<tr>
<td>Teaching</td>
<td>According to Confidentiality: NHS Code of Practice, teaching is not to be regarded as direct healthcare purposes and will require explicit consent.</td>
</tr>
<tr>
<td>Sure Start Teams</td>
<td>Disclosures to Sure Start teams for anything other than the direct continuing healthcare of young children needs explicit consent from those with parental responsibility.</td>
</tr>
<tr>
<td>Hospital Chaplains</td>
<td>When an individual is unable to give explicit consent because they are unconscious, the decision rests with the healthcare professional treating the individual. Care should be taken to restrict the amount of information disclosed to ‘what is necessary’ in the individual’s best interests, (refer to section 4.2 Best Interest) and, where appropriate, listening to the views of relatives before making a decision to share or not to share.</td>
</tr>
<tr>
<td>The Media</td>
<td>You need explicit consent to release information to the media about care and treatment (including an individual’s presence in a hospital) unless there is an exceptional robust public interest (refer to section above on the Public Interest) in releasing information (updates on celebrities, distressing incidents e.g. fire, road traffic accidents etc.)</td>
</tr>
<tr>
<td>Police</td>
<td>Information required by the Police either needs explicit consent of the individual, a Court Order or,</td>
</tr>
</tbody>
</table>
where criminal activities are concerned, refer to section 5.3 Enabling Information Sharing in the Public Interest. (Also, refer to your local information sharing agreements, if appropriate)

**Solicitors**

Solicitors requesting individual information must produce an up to date written, signed consent from the individual, before releasing any information to them. If you have any doubts as to the authenticity of the consent or the fact that the whole of the individual’s record has been requested, contact the individual direct – you must obtain consent from any third parties before releasing third party information.

**Companies and The paper Concordat and Moratorium on**

Genetics and Insurance effective from 14th March 2005 states that patients do not have to disclose predictive genetic tests results when applying for insurance cover unless required to do so under certain conditions. Care should be taken so that accidental disclosure of this information is avoided when insurance companies request medical reports in relation to an insurance policy to be taken out by an individual.

---

**Legislation Enabling Information Sharing in the Public Interest**

The following legislation enables information to be shared without seeking consent e.g. if you believe someone has committed a crime, the Crime and Disorder provisions in section 115 of that Act state you can share this information, e.g. Police Service. However, this type of legislation does not enforce you to do so. Decisions to share should be made on a ‘case by case’ basis, in the public interest, refer to section 5.3 Public Interest.

- **Child Protection** (Children’s Acts 1989 & 2004 and The Protection of Children Act 1999). Allows information to be shared if a child is considered at risk, e.g. Child Protection. General referred to as safeguarding provisions has an implied duty to share information to prevent harm.
- **Prevention and Detection of Crime** (Section 115 of the Crime and Disorder Act 1998) e.g. requests from the Police where someone is suspected of committing a serious crime.
- **Disclosures to a health professional within a Sure Start Team under the NHS Act 1997** where disclosures directly and only support healthcare of young children. If health records are to be held within partner organisations, those with parental responsibility must be properly informed.
- **Data Protection Act 1998** (the Act), section 29(3) provides that the non disclosure rules will not apply if information sharing is required for: the prevention or detection of crime, the apprehension or prosecution of offenders or the collection or assessment of any tax or duty. (The Police may request information under section 29(3) of the Act). Section 35 of the Act provides that disclosures required by law or made in connection with legal proceedings are also exempted from non disclosure. However, the decision to disclose must be weighed against the individual’s rights of data protection.
Legislation Restricting Information Sharing

The following legislation allows information to be shared only between the healthcare professionals actually treating the individual.

- Venereal Diseases Act 1917 & Venereal Diseases Regulations of 1974 and 1992
- Abortion Act 1967
- The Adoption Act 1976
- The Gender Recognition Act 2004

Additional useful relevant legislation/Acts of Parliament explained in brief

Access to Health Records 1990
This Act gives patients’ representatives right of access to their 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.

Mental Capacity Act 2005
From 1 October 2007 this Act is fully in force in England and Wales. It impacts on all staff working with or caring for adults (16+) who lack mental capacity (or have impaired capacity) to make their own decisions about health, social care and financial matters. The Act makes clear who has authority to make decisions in certain situations and sets out statutory principles which must guide decision-making. Doctors have a legal duty to have regard to the Code of Practice in their day to day decisions about the treatment and care of incapacitated patients. So it is important that doctors take steps to familiarise themselves with the legal principles, and the provisions of the Code which are of most relevance to their areas of practice.

Civil Contingencies Act 2004
The Act, and accompanying regulations and non-legislative measures, will deliver a single framework for civil protection in the United Kingdom to meet the challenges of the twenty-first century. The Act is separated into two substantive parts: local arrangements for civil protection (Part 1) and emergency powers (Part 2). The overall objective for both parts of the Act is to modernise outdated legislation. Key to this is an updating of the definition of what constitutes an “emergency”.

The Act focuses on three types of Threat:

This does not mean that the definition of “emergency” is the same in both Parts. In Part 1, the threat must pose a threat of serious damage to human welfare or the environment of a “place” in the United Kingdom. This reflects the fact that Part 1 is designed to deal with preparations by local responders for localised emergencies. In Part 2, the threat must pose a threat of serious damage to human welfare or the
environment of one of the English Regions, or one of the other constituent parts of the UK (Scotland, Wales or Northern Ireland). This higher threshold reflects the fact that Part 2 is designed for use in very serious emergencies which affect a larger geographical area, Cabinet Office (no date)

**Computer 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 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 would be considered to have committed a disciplinary offence and be dealt with accordingly.

**Crime and Disorder Act 1998**
This Act allows disclosures of information (including that which identifies a person) to the Police, Local Authorities, Probation Service or Health Service where disclosure is necessary or expedient for the purposes of any provision of the Act. The provisions of the Act include Orders (e.g. Anti-Social Behaviour and Sex Offender Orders) and the formulation and implementation of local Crime and Disorder Strategies. Furthermore the Act imposes a duty on Health Authorities (and other authorities) to exercise its various functions with due regard to the likely effect of the exercise of those functions, and the need to do all that it reasonably can to prevent, crime and disorder in its area. 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.

**Human Rights Act 1998**
This Act became law on 2 October 2000. It binds all Organisations and health care professionals 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 patient/individual’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 of 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.

**Criminal Procedures and Investigations Act 1996**
The Criminal Procedures and Investigations Act 1996 requires the police to record in durable form any information that is relevant to an investigation. The information must be disclosed to the Crown Prosecution Service CPS, who must in turn disclose it to the defence at the relevant time if it might undermine the prosecution case. In cases where the information is deemed to be of a sensitive nature then the CPS can apply to a judge or magistrate for a ruling as to whether it should be disclosed.
The Police and Criminal Evidence Act 1984

The Police and Criminal Evidence Act 1984 provides a guide to what may be regarded as sufficiently serious to justify disclosure in the public interest, but it should not be treated as either conclusive or exhaustive.

Section 116 contains definitions of what it calls a ‘serious arrestable offence’, i.e. one which has caused or may cause:

- serious harm to the security of the state or to public order
- serious interference with the administration of justice or with the investigation of a offence
- death
- serious injury (including any disease and any impairment of a person’s physical or mental condition)
- substantial financial gain or serious financial loss.

Criminal Justice Act 2003

The Criminal Justice Act 2003 received Royal Assent on 20 November 2003. It aims to modernise the criminal justice system. The Act supports victims, protects witnesses and delivers justice. Through joint working (Police and CPS) more crimes can be detected, reduction of offences committed on bail and more defendants brought to court. The criminal trial process reforms will ensure that all relevant evidence will be heard by magistrates, judges and juries. In conjunction with the Police Reform Act 2002 and Courts Act 2003, the new measures in the Criminal Justice Act 2003 will create a system which convicts the guilty, acquits the innocent and reduces offending and re-offending.

The Criminal Justice Act 2003

Key provisions in the Criminal Justice Act 2003
http://www.cjsonline.gov.uk

Freedom of Information Act (FOIA) 2000 requests

A number of the partner organisations are “public authorities” for the purposes of the Freedom of Information Act 2000 (FOI). This means that they could receive requests for information relating to the information sharing activities under the resultant PSISAs developed (e.g. statistics on the amount of data sharing being undertaken or the general nature of the data sharing). It is recognised that Public Authorities are required to act under the obligations departments are under by virtue of S45 Code of Practice depicted in the FOI act (Consultation with third parties), however care should be taken by the public authority receiving the FOI request to ensure that partners to the individual PSISA are consulted in a suitable manner of the nature of the request and their intended response.