South London and Maudsley NHS
NHS Foundation Trust

Information Sharing Policy

Version:	3.0
Ratified By:	Trust Executive
Date Ratified:	07/08/2013
Date Policy Comes Into Effect:	07/08/2013
Author:	Head of Information Governance
Responsible Director:	Director of ICT
Responsible Committee:	Caldicott Committee
Target Audience:	All Trust staff (permanent and temporary) and contractors
Review Date:	07/08/2015

Equalities Impact Assessment	Assessor: Head of IG	Date: 10/07/2013
HRA Impact Assessment	Assessor: Compliance Manager	Date: 13/07/2011

Document History

Version Control

Version No.	Date	Summary of Changes	Major (must go to an exec meeting) or minor changes	Author
1	March 2009	New Policy	First version	Information Governance Manager
1.1	April 2011	Amendments to information sharing arrangements with	Minor	Head of Information Governance
2	July 2011	Policy updated	Minor	Head of Information Governance
3	August 2013	Policy updated in line with DH IG Review	Major	Head of Information Governance

Consultation

Stakeholder/Committee/ Group Consulted	Date	Changes Made as a Result of Consultation
Caldicott Committee	10/07/2013	Updates based on the National IG Review

Plan for Dissemination of Policy

Audience(s)	Dissemination Method	Paper or Electronic	Person Responsible
All Staff	Via SLAM e-bulletin	Electronic	Policy Co-ordinator

Contents

1- Policy Summary

1.1 South London and Maudsley NHS Foundation Trust (the Trust) works with partner agencies to provide mental health, learning disabilities and substance misuse services.

1.2 Service users disclose sensitive personal confidential information about themselves relating to their health and other personal matters whilst using Trust services. This sensitive personal information is given in confidence for the provision of healthcare. Service users have the legitimate expectation that Trust staff will respect their privacy and act appropriately.

1.3 This information sharing policy is an overarching document, which provides guidelines to ensure that sensitive clinical information is shared between the Trust and its partner agencies for the purposes of delivering and improving service user care, teaching, research, audit and protecting the public in a secure and confidential manner and in accordance with the law.

1.4 The Trust is accountable for any decisions made to pass on information to another agency or individual. Corporate oversight of this is the responsibility of the Trust's Caldicott Guardian.

1.5 Staff should ensure that there is a justifiable 'need-to-know' on the part of the recipient requesting information, consider whether it is possible or appropriate to anonymise or pseudonymise the information, seek the service user's consent to such disclosure in accordance with this Policy and the guidance set out in the Trust Confidentiality Policy and keep disclosures to a minimum.

1.6 Staff provide sensitive personal information to the Trust during their employment. The Trust has a legal responsibility to ensure the security and the confidentiality of personal staff information in the same way as service user information.

1.7 Key disclosure models are summarised in Appendix A for guidance.

2- Introduction

Service users, their carers and families provide personal confidential information to clinical services in the Trust. Care professionals rely on this information as it enables clinical services to identify the most appropriate treatment and care options suitable for each service user. Such sensitive personal information is provided in confidence. Service users expect that that the Trust will respect their privacy and act responsibly, fairly and lawfully.

Whilst Trust staff maintain service user confidentiality, relevant clinical information needs to flow between health and social care professionals so that service users receive all relevant support options that are available to them.

The overarching aim of the approach to information governance in the Trust is to ensure that there is an appropriate balance between the protection of service users' personal confidential information, and the use and sharing of such information to improve care.

This version of the Policy has been updated following the publication of the DH Information Governance Review: To Share or Not to Share.

3- Definitions

Information governance is the term used to describe how organisations and individuals manage the way information is handled within the health and social care system in England. It covers the requirements and standards that the organisations and their suppliers need to achieve to fulfil the obligations that information is handled legally, securely, efficiently, effectively and in a manner which maintains public trust.

Personal confidential data is the term that describes personal information about identified or identifiable individuals, which should be kept private or secret.

De-identified (anonymised) data is the term that refers to personal confidential data, which has been through anonymisation in a manner conforming to the Information Commissioner's Office Anonymisation code of practice. There are two categories of de-identified data:
• ***De-identified data for limited access:*** this is deemed to have a high risk of re-identification if published, but a low risk if held in an accredited safe haven and subject to contractual protection to prevent re-identification.
• ***Anonymised data for publication:*** this is deemed to have a low risk of re-identification, enabling publication.

Caldicott Guardian: Appointed senior clinician, who carries the ultimate responsibility to oversee the use and sharing of personal confidential and sensitive clinical information.

Safe haven: An accredited organisation/unit/service with a secure electronic environment in which personal confidential data and/or de-identified data can be obtained and made available to users, generally in de-identified form.

Third party data means both data *from* third parties and data *about* third parties. An example of data *from* a third party would be Mrs X ringing about her husband's headaches, personality change and refusal to visit the doctor.

An example of data *about* a third party includes a family history of premature stroke in the patient's siblings and other family members all listed in the patient record.

4- Purpose of this Policy

Personal confidential data is the term introduced as part of the DH Information Governance Review (2013) that describes personal information about identified or identifiable individuals, which should be kept private or secret. 'Personal' includes the Data Protection Act (1998) definition of personal data, but has been adapted to include dead as well as living people and 'confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence' and is adapted to include 'sensitive' as defined in the Act. This information includes:

- Name, address, full post code, date of birth,
- NHS number and local hospital numbers,
- Photographs, videos, audio-tapes or other images of service users,
- Anything else that may be used to identify a service user directly or indirectly. (e.g.: rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified)

The Trust and partner agencies recognise the importance of sharing information for the purposes of delivering and improving service user care, teaching, research, audit and protecting the public. This overarching policy aims to provide guidelines to ensure that sensitive clinical information is shared between the Trust and its partner agencies to facilitate the provision of seamless care in a secure and confidential manner and in accordance with the law. The same stringent procedures are applied to personal information on staff.

The Policy does not override or alter any Trust Policy and should be read in conjunction with Trust's Confidentiality and ICT Security policies.

5- Scope of this Policy

This policy has been updated following the publication of the DH Information Governance Review: To Share or Not to Share and sets out the obligations on staff in the NHS, local authorities, the Police and other organisations that work with the Trust and applies to:

- Effective and lawful information disclosures about service users, their carers, families, staff or students,
- Maintaining confidentiality.

It does not impose new obligations but reflects current legislation and regulations. The policy applies to all forms of information sharing; through whatever medium the information is shared.

Organisations dealing with specialised areas will need to agree purpose specific protocols, for example for child protection and vulnerable adults. They must refer to and be compatible with the principles and standards set out in this policy and must be signed off by the Trust Caldicott Guardian.

6- Summary of Policy Development

This policy was developed by the Trust Caldicott Committee through which it was consulted and communicated with all clinical academic groups (CAGs) and directorates across the organisation including the heads of professions.

7- Basic Principles

The Trust acknowledges that, in order to protect vulnerable people and to ensure seamless care for these people, personal information pertaining to those individuals will need to be shared with other agencies. In some circumstances, it will be necessary to share what might normally be regarded as confidential information.

The Trust has a legal and ethical duty of confidentiality to individuals, whether that is service users or staff, their families and carers, but needs to share personal information lawfully and fairly where necessary. It is therefore appropriate for the Trust to inform service users and staff that while the Trust will always respect the confidential nature of the information given for the purposes of delivering and improving mental healthcare, teaching, research, audit, employment and protecting the public, it may be necessary to share parts or all of this information with other agencies that take part in the provision of these services, subject to a series of safeguards. This must be made explicit to service users and others throughout their contact with Trust services.

7.1 Checklist prior to information sharing

There should be 'no surprises' for service users and staff about who has had access and who a record has been shared with. Service users and staff need to be made aware of the right that they may object to the use and disclosure of confidential information that identifies them.

It is essential for anyone providing any confidential information to check the following before sending:

- **Who are they?**: The identity of the requestor
- **What do they need to know?:** The content of information requested
- **Why do they need to know?**: The validity of their justification of the request and appropriate use of approved requests forms (eg. Metropolitan Police S.29(3) form)
- **Data quality**: The accuracy of the requestor's contact details,
- **Data security**: The appropriateness and the security of the medium, which is going to be used (e.g. post, fax, telephone, e-mail, physical transfer etc.).

Partner organisations have nominated senior professionals (e.g. Caldicott Guardian or Information Governance Manager in the NHS and Social Services organisations), who are ultimately responsible for ensuring mechanisms are in place to ensure compliance with this Policy and other relevant legislation.

7.2 Consent to share information

The Trust will only share personal confidential information with other agencies on a 'need-to-know' basis **with consent** or when required to do so under the law or for the purposes of the protection of the public or the promotion of public health and knowledge.

Informed consent to share information will be obtained from individuals or, in the case of children without sufficient capacity from their parent, guardian or local authority. If this is not possible and the service user or others are at risk, it will be necessary to override this in accordance with the principles of the Data Protection Act (1998).

Where an individual is unable to give informed consent if they lack the capacity to make their own decisions, the Mental Capacity Act (2005) is intended to protect them. The Act allows the person, while they are still able, to appoint someone (for example a trusted relative or friend) to make decisions on their behalf, in their best interest once they lose the ability to do so. The Mental Capacity Act (2005) introduces a Code of Practice for healthcare workers who support people who have lost the capacity to make their own decisions. Staff should refer to section 16 of this guidance when making decisions about access to information for service users/patients who lack capacity.

The form in Appendix F (or a partner agency form designed for the same purpose with required information) of this Policy should be used when requesting disclosure of personal information without the consent of the individual. Staff may find it useful to refer to the disclosure models summarised in Appendix A for guidance. **It is essential for staff providing any sensitive information to check accuracy of contact details before sending.**

Each agency handling sensitive personal identifiable information must adhere to the Caldicott Principles when collecting, holding or disclosing such information.

Caldicott Principles are:

- Justify the purpose(s) for using personal confidential information
- Only use it when absolutely necessary
- Use the minimum that is required
- Access should be on a strict need-to-know basis
- Everyone must understand their responsibilities
- Understand and comply with the law
- The duty to share information can be as important as the duty to protect patient confidentiality.

These principles are explained in more detail in the Trust Confidentiality Policy.

Health and social care professionals should be able to rely on 'implied consent' when sharing personal confidential data in the interests of direct care, as long as the patient does not object, or has not already done so.

The need to share some information does not entail the sharing of everything; only relevant information about a service user should be shared between professionals in support of their care. Consent should be obtained before sharing a patient's whole care record.

When a patient does not want to share some or all of their personal confidential data with a health and social care professional, this should be noted in the person's ePJS record. It might mean that the care that can be provided is limited and, in extremely rare circumstances, that it is not possible to offer certain treatment options. The risk of not sharing the information should be explained to them, but in general, their wishes should be respected.

All clinical staff must explain to service users, their families and carers how personal information they collect will be used for provision of care and treatment but may also be used in a format that will not identify them (anonymised or de-identified form) for research, service improvement, clinical audit and other purposes. Such explanations must highlight what rights the individual may have to dissent. Staff should hand out the leaflet entitled 'Use of Personal Information- Your Rights' to service users when they come in contact with Trust services. This discussion must be recorded on e-PJS under 'Managing Patient Information' section. (Copies of 'Use of Personal Information- Your Rights' leaflet can be obtained by contacting the Data Protection Office or at this link:

http://sites.intranet.slam.nhs.uk/ICT/Services/TeamPortfolio/informationgovernance/confidentiality/For%20Trust%20Staff/Local%20Policies/patient%20leaflet%20FINAL.pdf

People give, refuse or withdraw explicit consent. Service users can change their consent decisions at any time. These decisions should be traceable and communicated to others involved in the individual's direct care. It is very important to make a clear note of service users' wishes in relation to their personal confidential data on ePJS.

7.3 Consent Exemptions

The exceptional circumstances which override an individual's wishes arise when the information is required by statute or court order, where there is serious public health risk or risk of harm, (to other individuals or self-inflicted) or for the prevention, detection or prosecution of serious crime. In such circumstances, it may be necessary to share information without a service user's agreement because obtaining it beforehand is not practicable in the immediate circumstances or it would prejudice the purposes for which the information is being disclosed.

The exceptional circumstances are limited the following circumstances:

- through **statute**, such as the powers to collect confidential data in section 251 of the NHS Act 2006 and the powers given to the Information Centre in the Health and Social Care Act 2012;
- through a **court order**, where a judge has ordered that specific and relevant information should be disclosed and to whom; and
- when the processing can be shown to meet the '**public interest test'**, meaning the benefit to the public of processing the information outweighs the public good of maintaining trust in the confidentiality of services and the rights to privacy for the individual concerned.

All information requests in such circumstances, where it may be necessary to override service user confidentiality must be referred to the Trust Caldicott Guardian by completing the information sharing form in Appendix F. The officer requesting information must complete section 1 of this form and return it to the Data Protection

Office that will forward the request for Caldicott Guardian approval. Once the Caldicott Guardian is satisfied with the reasons proposed by the requestor, section 2 of this form will be completed by the clinical team and the information will be returned to the requesting agency.

8- Roles and Responsibilities

The Information Sharing Policy applies to all Trust employees, substantive and honorary, permanent and temporary, including Non-Executive Directors and students attached to the Clinical Academic Groups or otherwise exercising responsibilities or providing services in relation to staff or students in the Trust.

The Trust will ensure that other bodies providing services for or in conjunction with the organisation are aware of this Policy and that the Trust is also aware of their policies on information sharing.

Staff, who work across King's Health Partners must be made aware of the King's Health Partners Information Sharing Policy, which is available on the Trust intranet at http://sites.intranet.slam.nhs.uk/Policies/default.aspx

Each partner organisation will ensure that:

- The Caldicott Guardian and the Information Governance Manager are widely known within the organisation,
- Organisational policies that relate to information security, governance and confidentiality are available for their staff,
- Their staff are aware of the need for information security and confidentiality to comply with this policy,
- Requests for information are responded to within the relevant time frames.

The Trust is accountable for any decisions made to pass on information to another agency or individual. Corporate oversight of this is the responsibility of the Trust's Caldicott Guardian.

Operationally, information sharing decisions will be made by the clinical professional responsible for an individual's assessment, care or treatment or on the advice of a senior professional within the Trust, which may include the Caldicott Guardian.

8.1 Responsibilities of Both Parties

8.1.1 Act in accordance with the legal framework- The parties to this policy are expected to be fully informed on the legal framework surrounding the processing of personal identifiable information and to act accordingly. In cases of doubt, the designated officers of each organisation (the Caldicott Guardian or the Head of Information Governance for the Trust) must obtain legal advice.

8.1.2 Only provide minimum information needed- Where further disclosures or discussions take place after the original referral (for example, confirming deletion or requesting further information), information transferred between organisations should only contain the minimum information needed to identify the service user and the associated information to satisfy the further enquiry.

8.2 Responsibilities of Recipients

8.2.1 Maintain confidentiality- Once a successful transfer has taken place the recipient organisation must ensure that the information is protected against unauthorised access, modification, loss and availability. Access to the information must be restricted on a need-to-know basis.

8.2.2 No onward disclosures of confidential information to another agency- The information disclosed to the recipient is disclosed in confidence and for the use of the recipient organisation only. It must not be further processed so as to disclose personal identifiable information to another agency without the prior consent of the originating organisation.

8.2.3 Keep records of receipt- The recipient should keep full records of receipt of information, and to manage those records in a manner commensurate with their confidential nature.

8.2.4 Process information only for the specified purpose- The information disclosed to the recipient is disclosed for specific circumstances only. The recipient organisation must not further process the information for any other purpose that is incompatible with the purpose of the original disclosure.

8.2.5 Ensure secure destruction of personal identifiable information when no longer needed- Personal information cannot be held indefinitely without substantial justification for doing so. The recipient must only keep the information for as long as required (or as agreed with the partner organisation), and must arrange for its secure disposal and destruction when no longer required or requested by the sender.

8.3 Responsibilities of Senders

8.3.1 Gain consent- Informed consent to share information must be obtained from individuals or, in the case of children from their parent or guardian. If this is not possible and the service user or others are at risk, it will be necessary to override this in accordance with the principles of the Data Protection Act (1998) and the common law on medical confidentiality. The form in Appendix F (or a partner agency form designed for the same purpose with required information) must be used when requesting disclosure of personal information without the consent of the individual.

8.3.2 Use anonymised data for research and audits where possible- If information is required for medical research or audit, staff should always evaluate each project whether personal identifiable information is needed for such purposes. Unless there is genuine justification, all personal identifiable information described in section 4 of this policy should be taken out to anonymise the data for research purposes (see Appendix A of this Policy and Section 8.3 of the Confidentiality Policy on Research).

There may be exceptional circumstances, where the use of personal confidential data in research outweighs issues of privacy for public good. The Confidentiality Advisory Group of the Health Research Authority has been given powers provided under Section 251 of the NHS Act (2006) (formerly Section 60 of the Health and Social Care Act 2001) in such circumstances. It is important to note that Section 251 permits the temporary setting aside of the common law duty of confidentiality but does not set aside the requirements of the Data Protection Act (1998).

If a member of staff identifies a potential application of Section 251 of the NHS Act (2006) prior to ethical approval of a project, the case should be made to the relevant partner organisation's Caldicott Guardian. Each case will be assessed individually by the Caldicott Guardian. If supported by the Caldicott Guardian, an application will be made under Section 251 to the Clinical Advisory Group of the Health Research Authority for their assessment and approval. Such applications for research must be made alongside an application to the relevant research ethics committee. The decisions of the Clinical Advisory Group must be notified to the Caldicott Guardian in writing.

8.3.3 Keep subject fully informed- The clinical team must always strive to fully inform the service user, wherever possible, of the potential uses of their information as well as potential consequences in order to comply with the Data Protection Act (1998). All parties must remain open and transparent.

8.3.4 Keep records of disclosure- The sender must record the disclosure of information in service user's clinical records and separate records of the process must be kept by the Data Protection Department. These records must also be kept confidential.

8.3.5 Select an appropriate secure transfer method- The sender is responsible for ensuring the method of transfer is the most secure available proportionate to the urgency of the case. Staff must ensure the principles in ICT Security Policy are adhered to. The use of E-mail for the external transfer of the personal information covered by this policy should be limited to e-mail which is encrypted or securely contained within the public sector e-mail systems, such as nhs.net. Further information on secure transfer methods are summarised in section 16 of this Policy and the ICT Security Policy.

If postal delivery is the preferred method, the senders must opt for recorded delivery and mark the envelope 'private and confidential' with the return address clearly displayed.

9- Statutory Duty and Exemptions

There are legal requirements that must be considered and complied with to ensure that individuals' rights are respected and that organisations are not in breach of the law. The main statutes governing individuals rights are: -

- Data Protection Act (1998)
- Access to Health Records Act (1990) (for the records of deceased people)
- Mental Health Act (2007)
- Mental Capacity Act (2005)
- Children Act (1989)
- Crime and Disorder Act (1998)
- Criminal Justice Act (2003)
- Human Rights Act (1998)
- Health and Social Care Act (2012)
- Prevention of Terrorism Act (2005)
- London Child Protection Guidelines
- Criminal Justice Information Sharing Policy

If a public body is seeking to collect, use or share confidential and sensitive data, that organisation will need to identify a statutory duty or power enabling it to act.

9.1 Data Protection Act 1998: Exemptions around Sensitive Information
Section 27(3) and (4)- defines certain exemptions that apply to "non-disclosure provisions".

Section 29 exempts personal data processed for the following reasons from certain provisions of the Act:

(i) the prevention or detection of crime
(ii) the apprehension or prosecution of offenders

only where the application of those provisions would be "likely to prejudice" any of these purposes. This exemption must be applied on a "case by case" basis and could not be used to justify routine data matching or sharing.

9.2 Common Law / Duty of Confidence
The processing of both personal and sensitive personal data may be shared (without consent), under the Data Protection Act if necessary for a particular statutory function as identified above.

A duty of confidence is characteristic of several types of relationship such as medical (doctor/patient), legal (solicitor/client) and caring (counsellor/client). However, a duty of confidence does not necessarily arise just because a document is marked "confidential", although such a marking may be indicative of an expectation of confidentiality. In deciding whether or not disclosure of information given in confidence is justified you need to weigh the harm that would result from the breach of confidence against the harm that might result from a failure to disclose. Any disclosure must be **proportionate and the minimum necessary** to achieve the public interest objective.

9.3 Human Rights Act 1998
Public authorities must act in a way that is compatible with and promotes individuals' rights under the European Convention of Human Rights and all legislation must be read and interpreted as far as possible in a way which is consistent with those rights.

Even if a statutory power to share information has been identified and any common law duty of confidentiality overridden, the disclosure must still comply with the Human Rights Act.

Article 3: no-one shall be subjected to inhuman or degrading treatment.

Article 8: guarantees an individual's right to respect to their private and family life.

Interference with this right by a public authority can only be justified if:
1- It is in accordance with a statutory or other power authorising disclosure.
2- It is necessary for one of the following reasons
(a) the prevention of disorder or crime.
(b) the protection of health or morals.
(c) the protection of the rights and freedom of others.

3- The disclosure was proportionate i.e. only to the extent necessary to achieve the particular pressing purpose.

9.4 Crime and Disorder Act 1998

Section 115: authorises (but does not require) relevant Authorities (such as Local Authorities, Health and Police) to disclose information where it is "necessary or expedient" for the purposes of any provision of the Act i.e. the prevention and reduction of crime and the identification and apprehension of offenders or suspected offenders.

S.115 overrides the common law duty of confidence and whilst there is no need to obtain consent from the person to whom the information relates prior to its disclosure, certain general principles still apply i.e. information should only be disclosed on a need to know basis and the minimum amount of information necessary to fulfil the statutory duty should be provided.

9.5 Relevant statutory provisions concerning children

7.5.1 Children Act

Section 17: it shall be the general duty of every Local Authority to safeguard and promote the welfare of children within their area who are in need.

Section 27: Local Authorities can seek assistance from others such as Housing, Health and Education if it believes it would assist it to perform its functions under Part III of the Children Act. Those consulted must provide help by responding to the request unless to do so would be "incompatible with its own duties or would unduly prejudice the discharge of its own functions."

Section 47: Where a Local Authority has reasonable cause to suspect that a child [in its area] is suffering, or is likely to suffer significant harm, it shall make such enquiries as it considers necessary to enable it to decide whether it should take any action to safeguard or promote the child's welfare. As with s.27, Housing, Health, PCTs and NHS Trusts have a duty to assist the Local Authority with its enquiries under s.47 unless to do so would be "unreasonable in all the circumstances."

9.5.2 Education Act 1996

Section 13- enables a Local Education Authority (so far as their powers enable them to do so) to contribute towards the spiritual, moral, mental and physical development of the community by securing that efficient primary and secondary education are available to meet the needs of the population of their area. As an example, details of the number of children in the Local Authority's area and an analysis of their needs would be required in order to fulfil this duty.

9.6 Local Government Act

Section 111(1) - provides that a Local Authority "shall have power to take actions which is calculated to facilitate, or is conducive or incidental to, the discharge of any of their statutory functions".

Section 2(1) - empowers Local Authorities, amongst other things, to do anything which they consider is likely to promote or improve the social well-being of their area, provided it is not prohibited by other legislation. Section 2 is of particular relevance as it is designed to ensure that service delivery is co-ordinated in ways which minimise duplication and maximise effectiveness. Section 2(5) makes it clear that a Local Authority may do anything for the benefit of a person outside their area if it achieves one of the objects of section 2(1).

10- Sharing Information with Carers and Families

Effective information sharing between mental health professionals and carers can greatly improve the level of care a patient receives. As a result, carers feel less isolated and are able to adopt a more supportive and proactive role in the patient's life. This is important, as the carer often knows the patient best and is the only constant support in a patient's life; so at times of sudden crises, they are usually the first to respond. However, issues around information sharing and confidentiality are often convoluted, creating barriers to effective treatment.

For example, determining what information is sharable can be difficult due to the sensitive nature of mental health problems, coupled with the ethical and legal obligations to confidentiality binding all healthcare professionals. Barriers also arise when a patient is unable to or refuses to give 'informed consent' to information sharing, even when the patient-carer relationship is good.

These barriers are not insurmountable. If a patient does continue to withhold consent, carers can still be given sufficient knowledge to enable them to provide effective care. For example, carers can be given: opportunities to discuss any difficulties, general information about mental illness and emotional and practical support.

Furthermore, by discussing the issue of confidentiality with patients at an early stage- when they are not acutely ill or incapacitated, and by prominently recording any issues discussed- the confusion and complexities of information sharing can be somewhat alleviated. For example, a simple conversation with a patient outlining the benefits of information sharing can increase their level of compliance with initiatives.

Information sharing is an important part of patient treatment, especially where carers are involved. However, many factors lead to the breakdown of communication between carers and healthcare professionals. But a mutually beneficial relationship between all those involved with the care of people with mental health problems can develop through proactive, thoughtful and well planned engagement.

The Trust is committed to finding the right balance between providing relevant information to families and carers to enable them to support the patient while respecting patients' and carers' confidentiality. In order to strike the balance right, care professionals need to understand patients' wishes in relation to sharing their information. Staff should refer to the guidance leaflet on sharing information with carers and families entitled "The Right Balance" at the following link: http://sites.intranet.slam.nhs.uk/ICT/Services/TeamPortfolio/informationgovernance/confidentiality/Information%20Governance%20Document%20Library/Carers_families_Leaflet%20130515.pdf

11- Organisations covered by this policy

This policy has been developed to meet the information security and confidentiality requirements for sharing personal identifiable information across organisations in the area covered by the South London and Maudsley NHS Foundation Trust (SLaM).

Organisations involved in sharing of information include NHS England, Health and Social Care Information Centre, NHS Trusts (including Acute, Ambulance, Mental Health), primary care providers, commissioning bodies, higher education institutions,

Local Authorities, the Police, Probation Services, Prosecution Service, voluntary and independent providers.

12- Sharing of Routine Information

A routine disclosure of personal information is one that happens as a matter of course and is relevant to the direct care of the individual. For example:

- A multi-professional ward round
- A Health Visitor discussing a family's circumstances with their G.P.
- A routine referral to another service
- Treatment under the supervision of a probation officer as a condition of a court order.
- Transfer of care-related information between the NHS, the Police and the Crown Prosecution Service

Professionals in partner organisations are regularly asked to provide information about their service users in these or similar situations. Before they do so, they must: -

- Ensure that there is a justifiable need to know on the part of the recipient of the information
- Consider whether it is possible or appropriate to anonymise or pseudonymise the information and, if so do so.
- Seek service user's consent to such disclosure in accordance with this Policy and the guidance set out in the Trust Confidentiality Policy unless the information is required by a care professional for direct provision of care.
- Keep disclosures to a minimum.

Express consent will not be needed where the information is being shared with care professionals for the purpose of direct provision of care and treatment. Health and social care professionals should be able to rely on 'implied consent' when sharing personal confidential data in the interests of direct care, as long as the patient does not object, or has not already done so. Service users must however, be told in general terms the purpose for which their information may be used, in order for the processing to be fair.

The need to share some information does not entail the sharing of everything; only relevant information about a service user should be shared between professionals in support of their care. Consent should be obtained before sharing a patient's whole care record.

13- Sharing of Non-Routine Information

A non-routine disclosure of personal information might be to the Police or a Government Department such as:

- Police requesting information for the investigation of serious crime.
- A regulatory body is requesting information for the investigation of a serious clinical incident like homicide.
- Serious case reviews (child death) organised by the Local Children Safeguarding Board (LCSB)

The person requesting information from another organisation must submit the request in writing to the Data Protection Office.

There may be exceptional circumstances, when emergency services like the Police require Trust staff to share information urgently. Staff should refer to the guidance in Appendix B.

14- Onward Transmission of Personal Data

The Trust retains ownership of the information that is disclosed and any recipient will have a duty of confidence and must not disclose it without the permission of the Trust, or use it for a purpose other than what was originally expressed. In considering whether to authorise wider disclosure, the Trust will ensure to gain the consent of the service user.

The Trust ICT Security Policy outlines appropriate security for the safe and secure inbound and outbound transfer of information.

15- Complaints

A complaint from a data subject or their representative about information held under the terms of this policy will be investigated by the organisation receiving the complaint.

16- Secure Transfer of Personal Confidential Information

Staff should always use secure electronic means to transfer personal confidential data. Such secure electronic means include slam.nhs.uk email for low profile and individual records, nhs.net for high profile individual cases and information about a number of service users.

Secure electronic transfer tool is available to all staff, which enables secure electronic transmission of confidential documents to recipients outside the Trust regardless of their security arrangements. This facility is available at the following link with useful instructions:

http://sites.intranet.slam.nhs.uk/ICT/help/selfservice/Shared%20Documents/Secure%20File%20Transfer.aspx

More detail on secure transfer of personal confidential information is provided in the ICT Security Policy.

Transfers of personal identifiable information both to and from third party organisations are subject to strict governance and technical security controls. All staff intending to undertake large volumes of (20 individuals or more) in-bound or out-bound personal confidential data transfers must contact the Information Governance Office to seek advice and register proposed information flows in or out of the organisation.

Staff will be required to provide details of the information to be transferred, which will include:

a) what information is to be transferred
b) number of records,
c) purpose of transfer,
d) nature of recipient,
e) method of transfer,

f) physical and technical security measures proposed by the sender and the recipient,
g) any processing that the third party may carry out.

Based on the details provided, the Information Governance Office will advise on necessary safeguards for the security of the personal information transfer, register the transfer to have a local record of what information is transferred and relevant safeguards agreed to maintain information security and patient confidentiality.

Third parties who receive Trust data for a specific purpose may be required to sign up to a Purpose Specific Information Sharing or Processing Agreement. When such requirements for purpose specific agreements arise, these agreements need to be reviewed by the Information Governance Office and will be signed off by the Caldicott Guardian.

17- Incidents involving breaches of Confidentiality and Information Security

Any incident that involves intentional or unintentional inappropriate disclosure of patient and staff information (on paper or electronic format) outside the legal framework of the Data Protection Act, the Caldicott Guidelines and this Policy, must be reported using Datixweb. It is the responsibility of the service where the incident took place to complete the incident form. Reported incidents will be investigated according to the Trust Incident Risk, Incident Management and Forensic Readiness Policy.

Information incidents will be reviewed by the Head of Information Governance and will be regularly reported to the Caldicott Committee using the classification endorsed by the Health and Social Care Information Centre.

18- Training

All Trust staff must attend the compulsory induction training when they start their employment with the Trust. During the induction training, all staff attend Confidentiality and Information Security Induction Session. This training is also available to existing staff upon request. All in-service training requests should be sent to the Data Protection Office.

In addition to classroom training, the Trust provides on-line e-learning resources to all Trust staff.

The e-learning programme can be accessed at the following link:

http://www.igte-learning.connectingforhealth.nhs.uk/igte/index.cfm

It is the duty of line managers to ensure that all staff can demonstrate that they have had the relevant confidentiality training during appraisals. Line managers should signpost staff to other resources that will enable them to improve confidentiality and information security awareness. Such resources include information leaflets, posters, guidance documents, procedures and intranet resources, which can be obtained by contacting the Data Protection Office.

19- Further Information

For further information on confidentiality and data protection, staff can refer to the Confidentiality site on the Trust intranet. Confidentiality intranet site can be accessed at this link:
http://sites.intranet.slam.nhs.uk/ICT/Services/TeamPortfolio/informationgovernance/confidentiality/default.aspx

Information Governace Office provides advice and support for staff as and when required.

Information Governance Office
CR2 – Clinical Records
Maudsley Hospital
Denmark Hill
London SE5 8AZ
Tel: 020 3228 5174
Fax: 020 3228 3132
e-mail: dataprotectionoffice@slam.nhs.uk

The Information Commissioner's Office is the independent authority set up to promote access to official information and protect personal information. Further information and help can be found at their website:
http://www.ico.gov.uk/

20- Links to other Trust Policies

The issues covered in this Policy have relevant interactions with other areas covered by the following Trust Policies and must be read in conjunction:

- Confidentiality Policy
- ICT Security Policy
- Information Governance Policy
- Information Governance Communications Plan
- Information Governance Strategy
- Clinical Records Policy
- Safeguarding Children Policy and Procedures
- Protecting Children and the Public – Working with MAPPA Arrangements
- Safeguarding Adults Policy
- Policy for Giving Information to Detained Patients and Their Relatives (Section 135)
- Mental Capacity Act Policy
- Information Risk, Incident and Forensic Readiness Policy
- HR Data Protection Policy for Employees' Personal Records
- Risk Management and Assurance Strategy

21- Monitoring Compliance and Effectiveness of this Policy

The compliance with the Information Sharing Policy is monitored by the Head of Information Governance and overseen by the Caldicott Committee.

The DH Information Governance Toolkit and the annual Information Governance Assurance Programme is a programme of internal and independent audits led by the Head of Information Governance. The programme reviews compliance with Trust

information governance policies (including the Information Sharing Policy) and national NHS confidentiality, data protection and information governance standards. The progress on the recommended actions is monitored by the Caldicott Committee.

The Trust Executive receives regular updates on the Information Governance Assurance Programme and monitors Trust compliance with the Information Governance Toolkit.

The Caldicott Annual Report features Trust compliance with Caldicott Principles, the Data Protection Act and this Policy and is presented to the Trust Board by the Caldicott Guardian. The report is made public through the Trust Publication Scheme.

All information risks related to clinical information are identified by the Caldicott Committee and the ICT Security Committee. The identified risks are reviewed by the Caldicott Guardian, Head of ICT, Head of Information Governance and reviewed regularly by the Risk Management Committee for their likelihood and impact.

All incidents that involve loss of patient information, medical records, loss of ICT equipment, inappropriate access to medical records, intentional or unintentional disclosure of patient identifiable information that breaches this Policy are reviewed and regularly reported to the Caldicott Committee by the Head of Information Governance. The Caldicott Guardian receives regular updates on actions plans from the Head of Information Governance. Serious incidents that fall under NHS Connecting for Health Category 3 and above are reported externally to Monitor, Connecting for Health and the Information Commissioner's Office.

Responses to information governance complaints are monitored for quality by the Caldicott Guardian.

What will be monitored i.e. measurable policy objective	**Method of Monitoring**	**Monitoring frequency**	**Position responsible for performing the monitoring/ performing co-ordinating**	**Group(s)/committee (s) monitoring is reported to, inc responsibility for action plans and changes in practice as a result**
Information governance compliance	Information Governance Toolkit and the Independent IG Review	Annual (with quarterly updates)	Head of Information Governance	Caldicott (for IGM, CDP, Clinical Records), ICT Security (for Information Security and SU) and FoI (for Corporate Records) Committees
Confidentiality, information sharing, Data Protection Act (1998),	IG Assurance Programme	Annual	Head of Information Governance	Caldicott Committee (and ICT Security Committee for technical aspects)
Confidentiality, information sharing, Data Protection Act (1998) incidents	Data breach incident reports and quarterly	Quarterly	Head of Information Governance	Caldicott Committee (and ICT Security Committee for technical incidents)

What will be monitored i.e. measurable policy objective	Method of Monitoring	Monitoring frequency	Position responsible for performing the monitoring/ performing co-ordinating	Group(s)/committee (s) monitoring is reported to, inc responsibility for action plans and changes in practice as a result
	lesson learned report			
Health records management and data quality	Health Records Review	Annual	Clinical Systems Manager	Caldicott Committee
ICT Security	Computer Audit Programme	Annual	ICT Compliance Manger	ICT Security Committee
Data Quality	Health Intelligence and Performance Management	Monthly	Head of Performance and Head of HI	Chief Executive's Performance Management Review process

22- Freedom of Information Act 2000

All Trust policies are public documents. They will be listed on the Trusts FOI document schedule and may be requested by any member of the public under the Freedom of Information Act (2000).

23- References

This document has been prepared in reference to the documents listed below. The documents listed below should be referred for detailed information.

1. Department of Health (2013): Information: To Share or Not To Share. The Information Governance (Caldicott 2) Review
2. Health and Social Care Information Centre (2013): Checklist Guidance for Reporting, Managing and Investigating Information Governance Serious Incidents Requiring Investigation
3. Department of Health (2003) Confidentiality: NHS Code of Practice. London: Department of Health
4. HMSO (1998) Data Protection Act 1998
5. HMSO (1998) Human Rights Act 1998
6. HMSO (2007) Mental Health Act 2007
7. HMSO (2005) Mental Capacity Act 2005
8. HMSO (1989) Children Act 1989
9. HMSO (2006) National Health Service Act 2006
10. HMSO (2012) Health and Social Care Act (2012)
11. HMSO (1998) Crime and Disorder Act 1998

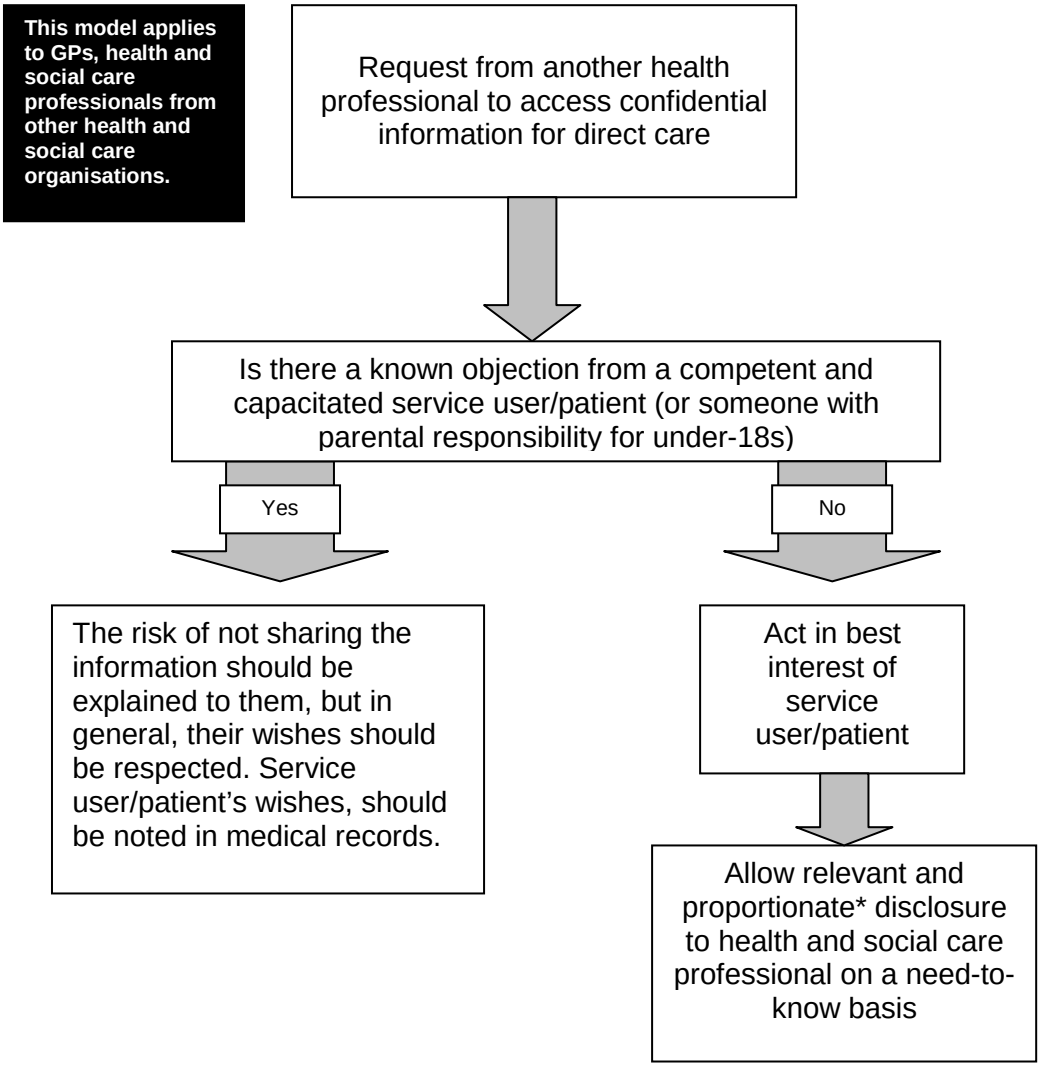
12. HMSO (2003) Criminal Justice Act 2003
13. HMSO (2000) The Criminal Justice and Court Services Act 2000
14. Home Office (2003) MAPPA guidance
15. HM Government (2006) What to do if you're worried a child is being abused – Every Child Matters
16. Department for Constitutional Affairs (2007) Mental Capacity Act 2005: Code of Practice. London: Department for Constitutional Affairs

24- Appendices

South London and Maudsley NHS
NHS Foundation Trust

APPENDIX A- DISCLOSURE MODELS

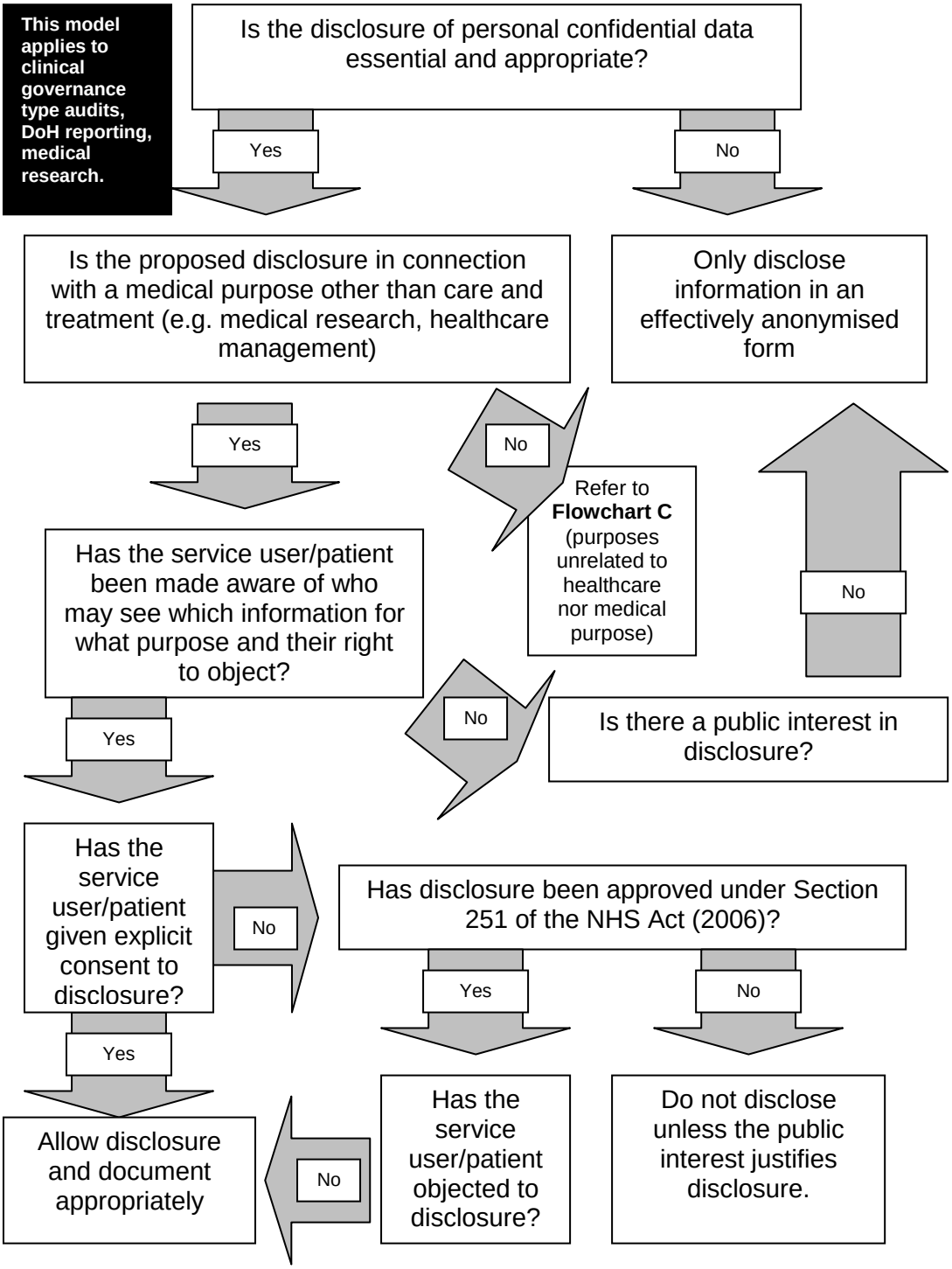
A. Disclosure of personal confidential information to another health and social care professional for direct provision of care:



*** Duty to share information with other health and social care professionals should be based on implied consent so that patients receive best possible care applies to sharing of information proportionate to the need (minimum information that is required). Disclosure of full medical records require patients' explicit consent.**

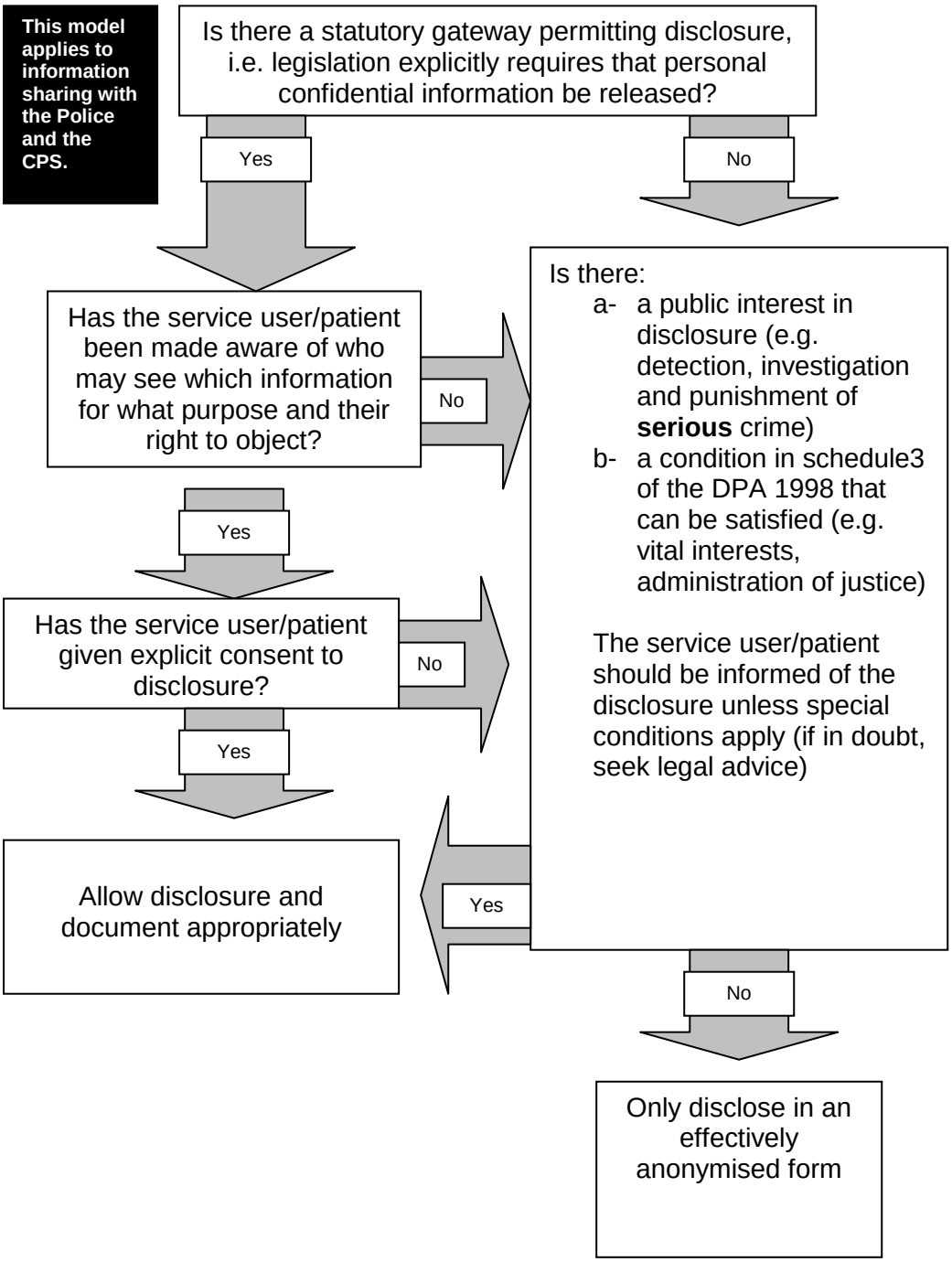
If in doubt, contact the Information Governance Office

B. Disclosure of personal confidential information for purposes not related to healthcare but another medical purpose as defined in the legislation (e.g. medical research, healthcare management):



If in doubt, contact the Information Governance Office

C. Disclosure of personal confidential information for purposes not related to healthcare nor another medical purpose:



If in doubt, contact the Information Governance Office

APPENDIX B – GUIDANCE FOR EFFECTIVE EXCHANGE OF INFORMATION WITH THE POLICE

The purpose of this guide is to outline the procedure for effective information flow between the Trust and the Police without jeopardising patient confidentiality.

The information disclosed to the recipient is disclosed in confidence and for the use of the recipient organisation only. Unless otherwise stated, there should no onward disclosure of information.

Trust staff: this section must not be read in isolation from the full the Trust Information Sharing Policy and is intended to be a practical, day-to-day guide.

PART A) REQUESTS TO THE TRUST

1- Initial contact by the Metropolitan Police Service should be made to:

Routine requests
8am - 5pm (Monday to Friday)
Data Protection Office (DPO) Tel: 020 3228 5174 Fax: 020 3228 3132 dataprotectionoffice@slam.nhs.uk
Weekends and Bank Holidays
The next working day to the Data Protection Office.

Urgent requests - Police Custody Officer/Nurses (IMMEDIATE ATTENTION)	
24 hours a day, 7 days a week	
Lewisham Tel: 0208 333 3030 ext 8423 and then ask for the Psychiatric Liaison Nurse	**Croydon** Croydon Psychiatric Liaison Team: Tel: 0203 228 0809 If no answer, call the Mayday Hospital on: 0208 401 3000 and ask for Bleep 714
Lambeth Tel: 0203 228 6000 and then ask for the Duty Senior Nurse for Lambeth **Southwark** Tel: 0203 228 6000 and then ask for the Emergency Team Leader for Southwark	

Urgency of requests:

a) Routine enquiries: All enquiries that relate to historic information about patients will be considered 'routine' and will be processed within working hours within a reasonable timeframe.

b) Urgent enquiries (often by Police Custody officers/Custody Nurses):

This document acknowledges that nurses are further duty-bound by confidentiality through the terms of their professional code of conduct.
A Custody Nurse may require information to assist in:

1) Managing the care and treatment of prisoners while being held in police detention.
2) Making a pre-release assessment.
3) Making arrangements for further support by mental health services after release.

The Police Officer or Custody Nurse making the request will supply the following information:

By telephone **or** using an appropriate e-mail address (if not urgent)	
About themselves	Name, job title and telephone number
About the subject they are enquiring about	• The name and date of birth • What information is required • Why it is required (indicating any relevant immediate risk of harm/death or statutory reason)
For routine and urgent requests:	• Confirm if they have capacity to provide consent. • Confirm if the person has given their consent to obtain disclosure (even if consent is not given, information may still be given)

2- Trust Response

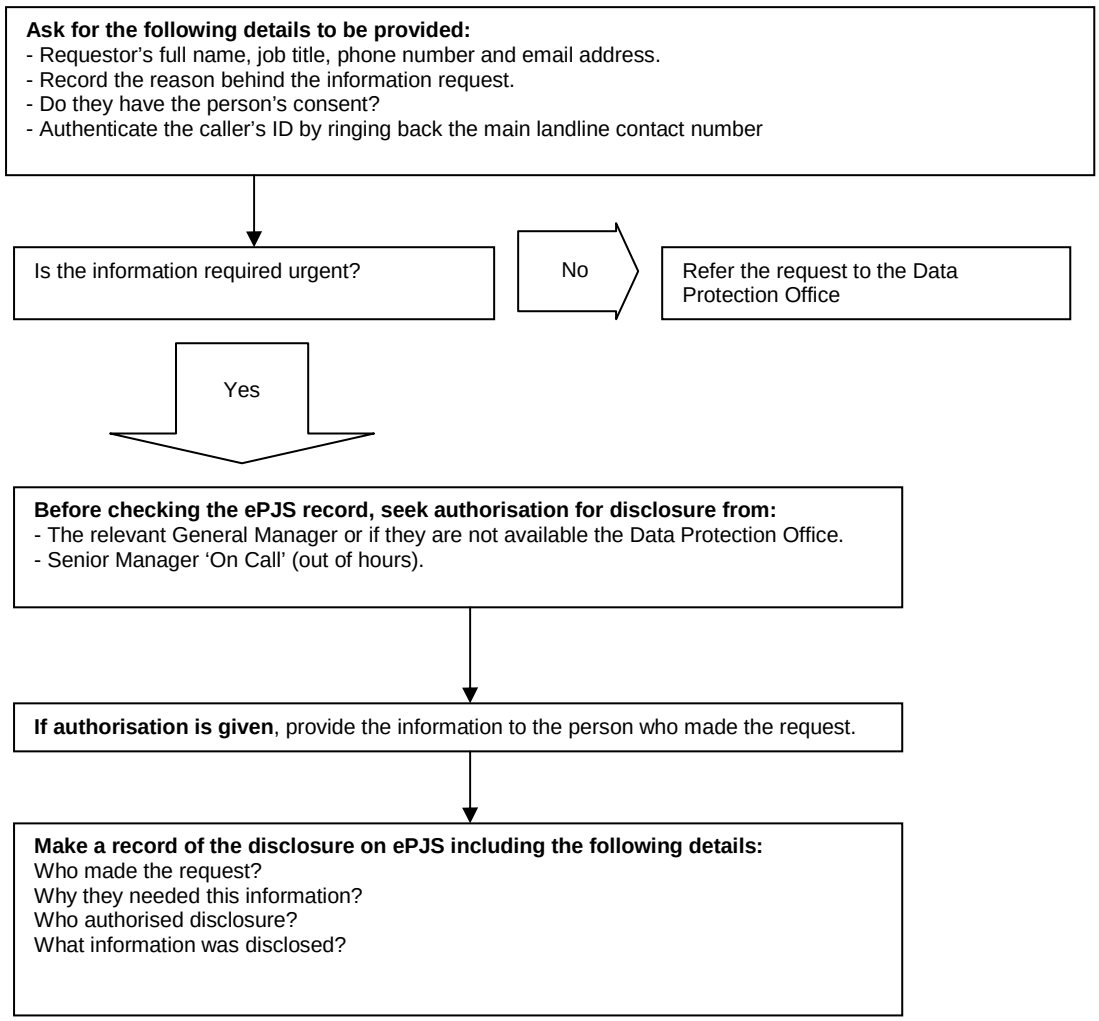
SLaM staff under the terms of this arrangement may disclose **ONLY** the following information:

- Whether they are known to SLaM Trust.
- Whether they are currently engaged with services.
- Known risk factors - to self or others.
- Diagnosis or nature of mental health problem.
- Recent significant life changes that can be established from patient records that may impact on behaviour.

3- Trust staff will keep a written record:

Trust staff will file a copy of the information exchange on ePJS under the 'Events' tab, indicating what information was provided, when, why and to whom.

4- Summary of General Principles for <u>Routine and Urgent Enquiries</u>:



PART B) REQUESTS TO THE METROPOLITAN POLICE

1- Initial contact by a SENIOR member of the SLaM Trust should be made to:

<table>
<tr><th colspan="2">8am - 5pm (Monday to Friday)</th></tr>
<tr><td><u>Lewisham's BMHLO</u>
Insp Tim Evans
Tel: 020 8284 7969
Email: tim.a.evans@met.police.uk
Team: Partnership Team</td><td><u>Croydon's BMHLO</u>
Inspector Jacqui Nicholas
Tel: 0208 649 0288
Email: Jacqueline.Nicholas@met.police.uk

OR

Police Constable Linda Allen
Tel: 0208 649 0288
Email: Linda.Allen@met.police.uk
Team: Community Liaison Office</td></tr>
<tr><td><u>Bromley's BMHLO</u>
Inspector Tony Nickalls
Tel: 07920 207 120 or 020 8284 8901
Email: Anthony.Nickalls2@met.police.uk
Team: Kelsey & Eden Park SNT</td><td><u>Southwark's BMHLO</u>
Sergeant Justin Davis
Tel: 020 7232 6691
Team: Operations MD (Events & Mental Health)
Email: md-mentalhealth@met.pnn.police.uk</td></tr>
<tr><td><u>Lambeth's BMHLO</u>
Inspector Peter O'Donnell
Tel: 020 8649 2053
Email: Peter.O'Donnell2@met.police.uk
Team: tbc</td><td></td></tr>
<tr><th colspan="2">Weekends and Bank Holidays</th></tr>
<tr><td colspan="2">The next working day for the relevant BMHLO.</td></tr>
</table>

2- The person making the request will supply the following information:

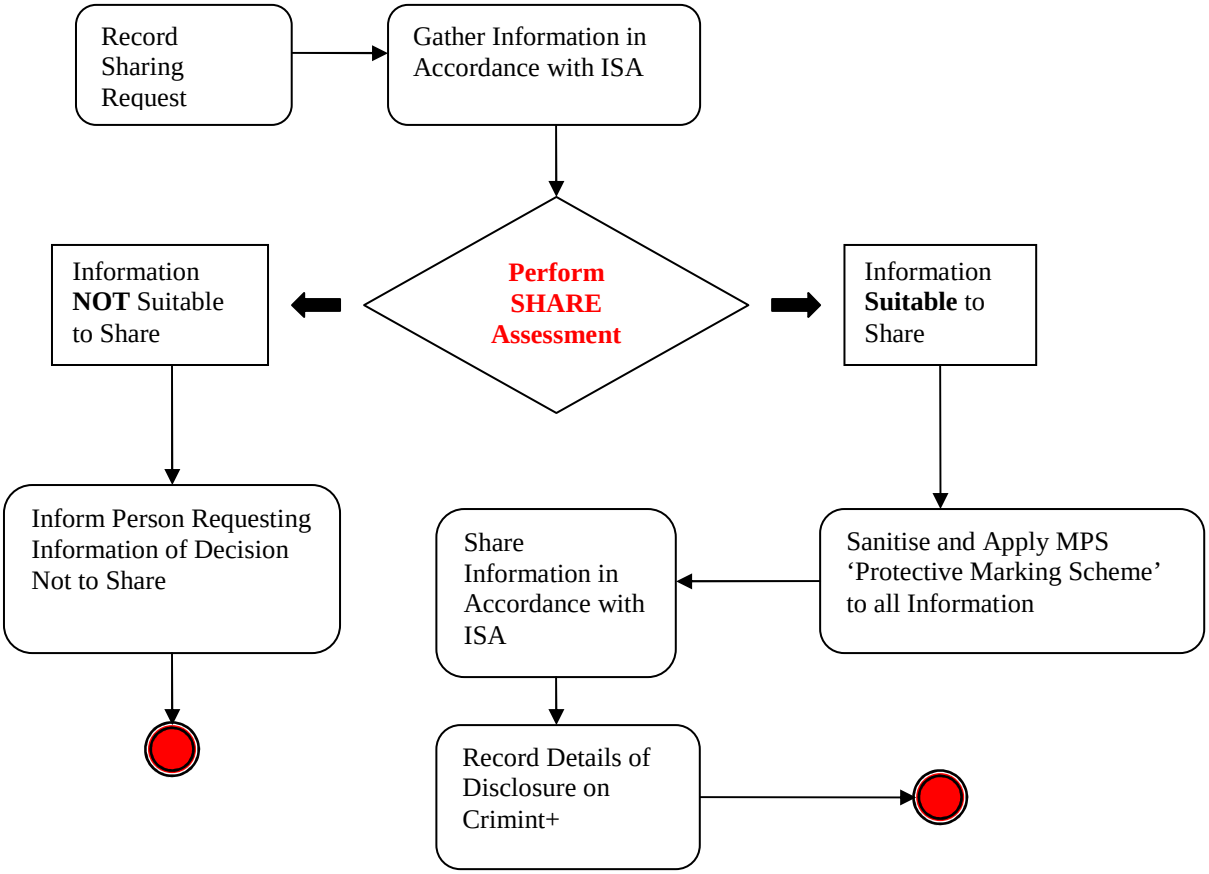
<table>
<tr><td colspan="2">In writing on headed paper or using an appropriate e-mail address or by telephone</td></tr>
<tr><td>About the subject they are enquiring about</td><td>• Name and date of birth?
• What information is required?
• Why is it required? (indicating any relevant immediate risk of harm/death or statutory reason)</td></tr>
<tr><td>About themselves</td><td>Name, job title and telephone number</td></tr>
</table>

3- The Police will keep a written record:

The Police may respond to information requests via MPS Form 141A.

If you are sharing information, you must create a Crimint+ Information Report as soon as possible after the sharing has taken place.

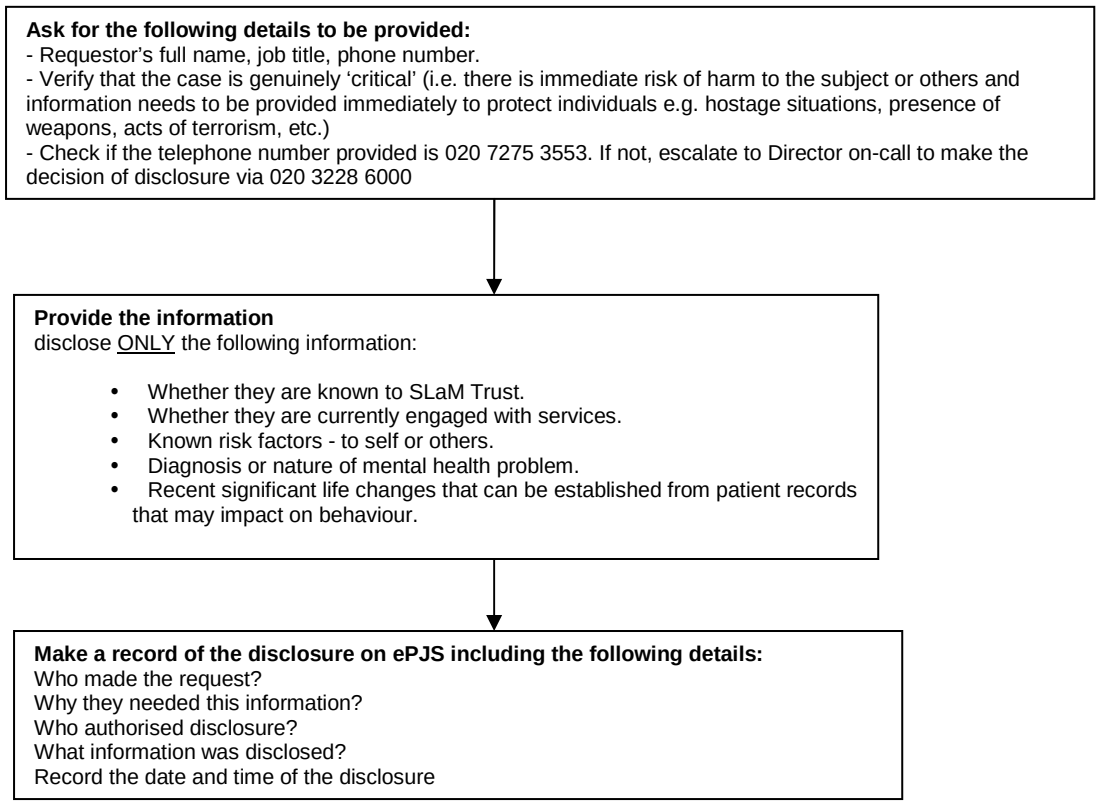
4- Police overview of sharing process following a disclosure request



Summary of General Principles for Critical Enquiries:

Critical requests (IMMEDIATE RESPONSE)
All Boroughs Tel: 0203 228 6000 and then ask for the Duty Senior Nurse for Lambeth
As a last resort contact the 'on call' Director via the switchboard on Tel: 0203 228 6000

c) Critical enquiries: A case will be considered 'critical' if there is immediate risk of harm to the subject or others and information needs to be provided immediately to protect individuals e.g. hostage situations, presence of weapons, acts of terrorism, etc.
Critical Enquiries will only be generated by scene of crime Firearms Officers.



APPENDIX C - EQUALITY IMPACT ASSESSMENT

South London and Maudsley NHS
NHS Foundation Trust

1. Name of the policy / function / service development being assessed?
Information Sharing Policy

2. Name of person responsible for carrying out the assessment?
Murat Soncul

3. Describe the main aim, objective and intended outcomes of the policy / function / service development?

Aim:
The aim of the Information Sharing Policy is to provide guidelines to ensure that sensitive clinical information is shared between the Trust and its partner agencies to facilitate the provision of seamless care in a secure and confidential manner and in accordance with the law.

Objective:
The main objective is to set out the obligations on staff in the Trust and partner agencies, including social services, other NHS Trusts, the Police etc. and other agencies that work with the Trust to ensure seamless information flow whilst maintaining service user confidentiality.

Intended outcomes:
- Confidential service user information is shared for justified purposes with organisations with legitimate reason to access such information
- Such information is only shared when absolutely necessary
- Minimum information is shared
- Access to such information should be on a 'need to know' basis
- All staff should understand their responsibilities
- All staff should understand and comply with relevant legislation

4. Is there reason to believe that the policy ~~/ function / service development~~ could have a negative impact on a group or groups?

No, sharing information with partner organisations with the consent of the service user whilst maintaining service user confidentiality is a key requirement and is an expectation of all service users.

Which equality groups may be disadvantaged / experience negative impact?

Race	NO
Disability	NO
Gender	NO
Age	NO
Sexual orientation	NO
Religion / belief	NO

5. What evidence do you have and how has this been collected?

None

Some

Substantial

6. Have you explained your policy ~~/ function / service development~~ to people who might be affected by it?

Yes

If 'yes' please give details of those involved

This is a revised policy that has been updated to keep it in line with national standards and the data protection legislation. The policy was consulted with CAGs and service user representatives via the Caldicott Committee

7. If the policy ~~/ function / service development~~ positively promotes equality please explain how?

N/A

8. From the screening process do you consider the policy / function / service development will have a positive or negative impact on equality groups? Please rate the level of impact and summarise the reason for your decision.

Positive: promote opportunity relations)	High (highly likely to promote equality of opportunity and good relations)	Medium (moderately likely to promote equality of opportunity and good relations)	Low (unlikely to equality of and good
Negative: not negative impact)	High (highly likely to have a negative impact)	Medium (moderately likely to have a negative impact)	Low (probably will have a

Neutral: **High (highly likely)**

Reason for your decision:

This is a revised policy to provide best practice guidance to staff in relation to the Data Protection Act (1998) and has been updated as part of regular policy review process. There is no direct impact on equality and diversity issues from this policy.

Date completed: 01/07/2013

Signed …… Print name Murat Soncul

APPENDIX D: HUMAN RIGHTS ACT IMPACT ASSESSMENT

To be completed and attached to any procedural document when submitted to an appropriate committee for consideration and approval. If any potential infringements of Human Rights are identified, i.e. by answering Yes to any of the sections below, note them in the Comments box and then refer the documents to SLaM Legal Services for further review.

For advice in completing the Assessment please contact Paul Bellerby, Legal Services [paul.bellerby@slam.NHS.co.uk]

HRA Act 1998 Impact Assessment	Yes/No	If Yes, add relevant comments
The Human Rights Act allows for the following relevant rights listed below. Does the policy/guidance NEGATIVELY affect any of these rights?		
Article 2 - Right to Life [Resuscitation /experimental treatments, care of at risk patients]	No	
• Article 3 - Freedom from torture, inhumane or degrading treatment or punishment [physical & mental wellbeing - potentially this could apply to some forms of treatment or patient management]	No	
• Article 5 – Right to Liberty and security of persons i.e. freedom from detention unless justified in law e.g. detained under the Mental Health Act [Safeguarding issues]	No	
• Article 6 – Right to a Fair Trial, public hearing before an independent and impartial tribunal within a reasonable time [complaints/grievances]	No	
• Article 8 – Respect for Private and Family Life, home and correspondence / all other communications [right to choose, right to bodily integrity i.e. consent to treatment, Restrictions on visitors, Disclosure issues]	No	
• Article 9 - Freedom of thought, conscience and religion [Drugging patients, Religious and language issues]	No	
• Article 10 - Freedom of expression and to receive and impart information and ideas without interference. [withholding information]	No	
• Article 11 - Freedom of assembly and association	No	
• Article 14 - Freedom from all discrimination	No	

Name of person completing the Initial HRA Assessment:	ICT Compliance Manager
Date:	17/06/2013
Person in Legal Services completing the further HRA Assessment (if required):	n/a
Date:	n/a

APPENDIX E – CHECKLIST FOR THE REVIEW AND APPROVAL OF A POLICY

This checklist must be used for self-assessment at the policy writing stage by policy leads and be completed prior to submission to an appropriate Executive Committee/Group for ratification.

	Title of document being reviewed:	Yes/No/ Unsure	Comments
1.	**Style and Format**		
	Does the document follow The South London and Maudsley NHS Foundation Trust Style Guidelines? i.e.: • The Trust logo is in the top left corner of the front page only and in a standard size and position as described on the Intranet • Front page footer contains the statement about Trust copyright in Arial 10pt • Document is written in Arial font, size 11pt (or 12pt) • Headings are all numbered • Headings for policy sections are in bold and not underlined • Pages are numbered in the format Page X of Y	Y	
2.	**Title**		
	Is the title clear and unambiguous?	Y	
3.	**Document History**		
	Is the document history completed?	Y	
4.	**Definitions**		
	Are all terms which could be unclear defined?	Y	
5.	**Policy specific content**		
	Does the policy address, as a minimum, the NHSLA Risk management Standards at Level 1 where appropriate	N/A	
6.	**Consultation and Approval**		
	Has the document been consulted upon?	Y	
	Where required has the joint Human Resources/staff side committee (or equivalent) approved the document?	N/A	
7.	**Dissemination**		

	Title of document being reviewed:	Yes/No/ Unsure	Comments
	Does the document include a plan for dissemination of the policy?	Y	
8.	**Process for Monitoring Compliance**		
	Is it explicit how compliance with the policy will be monitored?	Y	
9.	**Review Date**		
	Is the review date identified on the cover of the document?	Y	
10.	**References**		
	Are supporting references cited?	N/A	
11.	**Associated documents**		
	Are associated SLaM documents cited?	Y	
12.	**Impact Assessments**		

APPENDIX F-INFORMATION SHARING FORM

South London and Maudsley NHS
NHS Foundation Trust

Request for Information

This form must be used when requesting disclosure of personal information without the consent of the individual.

Please print clearly using black ink. Illegible forms will be returned.

The requestor should complete section 1 of this form and send it to:
Data Protection Office
CR2-Clinical Records, Maudsley Hospital, Denmark Hill, London SE5 8AZ
Fax: 020 3228 3132
e-mail: dataprotectionoffice@slam.nhs.uk

SECTION 1- to be completed by the requestor			
Request from			
Name of Requestor		Organisation	
Job Title		Telephone	
Date of request		PRIORITY	☐Critical ☐Urgent ☐Routine
Patient Details			
Surname		Address (if known)	
Forename			
Date of birth		Other relevant identifiers (if appl.)	

Purpose of the disclosure request	
Purpose for which the information is requested:	
Legal basis for request (specific statute or exemption of the DPA):	SECTION ___ of the _____ Act
Reasons for disclosure without consent:	

Information required

Declaration
I confirm that the above information is required for the purposes stated. Any obligations arising from the Data Protection Ac 1998, Article 8 of the Human Rights Act 1998 or any Common Law Duty of Confidentiality will be observed. The information will not be used for any purpose other than that for which it is being requested and will not be further disclosed to any unauthorised person. It will be kept securely and where necessary, disposed of correctly in accordance with the relevant retention schedule.

Print Name		**Signature**		**Date**	

Record of Disclosure

This form must be used when disclosing personal information without the consent of the individual.

Please print clearly using black ink.

For Data Protection Office Use				
Caldicott Guardian Approval ☐ **full disclosure** ☐ **limited disclosure** ☐ **non-disclosure**				**Caldicott Guardian's Comments**
Signed		**Dated**		

SECTION 2 – to be completed by the Trust staff disclosing the information Trust staff must only provide information for requests approved by the Caldicott Guardian			
Request received by			
Name of Trust staff		Team	
Job title		Directorate	
Date received		Telephone	
Patient Details			
Surname		Address (if known)	
Forename			
Date of birth		Other relevant identifiers (if appl.)	

Information disclosed	
State reasons for sharing information without patient consent or after consent was refused:	
Means of disclosure:	
Details of any differences between request and disclosure:	
Reasons for refusal / limited disclosure:	

Declaration			
I confirm that to my knowledge, the above information is a true record of the information as held by the Trust, that it was obtained fairly and lawfully, and that I am authorised to make the disclosure as detailed above.			
Signed		**Date**	