South London and Maudsley NHS
NHS Foundation Trust

Confidentiality Policy

Version:	8.1
Ratified By:	Clinical Policy Working Group
Date Ratified:	3rd October 2017
Date Policy Comes Into Effect:	3rd October 2017
Author:	Head of Information Governance
Responsible Director:	Caldicott Guardian
Responsible Committee:	Caldicott Committee
Responsible Committee Approval Date:	22nd September 2017
Target Audience:	All Staff (permanent and temporary) and contractors
Review Date:	18th August 2019

Equality Impact Assessment	Assessor: Deputy IG Lead	Date:18/09/17
HRA Impact Assessment	Assessor: Deputy IG Lead	Date: 18/09/17

This policy document is subject to South London and Maudsley copyright. Unless expressly indicated on the material contrary, it may be reproduced free of charge in any format or medium, provided it is reproduced accurately and not used in a misleading manner or sold for profit. Where this document is republished or copied to others, you must identify the source of the material and acknowledge the copyright status

Document History

Version Control

Version No.	Date	Summary of Changes	Major (must go to an exec meeting) or minor changes	Author
2	May 2007	Policy updated	Minor	Information Governance Manager
3	February 2008	Policy rewritten	Major	Information Governance Manager
4	April 2010	Policy updated	Minor	Head of Information Governance
5	July 2011	Policy updated	Minor	Head of Information Governance
6	July 2013	Policy updated	Major	Head of Information Governance
6.1	October 2014	Section on Family and Carers revised	Minor	Head of Information Governance
7	August 2015	Updated definitions	Minor	Head of Information Governance
8	September 2017	Policy updated to include New General Data Protection Regulation, updates to include Leap for access to training.	Minor	Deputy Information Governance Lead
8.1	September 2017	Inclusion of confidentiality on gender identity and updates made to Equalities Impact Assessment	Minor	Deputy Information Governance Lead

Consultation

Stakeholder/Committee/ Group Consulted	Date	Changes Made as a Result of Consultation
Caldicott Committee	10/07/2013	Updates arising from the National IG Review
Caldicott Committee	01/10/2014	Updated section on Family and Carers
Caldicott Committee	15/07/2015	Updated definitions
Caldicott Committee and Equality Manager	18/09/17	Updated definitions. Updated to include the New Data Protection Legislation (GDPR) and confidentilaty relating to gender identity, with link to guidance on supporting Adults transgender service users

Plan for Dissemination of Policy

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

Plan for Implementation of Policy

Details on Implementation	Person Responsible
Upholding confidentiality	All staff
Breach of Confidentiality	Caldicott Guardian
Data security	Chief Information Officer

Contents

1 Policy Summary

1.1. South London and Maudsley NHS Foundation Trust (SLaM) is committed to the delivery of a first class confidential service that follows Caldicott principles. All staff must ensure that all service user information is processed fairly, lawfully and as transparently as possible.

1.2. All Trust staff have responsibility to meet the confidentiality standards outlined in this policy in accordance with the standard terms and conditions of their employment.

1.3. Any breach of this Policy would jeopardise the confidentiality of service users and the security of clinical information, and would breach the Data Protection Act (1998). Breaches will be reported as incidents, which will be investigated by the Information Governance Office and may lead to disciplinary action against staff or heavy penalties against the Trust by the Information Commissioner's Office.

1.4. Confidential information about service users can only be used for healthcare purposes and unless exceptional circumstances are present, can only be disclosed with the informed consent of the service user. Where the service user lacks capacity and unable to consent, information should only be disclosed in the service user's best interests. When in doubt, staff must seek guidance from the Caldicott Guardian.

1.5. The only exceptional areas for disclosure of information when the service user has capacity are when statute law requires us to do so, when there is a court order and when disclosure may be necessary in the public interest.

1.6. Researchers can access clinical information to conduct research only when explicit consent has been obtained from the service user.

1.7. Staff must always consider the safety and welfare of a child or young person when making decisions on whether to share information about them. Where there is concern that the child may be suffering or is at risk of suffering significant harm, the child's safety and welfare must be the overriding consideration. The same sensitivity should be applied to vulnerable adults.

1.8. All requests to access records should be processed following the "Procedures for Trust Staff on How to Deal with Requests of Access to Clinical Records according to the Data Protection Act"

1.9. All Trust staff must attend the compulsory Confidentiality and Information Security Training. This training is available at induction for new staff and via e-learning or as team training to existing staff. All in-service training requests should be sent to the Data Protection Office.

2 Introduction

Service users disclose personal confidential information about themselves relating to their health, social and personal circumstances whilst using Trust services. Confidential details about service users' health contain personal confidential and sensitive information.

Personal confidential data is any piece of information which can potentially be used to uniquely identify, contact, or locate a single person. This information includes:

- Name, address, full post code, date of birth, gender, ethnicity,
- 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

This sensitive personal confidential 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 at all times. Genetic information will not be treated any differently from other forms of personal confidential information.

The duty of confidence that arises following disclosure of sensitive personal confidential information is a legal and professional obligation. This fundamental requirement is established within professional codes of conduct and is also included within Trust employment contracts as a specific requirement linked to disciplinary procedures. It is crucial that the Trust provides a confidential service to meet legal requirements and retain the trust of service users.

Service users' rights in relation to their personal confidential data:

- The right of access to their own personal records within the health and social care system.
- The right to privacy and confidentiality and to expect the health and social care system to keep their confidential information safe and secure.
- The right to be informed about how their information is used.
- The right to request that their confidential data is not used beyond their own care and treatment and to have their objections considered, and where their wishes cannot be followed, to be told the reasons including the legal basis.

Trust's commitment to service users in relation to their personal data:

- to ensure those involved in service users' care and treatment have access to relevant healthcare data so they can provide safe and effective care;
- to anonymise the data collected during the course of care and treatment and use it to support research and improve care for others;
- where identifiable data has to be used, to give service users the chance to object wherever possible;
- to inform service users of research studies in which they may be eligible to participate; and
- to share with service users any correspondence sent between staff about their care.

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.

General Data Protection Regulation: The new General Data Protection Regulation (GDPR) which will be implemented in the UK in May 2018, GDPR requires the trust to apply stricter controls to patient-level data as the data rows get longer and richer even when the data is de-identified.

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.

Data is used to describe 'qualitative or quantitative statements or numbers that are assumed to be factual, and not the product of analysis or interpretation.'

Information is the 'output of some process that summarises interprets or otherwise represents data to convey meaning.'

Carers include the most significant people in the life of the service user, including children and young carers. It is important to clarify with the service user who they consider as their carer. It is important to note that the carer is not always the "nearest relative". The term "nearest relative" is defined in the Mental Health Act.

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.

The Health and Social Care Act 2012 did not make substantive changes to the overarching legal framework for data protection, the common law duty of confidentiality, or human rights requirements. However, it introduced an important legal basis for the Health and Social Care Information Centre to access personal confidential data.

Patient-owned records are less common forms of record that individuals create and manage themselves. They are kept separate from any electronic patient record and the individual has total control and responsibility for the content. Patient-owned records may include extracts from electronic patient records, but may also contain information added by the individual such as exercise monitoring data, weight etc; commercial contributions e.g. from over the counter drug purchases or from supermarket alcohol purchases; and contributions from personally acquired 'medical devices'.

Health and social care records are the most common type of record supported by the information strategy. A professional creates an electronic patient record, which is then shared with the patient and their relevant care teams. The health or social care professional is responsible and accountable for that record when it is for the purpose of direct care. Patients may get right of access, the ability to see, interact and request corrections but not the right to change the content because that might be clinically unsafe. This access is sometimes referred to as 'patient online access' or 'record access'.

Guardian: A person lawfully invested with the power, and charged with the obligation, of taking care of and managing the property and rights of a person who, because of age, understanding, or self-control, is considered incapable of administering his or her own affairs.

4 Purpose of the Policy

The main purpose of service users' medical records is to support the provision of healthcare. Information that can identify individual service users must not be used or disclosed for purposes other than healthcare without the individual's explicit consent. The only exception is when there is some other legal basis, or where there is a public interest consideration or legal justification to do so.

Decisions about the public interest are complex and must take account of both the potential harm that disclosure may cause and the interest of public in the continued provision of confidential health services. In contrast, anonymised information is not confidential and may be used with relatively few constraints.

The purpose of this policy is to outline the principles to maintain confidentiality of personal information provided by service users to receive healthcare service and lay out the few exceptions when duty of confidentiality can be temporarily set aside for the benefit of the service user or other members of public or when there is an applicable legal basis.

All Trust staff has a legal and professional responsibility to meet the confidentiality standards outlined in this policy as an obligation of their terms of employment. These requirements are based on existing codes of conduct, relevant legislation and best practice. This policy aims to outline responsibilities for all Trust staff and provide guidance to ensure service user confidentiality.

It is inevitable that there will be new areas, where organisational processes are not yet in place. There will be need to change many existing procedures with changing legislation and requirements. In these circumstances, Trust Caldicott Guardian and the Head of Information Governance will be available to give guidance for staff when they are informed of any specific problems or barriers.

5 Scope of the Policy

This version of the Policy has been updated following the publication of the DH Information Governance Review: To Share or Not to Share and sets the standards for a first class confidential clinical service that follows Caldicott principles.

Caldicott principles are:

I- Justify the purpose(s)
Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

II- Don't use personal confidential data unless it is absolutely necessary
Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

III- Use the minimum necessary personal confidential data
Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

IV- Access to personal confidential data should be on a strict need-to-know basis
Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

V- Everyone with access to personal confidential data should be aware of their responsibilities
Action should be taken to ensure that those handling personal confidential data — both clinical and non-clinical staff — are made fully aware of their responsibilities and obligations to respect patient confidentiality.

VI- Comply with the law
Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

VII- The duty to share information can be as important as the duty to protect patient confidentiality.

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles.

The principles and standards set out in this policy covers **all personal confidential data**, whether it is information that identifies service users, carers, families, staff, students or other members of public. The policy applies to all staff, permanent and temporary, clinical, management and administrative, including contractors and partner agency staff who handles personal confidential data controlled by the Trust.

It is crucial that all staff understands the reasons for processing personal confidential data. This policy will describe the purpose of obtaining sensitive information from service users, the principles to follow to safe-keep the information provided in confidence, circumstances when this information may need to be shared, disclosed or accessed and will signpost staff to relevant procedures.

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) across the organisation including the heads of professions.

7 Roles and Responsibilities

7.1 The Trust

South London and Maudsley NHS Foundation Trust (SLaM) is committed to the delivery of a first class confidential service. This means ensuring that all service user information is processed fairly, lawfully and as transparently as possible. The Trust will ensure necessary improvements are made to the way sensitive personal confidential information is kept confidential, the service users are kept informed of the way this information is used and that they are given a choice whether this information can be disclosed.

The Trust will ensure sensitive clinical information and the interest of service users are protected through a number of procedures, including:

- Procedures to ensure that all staff, contractors and volunteers are at all times fully aware of their responsibilities regarding confidentiality;
- Recording clinical information accurately, consistently and contemporaneously;
- Keeping information about service users private;
- Keeping information about service users physically secure;
- Disclosing and using information with appropriate care.

The Trust provides mandatory staff training on confidentiality at induction and during employment. Further information on training is in section 16 of this Policy.

It is the role of the Trust Executive to define the Trust's policy in respect of service user/carer confidentiality, taking into account legal and NHS requirements. This policy and the procedures that support it will be reviewed on an annual basis. The Executive is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

The Trust has incident reporting procedures in place to report breaches of confidentiality.

Risk Management Assurance Strategy is in place to assess potential security risks and ensure that risk action plans are kept under regular review.

7.2 Caldicott Guardian and the Caldicott Committee

The Caldicott Guardian is the appointed senior clinician, who carries the ultimate responsibility to oversee the use and sharing of patient identifiable clinical information. This is a key role in ensuring the Trust satisfies the highest practical standards for handling personal confidential data. Acting as the 'conscience' of the Trust, the Caldicott Guardian actively supports work to facilitate and enable information sharing and advises on options for lawful and ethical processing of information as required

The Caldicott Committee supports the Caldicott Guardian and the Head of Information Governance to ensure the Trust meets its legal obligations for data protection and confidentiality implementing the Caldicott principles, the regulations outlined in the Data Protection Act (1998), the new General Data Protection Regulation (May 2018) and new Data Security standards for the NHS and social care (2016)

7.3 Head of Information Governance

The Head of Information Governance is responsible for the strategic and operational management of the Information Governance Team and is the Trust lead for the annual Health and Social Care Information Governance Toolkit self-assessment. Head of Information Governance supports the Caldicott Guardian to ensure the Trust meets the highest standards for appropriate handling of patient information in accordance with the Care Quality Commission regulations (Outcome 2/ Regulation18- Consent; Outcome 21/ Regulation 20- Records and Confidentiality).

The Head of Information Governance is responsible for overseeing day to day issues regarding service user confidentiality; developing and maintaining policies, standards, procedures and guidance, and raising awareness where and when necessary.

7.4 Clinical Academic Group Directors and Senior Managers

All Directors and senior managers within the Trust are responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance.

7.5 All Staff

All staff, whether permanent, temporary or contracted are responsible for ensuring that they are aware and respect the confidentiality of SLaM service users, their carers and families, other relevant members public, staff and students, and that they know the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis.

Most importantly, all Trust staff has responsibility to act professionally in order to meet the confidentiality standards outlined in this policy. This is a legal and professional obligation, which is also set out in Trust employment contracts.

Breaches of confidentiality and the standards set out in this policy due to negligence and ignorance may lead to disciplinary action.

7.6 All Clinical Staff

Clinical staff must ensure that:

- Service users are aware when their information is recorded or health records are accessed;
- Information leaflets on confidentiality and information disclosures are available for service users and have been read and understood;
- Service users know when their personal information may be shared with others involved in their care;
- They will be given the choice not to disclose their information for purposes other than which they were given;
- Their decision to restrict the disclosure or use of information is respected, except where exceptional circumstances apply;
- They understand what the implications may be if they choose to agree to or restrict the disclosure of information;
- They are facilitated in exercising their right to have access to their health records;
- Rights of service users are respected;
- Service users' concerns and queries are answered.

8 Using and Disclosing Confidential Information

8.1 Legal Considerations

There are four main areas of law which constrain the use and disclosure of confidential personal health information. These are briefly described below.

8.1.1 Common Law Duty of Confidentiality

This is built up from case law where practice has been established by individual judgements. The key principle is that information provided in confidence should not be used or disclosed further, except as originally understood by the confider, or with their subsequent permission.

Whilst judgements and other relevant legislation have established that the duty of confidentiality can be overridden 'in the public interest', these have centred on case-by-case consideration of exceptional circumstances.

8.1.2 Data Protection Act (1998)

The Data Protection Act (1998) is the legislation that provides a framework that governs the processing of information that identifies living individuals – personal data in Data Protection terms. Processing includes holding, obtaining, recording, using and disclosing of information and the Act applies to all forms of media, including paper and images. It applies to confidential patient information but is far wider in its scope, e.g. it also covers staff records.

The Act identifies eight Data Protection Principles that set out standards for information handling and sets the foundations for personal data to be:

1. Processed fairly and lawfully
2. Processed for specified purposes
3. Adequate, relevant and not excessive
4. Accurate and kept up to date
5. Not kept for longer than necessary
6. Processed in accordance with the rights of data subjects
7. Protected by appropriate security (practical and organisational)
8. Not transferred outside the EEA without adequate protection

More information can be found at the Information Commissioner's web site at http://www.ico.gov.uk

8.1.3 General Data Protection Regulation (2018)

The new General Data Protection Regulation (GDPR). GDPR will apply in the UK from 25 May 2018. Like the DPA, the GDPR applies to 'personal data'. However, the GDPR's definition is more detailed and makes it clear that information such as an online identifier – e.g. an IP address – can be personal data. The more expansive definition provides for a wide range of personal identifiers to constitute personal data, reflecting changes in technology and the way organisations collect information about people.

The Trust Information Governance (GDPR Compliance) Policy will cover more details on the new legislation.

8.1.4 Human Rights Act (1998)

Article 8 of the Human Rights Act (1998) establishes a right to respect for private and family life. This underscores the duty to protect the privacy of individuals and preserve the confidentiality of their health records. Current understanding is that compliance with the Data Protection Act (1998) and the common law duty of confidentiality should satisfy Human Rights requirements. There is also a more general requirement that actions that interfere with the right to respect for private and family life (e.g. disclosing confidential information) must also be justified as being necessary to support legitimate aims and be proportionate to the need.

8.1.5 Access to Health Records Act (1990)

The records of deceased persons are protected by the provisions of the Access to Health Records Act (1990). These apply only to health records created after 1st November 1991. Where a patient has died, records created after the said date may only be accessed by the following:

- The legal personal representative of the deceased (i.e the executor of the deceased's will or [where there is no will] the administrator of his/her estate).

- A person with a possible claim arising out of the death of the patient. The claim does not need to be against the Trust. It may, for example be an insurance claim. In this case the person is entitled only to such information as is relevant to the potential claim.

It should be noted that if the deceased patient gave a written instruction that any of the above were not to see his/her records, such an instruction overrides the rights contained in the 1990 Act and must be respected.

There are no rights of access to records created before 1st November 1990 and the usual rules of confidentiality apply.

8.1.6 Administrative Law

Administrative law governs the actions of public authorities. According to well-established rules a public authority must possess the power to carry out what it intends to do. If not, its action is *"ultra vires"*, i.e. beyond its lawful powers. The Trust will therefore ensure that it provides mental healthcare and substance misuse services for the public and use its power for this purpose or those that are "reasonably incidental" to the defined purpose in order to act *"intra vires"*.

8.2 Service User Consent for Disclosure of Confidential Information

People using health and social care services are entitled to expect that their personal information will remain confidential. These services cannot work effectively without trust and trust depends on confidentiality. People also expect professionals to share information with other members of the care team, who need to co-operate to provide a seamless, integrated service.

Personal confidential data about service users are given by service users for provision of care and can only be used for healthcare purposes, and unless exceptional circumstances are present, can only be disclosed and used for other purposes with the informed consent of the service user.

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

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.

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.

8.2.1 Gender Identity

Details relating to an individual's gender identity are confidential and classified as 'sensitive' information under the Data Protection Act 1998.

Any individual who has a gender recognition certificate has additional legal protection against inappropriate disclosure of their previous gender under the Gender Recognition Act 2004. Inappropriate disclosure of information about the gender history of a service user with a gender recognition certificate is a criminal offence for which staff members can be prosecuted.

This information can only be disclosed by certain staff in very strict circumstances when consent has been sought and the transmission of data is required for the medical care of the trans person. Service users who hold gender recognition certificates, may or not inform us, and may well wish to keep any discussion of their previous gender to an absolute minimum, unless it is really necessary. Much of the care and support SLaM provides can proceed without the need for knowledge or reference to a trans service user's previous gender.

Staff must take additional measures, in the management of clinical records and any subsequent internal or external communication about the service user, to ensure that a person's previous gender is not disclosed without consent or for non-medical reasons. Doing so could constitute a criminal offence under the Gender Recognition Act 2004 and will put the staff member making such an unlawful disclosure at risk of criminal prosecution.

More more information please refer to the Trust's **Guidance on supporting adult transgender service users.**

8.2.2 Competence to Consent

Seeking consent of service users may be difficult due to illness, disabilities or circumstances that may prevent them from comprehending the likely uses of their information. Mental Capacity Act (2005) is intended to protect people who lack the capacity to make their own decisions. 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, for their health and personal welfare, not just financial matters, once they lose the ability to do so.

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 who lack capacity.

8.2.3 Disclosure without Consent

There are **only three exceptional circumstances that disclosure without consent in a patient with capacity may be justified**. These are:

- 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.

The Courts, including Coroner's Courts, some Tribunals and persons appointed to hold inquiries have legal powers to require disclosure of information that may be relevant to matters within their jurisdiction. This does not require the consent of the service user, whose records are to be disclosed. Such disclosures must be strictly in accordance with the terms of a Court order and should only provide the required information to the bodies specified in the order.

Disclosures in the public interest may be necessary to prevent serious crime or risk of significant harm. Public interest is described as exceptional circumstances that justify overruling the right of an individual to confidentiality in order to serve a broader societal interest. **Decisions about the public interest are complex and must take account of both the potential harm that disclosure may cause and the interest of society in the continued provision of confidential health services.**

Serious crime can be defined as cases involving murder, manslaughter, rape, treason, kidnapping and child abuse, and may all warrant disclosure of confidential information in the public interest. Significant harm to the security of the State or public order also fall within this category. In contrast, theft, fraud or damage to property where loss or damage is less substantial would generally not warrant breach of confidence.

Any disclosure of information should be proportionate and limited to relevant details. Each case must be considered on its merits. In circumstances, where it is difficult to make a judgement, staff should contact the Information Governance Office or seek legal or other specialist advice through Trust Legal Services.

8.2.4 Multi Agency Public Protection Agreements (MAPPA)

The aim of Multi Agency Public Protection Arrangements (MAPPA) is to co-ordinate a risk management plan drawn up for the most serious offenders from the information, skills and resources provided by the individual agencies.

Three groups of people who might be referred to MAPPA are registered sex offenders, all violent and non-registered sex offenders sentenced to 12 months or more in prison (also includes patients on hospital orders) and any other offender posing a risk of serious harm. The Criminal Justice Act (2003) puts a duty on NHS organisations to co-operate with MAPPA.

Further guidance on MAPPA for safeguarding of children can be found in the Trust Child Protection and MAPPA Policy. Further information on MAPPA can be found at the Ministry of Justice web site at http://www.justice.gov.uk/publications/corporate-reports/mappa-reports

8.2.5 Representation at Mental Health Act Tribunals

Care Quality Commissioners, Associate Hospital Managers, Independent Opinion Doctors, Second Opinion Approved Doctors (SOADs), Mental Health Review Tribunal Doctors, Independent Mental Health Advocates(IMHAs), Independent Mental Capacity Advocates, Best Interest Assessors (BIAs), Mental Health Assessors for Deprivation of Liberties (DoLs), solicitors and other legal representatives who are involved in the representation of patients detained under the Mental Health Act (2007) before the Mental Health Review Tribunal (MHRT) require access to medical records.

It is essential that service users' representatives maintain the highest possible standards in the preparation, presentation and conduct of their client's case before the Tribunal. These representatives have a general duty at all times to act in the best interests of the service user and are under a duty to keep the service users' affairs confidential.

The Trust Procedure for External Access to ePJS v4 by Roles Defined under the MHA and MCA is in place to provide guidance to clinical staff to enable temporary read-only access to the relevant service user records. The procedure can be found at the following link:
file://achlys/shared/Published_IT_Documents/Procedures/Procedure_for_MHA_External_Access_to_ePJSv4_091126.pdf

Staff must contact the Mental Health Act Office for further guidance.

8.3 Research and Audit

The Trust is in an academic partnership with the King's College London, King's College Hospital and Guy's and St Thomas' NHS Foundation Trusts as part of King's

Health Partners (KHP). Researchers, who have contractual agreements with the Trust, may want to use clinical information to conduct scientific projects to improve care and treatment of service users.

Similarly, the Trust regularly reviews its clinical practices to improve the quality of its services and safeguard high standards of care. There are Trust procedures in place to plan and conduct clinical audits and service evaluations. Further information on clinical audits and support can be obtained from the Clinical Governance Team.

If information is required for medical research or audit, staff should always evaluate each project whether personal confidential data is needed for such purposes. Unless there is genuine justification, all personal confidential data described in Section 2 of this policy should be taken out to anonymise the data for research purposes.

If data clearly identifies individuals, it must not be processed without a clear legal basis. If data is anonymised in line with the ICO's anonymisation code, it can be freely processed and publicly disclosed.

NHS guidance describes the following information as 'strong identifiers':

- Name
- Full Address
- Full Postcode

The following items are described as 'indirect identifiers':

- Date of Birth
- Ethnic Category
- NHS Number
- Local ID Numbers

Effective anonymisation of sensitive clinical information can be achieved through all or a combination of the following:

- Not displaying strong and indirect identifiers,
- Using derivations to replace the values of certain identifiers in systematic ways, such as using:
    - electoral ward instead of postcode,
    - displaying age instead of date of birth
    - banding of values, such as displaying age bands (e.g. 5-10) instead of date or year of birth using post code sector (first 4 characters e.g. DE3 7) instead of the full post code (e.g. DE3 7FZ)
- Using pseudonyms

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.

Research and audit that utilise information in an effectively anonymised or pseudonymised format may need to identify data subjects later for further contact and recruitment (de-anonymisation). Researchers should clarify in research proposals whether they will need to reverse the anonymisation process to access personal confidential data with relevant justification and if so, the arrangements to obtain permission to access clinical information.

All staff undertaking research and audit must keep personal confidential data secure at all times.

Regular training on research governance is supplied by the Graduate School at King's College London, Research Ethics and Information Governance teams.

All research staff must keep personal identifiable information secure at all times. Associated researchers should clarify in research proposals the arrangements to obtain permission to access clinical information. Once explicit consent is obtained, researchers can use clinical information to conduct research.

The technical management of personal confidential data is regulated by the Trust IT Security Policy and must be adhered to by all staff, including research staff. All staff must ensure personal confidential data is not stored on local hard disks (C drives), unencrypted memory sticks or other portable media. Personal confidential data should only be stored in network drives in password protected files or encrypted drives. This information cannot be e-mailed using unsecured means, including email which is not secure. Details of secure storage and transmission can be found in the Trust ICT Security and e-Mail Policies.

8.3.1 Clinical Record Interactive Search (CRIS)

The Trust and the NIHR Biomedical Research Centre (BRC) for Mental Health has jointly developed a new, safe and secure information system which allows staff to carry out research using information from e-PJS. The system is called the Clinical Record Interactive Search (CRIS). CRIS automatically searches through ePJS records based on specified criteria and keywords, pulls out clinical information relevant to keywords and specified criteria and anonymises such information for research. This enables research staff to use clinical details for research without accessing personal confidential data as CRIS removes all personal information.

Further information about CRIS can be obtained by contacting cris.administrator@kcl.ac.uk

8.4 Key Decisions on Confidentiality

The questions below can be used to underpin key decisions on confidentiality:

- **Is the disclosure needed to support the provision of healthcare or to assure the quality of care?**
  Service users must be informed in advance that some information about them may need to be shared in order to provide them with complete care and treatment. This information can only be shared unless the service user has instructed otherwise. It is good practice to have this discussion with the service user at an early stage and record their wishes on e-PJS.

- **If not healthcare, is the disclosure to support a broader medical purpose, like medical research?**
  Preventative medicine, medical research, health service management, epidemiology are legitimate pursuits to support a broader medical purpose for Trust staff. However, the explicit consent of service users must be sought for information about them to be disclosed for these purposes. This information should be anonymised for research purposes unless disclosure of patient identifiable data is exceptionally justified in the public interest or has temporary support in law under section 251 of the NHS Act (2006).

- **If the purpose served by disclosing is not healthcare or another medical purpose, what is the basis in administrative law for disclosing?**
  The Trust obtains sensitive information from service users for the provision of healthcare services. Information provided in confidence by service users can only be disclosed to other agencies if service user's explicit consent is gained.

- **Is disclosure either a statutory requirement or required by order of a court?**
  Any disclosure that has either a statutory requirement or court order must be complied with. The disclosure should be limited to required information.

- **Is the explicit consent of a service user needed for a disclosure to be lawful?**

  Unless disclosure of patient identifiable information is required by law or the courts, is for a healthcare purpose, can be justified as sufficiently in the public interest to warrant breach of confidence, or is supported by section 251 of the NHA Act (2006), explicit consent is required.

Further information on the principles of sharing information effectively, staff should refer to the Trust Information Sharing Policy.

The General Medical Council (GMC) has issued a guidance document on Confidentiality, which outlines the duties of doctors registered with the GMC. The guidance document explains the new responsibilities on doctors in relation to:

a) reporting concerns about patients to the DVLA
b) disclosing records for financial and administrative purposes
c) reporting gunshot and knife wounds
d) disclosing information about serious communicable diseases
e) disclosing information for insurance, employment and similar purposes
f) disclosing information for education and training purposes

g) responding to criticism in the press

The guidance document is available at the following link:
http://sites.intranet.slam.nhs.uk/ICT/Services/TeamPortfolio/informationgovernance/confidentiality/For%20Trust%20Staff/Guidance%20on%20Confidentiality/Professional%20Guidance/GMC%20Confidentiality%20Guidance%20October%202009.pdf

9 Children and Young People

This section aims to provide staff working with children and young people with the guidance needed to judge when and how to share information about a child or young person. The overriding principle is to improve the outcomes for children, young people and their families.

Sharing information is a vital part of delivering early intervention for children who need additional services, effective safeguarding for children at risk of harm, and preventing youth crime. It is important that staff are confident in making judgements about when and how to share information.

For any service user under 16 years of age, the following 6 key points apply:

- Staff should explain to children, young people and families at the outset, openly and honestly, how sensitive information may be shared and why, and seek their agreement. The exception to this is, where to do so would put that child, young person or others at increased risk of significant harm or an adult at risk of serious harm, or if it would undermine the prevention, detection or prosecution of a serious crime, including where seeking consent might lead to interference with any potential investigation.

- Staff must always consider the safety and welfare of a child or young person when making decisions on whether to share information about them. Where there is concern that the child may be suffering or is at risk of suffering significant harm, the child's safety and welfare must be the overriding consideration.

- Staff should, where possible, respect the wishes of children, young persons or families who do not consent to share confidential information. Staff may still choose to share information, if in their judgement on the facts of the case, there is sufficient need in the public interest to override that lack of consent.

- Staff should seek advice when in doubt, especially where the doubt relates to a concern about possible significant harm to a child or serious harm to others. **It is crucial that staff contact Child Protection Advisors, Information Governance Office and Trust Legal Services as early as possible to discuss the case.**

- Staff should ensure that the information they share is accurate and up-to-date, necessary for the purpose, shared only with those people who need to see it, and shared securely.

- Staff should always record the reasons for their decision – whether it is to share information or not.

Gillick competence is a term used in English medical law to describe the ruling relating to the rights of children under the age of 16 to consent to medical treatment without their parent's knowledge. The parental right to determine whether or not a child below the age of 16 will or will not have medical treatment comes to an end if and when the child achieves sufficient understanding and intelligence to enable them to understand fully what is proposed. Gillick competence relates to the particular child and the particular treatment. It is for the doctor to decide whether or not an individual child is Gillick competent. Should a Doctor decide that a child is Gillick competent then they can only disclose information to the parent with the child's consent, regardless of parental responsibility.

These are only general key points and this is a complex area of the law. For more thorough guidance, *"What to do if you're worried a child is being abused – Every Child Matters; Change for Children"* is the main reference document from HM Government. This document outlines guidance to topics such as sharing information where there are concerns about significant others, what constitutes consent, whose consent should be sought, when not to seek consent. This document and other useful guidance including London Child Protection Procedures can be found on the Trust intranet at the following link:
http://sites.intranet.slam.nhs.uk/childprotection/default.aspx

Staff should also refer to the Trust Child Protection Policy for all issues around the safety of children and young people. This policy can be found at this link:
http://sites.intranet.slam.nhs.uk/Policies/default.aspx

A summary of this guidance on disclosing information when there are concerns about a child can be found in Appendix D.

10 Adults with Learning Disabilities

It is important for staff to assess the competence of service users to consent to disclosure of their personal information when need arises. Staff should follow the guidance outlined in section 8.2.1 of this policy (Competence to Consent) if the service user's disability may prevent them from becoming informed about the likely uses of their information and it is difficult for them to give informed consent. Where the service user is unable to consent, information should only be disclosed in the service user's best interests. It is essential that only information that is needed to support their care is disclosed. Additionally, consideration should be given to disclosure without consent to prevent abuse of these service users, serious injury or damage to their health or if disclosure is required by law or under an order of the court.

11 Carers and Families

South London and Maudsley NHS Foundation Trust is committed to working collaboratively with people who experience mental health problems, and with their families and carers. It recognises that providing effective services relies on a three-way partnership between people who experience mental health problems, their families and carers, and staff. Trust staff have clear responsibility to be proactive in establishing constructive and supportive working relationships with all carers who play a significant part in the lives of service users.

Although it is necessary for the service user to give consent about their treatment to be shared with their carers, information that is not personal can still be given without breaching confidentiality.

The following should guide best practice:

Staff should seek service user's views on sharing information at the earliest opportunity when they present to service. This will normally be during initial assessment or admission.

There needs to be a clear understanding that the issue will need to be re-visited when things have calmed down. Regular review of the situation by the care team is essential.

If permission to share information is refused at this point this must not mean that staff feel unable to give general information about mental illness and treatment options, or to discuss carer's concerns or fears, or to signpost them to carer's support services.

Deciding what information is general and what is personal will be a clinical judgement in each individual case.

When dealing with confidential information provided by carers the same principle of confidentiality still applies. When receiving information from a carer, staff must establish the carer's expectation as to who the information can be shared with. The ePJS has a carer/third party tab for recording confidential information which the carer does not want their relative to have access. Information recorded in the carer/third party section will not be disclosed to a service user even when they make subject access request.

Even when the patient continues to withhold consent, carers must be given sufficient knowledge to enable them to provide effective care. They are also given the opportunity to discuss any difficulties they are experiencing in their caring role and help to try and resolve these. The provision of general information about mental illness, emotional and practical support for carers does not breach confidentiality.

Where someone has already experienced acute illness then the use of **'advance directives',** which include the service user's wishes regarding information sharing with family and carers can be used. When discussing advance directives, emphasis should be placed on the importance of information sharing to providing effective care.

In finding the right balance in sharing information with all parties, staff must consider the carer's, as well as the service user's own health needs, cultural expectations, willingness and capability, when recognising the vital contribution that so many make, often for long periods, with little respite and sometimes little sense of reward.

The guidelines to assist staff, service users and their carers in navigating the minefield of information sharing without compromising service user's confidentiality or excluding the carers from the care of their loved ones are provided in the leaflet entitled "Confidentiality and Carers: Finding the Right Balance" and copies can be accessed at the following link:
http://sites.intranet.slam.nhs.uk/ICT/Services/TeamPortfolio/informationgovernance/confidentiality/default.aspx

12 Requests to Access Medical Records

The Data Protection Act (1998) defines the right to access personal data by the owner or others that have owner's authority to access this information. The right to access can be limited to a particular section or cover the full set of information held by the Trust. **The Trust is under a legal obligation to disclose the information within 30 days subject to health professional approval to disclose the information.**

Requests to access confidential clinical information may come from the following:

- Current or former service users
- A representative (e.g., solicitor, advocate, relative)
- A health professional outside SLaM
- Partner agencies (e.g. social services)
- The Police

Once a request has been received by the clinical team, the Data Protection Office should be contacted immediately following the procedures document. Procedures for staff on how to deal with requests of access to medical records according to the Data Protection Act (1998) can be found at the following link:
http://sites.intranet.slam.nhs.uk/ICT/Services/TeamPortfolio/informationgovernance/confidentiality/default.aspx

The responsibility of authorising disclosure in response to requests to access clinical records lies with the Consultant, who provided the most recent episode of care after reviewing the sensitivity of the information and protecting third party information. Consultants can delegate this task to another member of the clinical team who is familiar with the case. Once this process has been completed, the Consultant will instruct a member of his team (e.g. a member of the local administrative team) to photocopy the records and send to the requestor by recorded delivery. A confirmation of the completion of this procedure will be sent to the Data Protection Office on the 'Health Professional Approval' form. This form can be obtained from the Data Protection Office.

If the requestor asks to view the information on site, the same process applies, but instead of photocopying the notes, an appointment will be made by the Consultant's team so someone from the team will sit with the requestor as they go through the notes.

If a Consultant cannot be located to deal with a request (e.g. Consultant is on leave or no longer employed by the Trust) then the request will be sent to the relevant CAG clinical director, who will instruct appropriate clinical member of staff to approve and release of the information as described above.

If it is a case where a Service cannot be determined, e.g., with very old records, then the request will be sent to the Caldicott Guardian. Only records approved by the Caldicott Guardian will be sent back to Information Governance Department (CR2-Maudsley Hospital) for photocopying and delivery.

Administrative staff will make every effort to check the accuracy of the delivery address and send copies **via recorded delivery.**

12.1 Requests to Access Medical Records from Current Inpatients

Requests from current inpatients can be managed entirely on the ward in line with service user empowerment, openness and therapeutic procedures. Staff should inform the Consultant, who is responsible for the service user and the Consultant should go through the records to make sure that third party information is protected if consent of these individuals cannot be obtained. Information that may cause serious harm to the service user or someone else should be evaluated carefully before disclosure is determined.

It is essential that a clinical member of staff is available during this appointment to answer questions as they view their records on site. This session should be clearly recorded in the 'events' section of the ePJS. If the service user requests to have a copy of the records, the request should be forwarded to the Data Protection Office to be processed in the usual manner.

12.2 HealthLocker

As part of Trust's commitment to empower service users and place them at the centre of their care by providing sufficient, clear and accurate information about their health, treatment and care, the Trust has developed a personal health records system called HealthLocker

Healthlocker is a type of 'Personal Health Record' or online portal, connecting patients to their healthcare provider and parts of their health and social care records. The purpose of this new digital service is to support our service user's care and treatment.

Health Locker can be accessed at the following link:
www.healthlocker.uk

13 Methods of Disclosure

When sharing information, staff must ensure that the information is going to be received by the requestor only. Guidance for staff to follow when disclosing information by post, telephone and fax can be found in the Trust Information Sharing Policy.

If hard copies of medical records are requested, personal identifiable information should be sent either by an authorised courier or recorded delivery. It is crucial to make sure the parcel is named and addressed correctly.

14 Secure Transfer of Personal Identifiable Information

All 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 in-bound and/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 either approve the security of the personal information transfer and complete the registration or make recommendations to improve the security arrangements. All third parties who regularly receive Trust data must be signed up to an Information Processing Agreement (IPA).

15 Bulk Mailing of Service Users

Any planned bulk mailing must be referred to the Trust Communications Department. On completion of a successful needs diagnosis and assessment, the plans will be submitted to the Head of Information Governance. A form detailing the planned mailing will be completed along with updates to the Register of Information Assets and the Inbound and Outbound Register of Secure Transfers.

16 Enhancing Privacy

The Trust recognises that some service users may require additional privacy measures. In order to meet the privacy requirements of these service users, there is a process that aims to provide a confidential solution to service users who are otherwise known to Trust employees through other / professional links (this is also available to Trust staff).

If a service user requests to have their medical records kept under a pseudonym (a fake name), they should discuss this with their care co-ordinator and complete the pseudonymisation form. Once the form is approved by their care co-ordinator, it should be sent to the Data Protection Office.

The procedure and relevant forms can be found at the following link:
http://sites.intranet.slam.nhs.uk/ICT/Services/TeamPortfolio/informationgovernance/confidentiality/PatientWPP/alias2.aspx

17 Commissioning

Commissioners cannot organise the improvement of services unless they know quite a lot about the people using them. However, knowing about service users need not necessarily require commissioners to know their identities.

The Trust has policies and processes in place to ensure that service users are correctly identified by checking their data against the Personal Demographics

Services to improve data quality and hence remove the requirement for commissioners to have personal confidential data.

Local commissioners may be able to use safe havens, within which the personal information they want to assess may be pseudonymised without risk of anyone's sensitive data being disclosed.

Although it may seem necessary for some clinical commissioning bodies or some clinical professionals acting as commissioners to access personal confidential data because they were providing a form of direct care, this is not the function of clinical commissioning groups, as set out in the Health and Social Care Act 2012.

The Trust will only disclose pseudonymised and aggregated data sets for commissioning purposes. Without explicit patient consent e.g. (Individual Funding Request (IFR) or Continuing Healthcare (CHC) , any other disclosure can only happen through a statutory gateway or with specific section 251 approval. The Trust has developed a pseudonymisation process to enable disclosure of de-identified data for limited access to safe havens developed in commissioning organisations when commissioner require to undertake more detailed assessment on individual cases.

18 Public Health

Public Health England is the lead organisation in planning for and responding to emergency situations. This activity requires information to be shared across boundaries and between different organisations.

There are three 'domains' of public health, and the legal basis for staff to handle information about people differs across the domain boundaries:

- *health protection:* Healthcare professionals who are responsible for health protection sometimes need to know personal confidential data about specific individuals. This side of public health resembles the direct care of patients. It would be impractical for them to ask everyone at risk from an infectious disease to give specific consent for staff to provide appropriate information and care. Furthermore, it would not be the most effective way of bringing the infection under control. Preventing the spread of infection is in the public interest and therefore the use of personal confidential data for this purpose has been provided with statutory support through the Health Protection (notification) (and related) regulations 2010 and the Health Service (control of patient information) regulations 2002.

- *health improvement:* The justification above for accessing personal confidential data does not apply to other aspects of public health work, including most health improvement activities (except screening programmes). Understanding the complex relationships that exist between the environment, personal behaviours and disease requires information that can only be derived by linking data from several different sources, which resembles research and the rules and procedures that have developed to provide the information governance for research can usefully be applied to public health intelligence.

- *health services:* A third dimension of public health is to assist people planning healthcare services to understand the health needs of the local population. This

activity resembles commissioning. Although some patient level detail is needed, patients themselves do not need to be identified.

19 Incidents involving breaches of Confidentiality and Information Security

Any incident that involves the loss of personal information (on paper or electronic format), medical records, loss of IT equipment (Trust PC, laptop, memory stick, CDs and other portable media), intentional or unintentional disclosure of personal identifiable information 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 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 NHS Connecting for Health.

19.1 Serious Incidents Requiring Investigation (SIRI)

All staff have a duty to report any breaches of data confidentiality involving significant impact on a number of individual's privacy and/or bulk data transfer as soon as these occur as this is the only way that the Trust can continue to safeguard the integrity of the information entrusted by service users. Staff must not attempt to cover up any data loss as this may expose the Trust to sanctions from the Information Commissioner's Office (ICO). With effect from April 2010, if the ICO identifies that an organisation has not complied with the Data Protection Act and disregarded the law, they can impose tough new sanctions under Section 55 of the Act. **These sanctions include monetary penalties of up to £500,000 or custodial sentences.**

All incidents involving significant impact on a number of individual's privacy and/or bulk data transfer must be immediately reported using Datixweb and a notification must be sent at the same time to the Head of Information Governance, the Caldicott Guardian and the SUI Office.

Once notification is received, the Head of Information Governance will request a fact finder report to be compiled within 24 hours by the relevant service manager and will escalate the incident to the Caldicott Guardian, the SIRO, the relevant Service Director and relevant members of the Executive. Once the fact finder report is finalised, the incident will be reported externally to Department of Health, Monitor, and the Information Commissioner's Office in line with the Information Risk, Incident and Forensic Readiness Policy.

The Trust follows the Health and Social Care Information Centre process for reporting, managing and investigating serious information related incidents on the Health and Social Care Information Governance Toolkit. The Trust Information Risk, Incident and Forensic Readiness Policy has been updated in line with this process.

An overview of all information incidents is included in the quarterly Learning Lessons Report on Information Related Incidents and the Caldicott Annual Report to the Trust Board.

19.2 Incidents involving inappropriate access to records

Any concerns of inappropriate access to electronic patient records should be initially addressed to the relevant clinician. Service users or staff raising the concern will be expected to explain the basis of their concern. They may be required to provide names of people who might have accessed records inappropriately and a specific time period. Based on this information, the clinician will request a check on e-PJS access audit logs from the Information Governance Office in order to identify if there is cause for concern. If there is cause for concern, the clinician must report this as an incident of inappropriate access on Datixweb and request more detailed audit log by contacting the Head of Information Governance.

If former service users do not want to re-establish contact with their clinician, they can lodge concerns of inappropriate access to their medical records by contacting the Information Governance Office and explain the basis of their concern in writing. They may be required to provide names of people who might have accessed records inappropriately and a time period to guide the investigation. If there is cause for concern, the relevant care co-ordinator will be notified to report this as an incident of inappropriate access to be fully investigated.

The Trust undertakes regular random audits on ePJS to identify potential inappropriate access. If and when such inappropriate access has been identified, relevant service director and care co-ordinators are notified to undertake an investigation.

Inappropriate access to records on ePJS will be always investigated. Staff who have knowingly accessed records of individuals whom they have no legitimate clinical relationship may be subject to disciplinary procedure.

20 Training

All Trust staff must attend the compulsory induction training when they start their employment with the Trust. Information Governance Training must be completed within 14 days of starting their role. All staff must either attend face to face Confidentiality and Information Security classroom session or the information governance training on the LEAP system. This training is also available to existing staff. 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 LEAP icon on desktops.

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.

21 Further Information

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

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

Information Governance Office
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/

22 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:

- Information Sharing Policy
- IT Security Policy
- Information Governance Policy
- IT Acceptable Use Policy
- 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
- Multimedia Policy

23 Monitoring Compliance and Effectiveness of this Policy

The compliance with the Confidentiality 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 Confidentiality Policy) and national NHS confidentiality, data protection and information governance standards. The progress on the recommended actions is monitored by the Caldicott Committee.

The Governance Executive Committee 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 Information Security Committee. The identified risks are reviewed by the Caldicott Guardian, Head of IT, and 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 IT 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 Digital Category 2 and above are reported externally to Monitor, NHS Digital 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), IT Security (for Information Security and SU) and FoI (for Corporate Records) Committees
Confidentiality, information sharing,	IG Assurance	Annual	Head of Information	Caldicott Committee (and

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
Data Protection Act (1998),	Programme		Governance	Information Security Committee for technical aspects)
Confidentiality, information sharing, Data Protection Act (1998) incidents	Data breach incident reports and quarterly lesson learned report	Quarterly	Deputy Head of Information Governance	Caldicott Committee (and Information Security Committee for technical incidents)
Health records management and data quality	Health Records Review	Annual	Clinical Systems Manager	Caldicott Committee
Information Security	Computer Audit Programme	Annual	Deputy IG Lead	Information Security Committee
Data Quality	Health Intelligence and Performance Management	Monthly	Head of Performance and Head of HI	Chief Executive's Performance Management Review process

24 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).

25 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. Information Commissioner's Office (2013): Anonymisation Code of Practice
4. Department of Health (2003) Confidentiality: NHS Code of Practice. London: Department of Health
5. HMSO (1998) Data Protection Act 1998
6. HMSO (1998) Human Rights Act 1998
7. HMSO (2007) Mental Health Act 2007
8. HMSO (2005) Mental Capacity Act 2005
9. HMSO (1989) Children Act 1989
10. HMSO (2006) National Health Service Act 2006
11. HMSO (2012) Health and Social Care Act (2012)
12. HMSO (1998) Crime and Disorder Act 1998
13. HMSO (2003) Criminal Justice Act 2003
14. HMSO (2000) The Criminal Justice and Court Services Act 2000
15. Home Office (2003) MAPPA guidance
16. HM Government (2006) What to do if you're worried a child is being abused – Every Child Matters
17. Department for Constitutional Affairs (2007) Mental Capacity Act 2005: Code of Practice. London: Department for Constitutional Affairs
18. General Medical Council (2009) Confidentiality: Guidance for Doctors. London: General Medical Council
19. BMA (1999) Confidentiality and Disclosure of Health Information. London: British Medical Association.
20. Royal College of Psychiatrists (2000) Good Psychiatric Practice: Confidentiality. Council report CR85. London: RCPsych.
21. Nursing and Midwifery Council (2006) A-Z Advice Sheet (Confidentiality)
22. The British Psychological Society (2005) Code of Conduct, Ethical Principles and Guidelines
23. College of Occupational Therapists (2000) Code of Ethics and Professional Conduct for Occupational Therapists
24. General Social Care Council (2002) Code of Practice for Social Care Workers and Code of Practice for Employers of Social Care Workers
25. Health Professions Council (2003) Standards of Conduct, Performance and Ethics
26. Department of Health (1997) The Caldicott Committee – Report on The Review of Patient-Identifiable Information

Appendix 1 - Equality Impact Assessment

South London and Maudsley NHS
NHS Foundation Trust

PART 2: Equality Impact Assessment

1. Name of policy or service development being assessed?

Confidentiality Policy

2. Name of lead person responsible for the policy or service development?

Mustapha Haruna, Deputy IG Lead

3. Describe the policy or service development

What is its main aim? The aim of the Confidentiality Policy is to outline staff responsibilities and provide guidance to ensure service user confidentiality

What are its objectives and intended outcomes?

The main purpose of the information provided by service users in relation to their personal, family, social and medical history and circumstances is to support direct provision of healthcare. Such information that can be used to identify individuals must not be used or disclosed for purposes other than their intended use with the individuals' explicit consent. The policy outlines the standards and sets guidelines to support all Trust staff to maintain service user confidentiality.

Intended outcomes

- Confidential service user information is only used for justified purposes
- Such information is only used when absolutely necessary
- Minimum information is used
- 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

What are the main changes being made? The policy has been updated to reflect the new Data Protection Regulation (GDPR).

What is the timetable for its development and implementation? The policy was consulted with CAGs and service user representatives via the Caldicott Committee previously.

4. What evidence have you considered to understand the impact of the policy or service development on people with different protected characteristics?

(Evidence can include demographic, ePJS or PEDIC data, clinical audits, national or local research or surveys, focus groups or consultation with service users, carers, staff or other

relevant parties).

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 when it was initially rolled out.

5. Have you explained, consulted or involved people who might be affected by the policy or service development?

(Please let us know who you have spoken to and what developments or action has come out of this)

The policy has not change from the last version of the policy (V7). The current update is to include the new Data Protection Regulation (GDPR).

The policy was consulted with CAGs and service user representatives via the Caldicott Committee.

6. Does the evidence you have considered suggest that the policy or service development could have a potentially positive or negative impact on equality, discrimination or good relations for people with protected characteristics?

(Please select yes or no for each relevant protected characteristic below)

Age	**Positive impact:** Yes	**Negative impact:** no

Please summarise potential impacts:

Positve impact : The policy provides guidance for staff on how to uphold service users, carer's and stakeholders confidentiality.

Disability	**Positive impact:** Yes	**Negative impact:** No

Please summarise potential impacts:

Positve impact : The policy provides guidance for staff on how to uphold service users, carer's and stakeholders confidentiality.

Gender re-assignment	**Positive impact:** Yes	**Negative impact:** No

Please summarise potential impacts:

Positve impact : The policy provides guidance for staff on how to uphold service users, carer's and stakeholders confidentiality.

The policy sets out the specific confidentiality requirements for individuals with gender recognition certificates to guide staff on this specific legal protection and the correct procedure for discussing or disclosing individuals' gender identity. Therefore the policy should impact positively on the legal protections around gender reassignment as well as helping to combat discrimination.

Race	**Positive impact:** Yes	**Negative impact:** No

Please summarise potential impacts:

Positve impact : The policy provides guidance for staff on how to uphold service users, carer's and stakeholders confidentiality.

Pregnancy & Maternity	**Positive impact:** Yes	**Negative impact:** No

Please summarise potential impacts:

Positve impact : The policy provides guidance for staff on how to uphold service users, carer's and stakeholders confidentiality.

Religion and Belief	**Positive impact:** Yes	**Negative impact:** No

Please summarise potential impacts:

Positve impact : The policy provides guidance for staff on how to uphold service users, carer's and stakeholders confidentiality.

Sex	**Positive impact:** Yes	**Negative impact:** No

Please summarise potential impacts:

Positve impact : The policy provides guidance for staff on how to uphold service users, carer's and stakeholders confidentiality.

Sexual Orientation	**Positive impact:** Yes	**Negative impact:** No

Please summarise potential impacts:

Positve impact : The policy provides guidance for staff on how to uphold service users, carer's and stakeholders confidentiality.

Marriage & Civil Partnership *(Only if considering employment issues)*	**Positive impact:** Yes	**Negative impact:** No

Please summarise potential impacts:

Positve impact : The policy provides guidance for staff on how to uphold service users, carer's and stakeholders confidentiality.

Other (e.g. Carers)	**Positive impact:** Yes	**Negative impact:** No

Please summarise potential impacts:

Positve impact : The policy provides guidance for staff on how to uphold service users, carer's and stakeholders confidentiality. .

7. Are there changes or practical measures that you can take to mitigate negative impacts or maximise positive impacts you have identified?

N/A

8. What process has been established to review the effects of the policy or service development on equality, discrimination and good relations once it is implemented?

(*This may should include agreeing a review date and process as well as identifying the evidence sources that can allow you to understand the impacts after implementation)*

The policy is set for review in September 2019 whereby the Trust Caldicott Committee will be consulted in the first instance. If the policy requires a lot of revision then a decision will be made as to whether a working group should be established for this revision.

PART 3: Equality Impact Assessment Action plan

Potential impact	Proposed actions	Responsible/ lead person	Timescale	Progress
Positive impact in relation to gender identity	Review entries into Information Sharing Policy on the sharing of on Gender re-assignment	Policy Lead	November 2017	
Review actual impact of policy	Review EIA	Policy Lead	September 2019	

Date completed: 18 /09 / 2017
Name of person completing: *Mustapha Haruna*
CAG: *Corporate*
Service / Department: *Digital Service*

Appendix 2- 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 Tony Konzon, Claims and Litigation Manager (Anthony.Konzon@slam.nhs.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?	NO	
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	No	

HRA Act 1998 Impact Assessment	Yes/No	If Yes, add relevant comments
to receive and impart information and ideas without interference. [withholding information]		
• Article 11 - Freedom of assembly and association	No	
• Article 14 - Freedom from all discrimination	No	

Name of person completing the Initial HRA Assessment:	Deputy IG Lead
Date:	18/09/2017
Person in Legal Services completing the further HRA Assessment (if required):	
Date:	

Appendix 3- Checklist For The Review And Approval Of A Policy

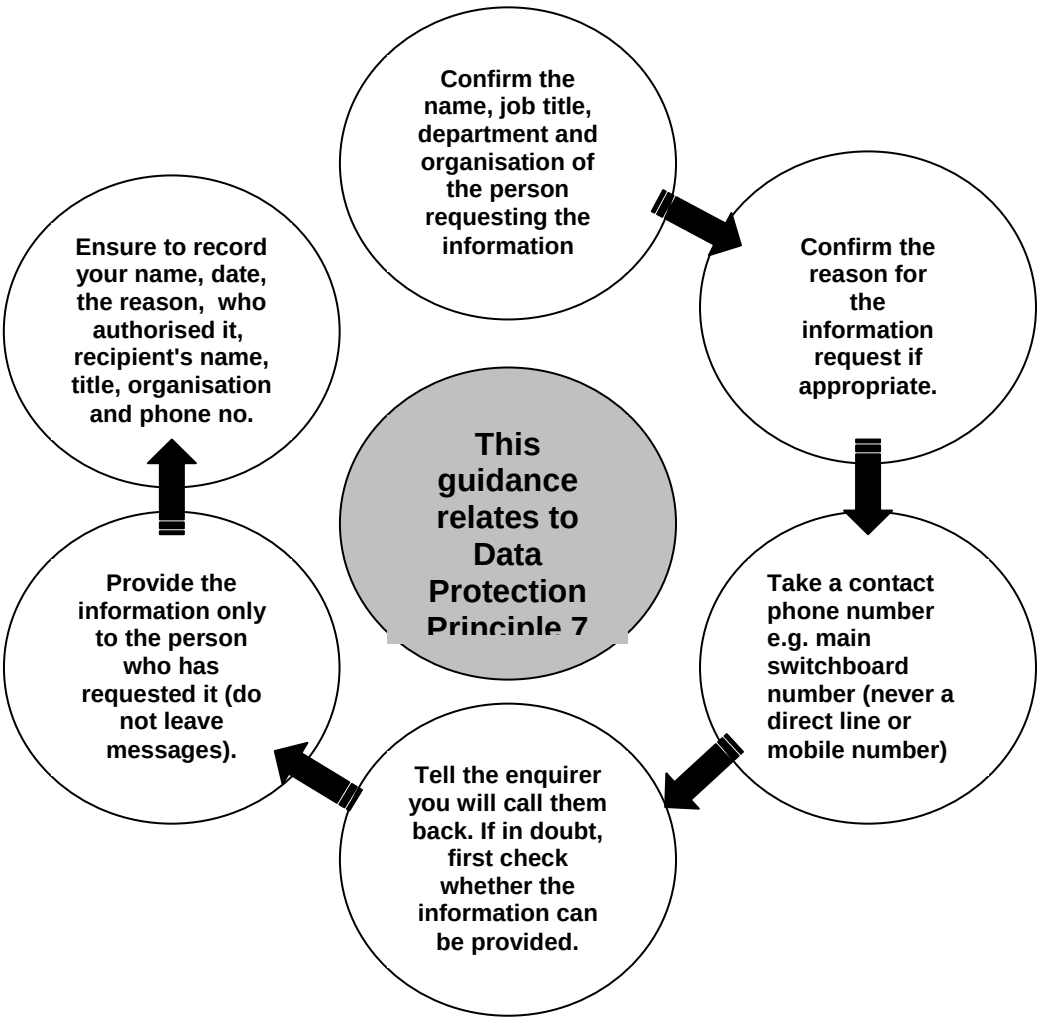
This checklist must be used for self-assessment at the policy writing stage by policy leads and be completed prior to submission to an appropriate Executive Committee/Group for ratification.

	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**		
	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**		

	Title of document being reviewed:	Yes/No/ Unsure	Comments
	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**		
	Is an Equality Impact Assessment included as the appendix of the document?	Y	
	Is a HRA Assessment included as an appendix of the document?	Y	

South London and Maudsley NHS
NHS Foundation Trust

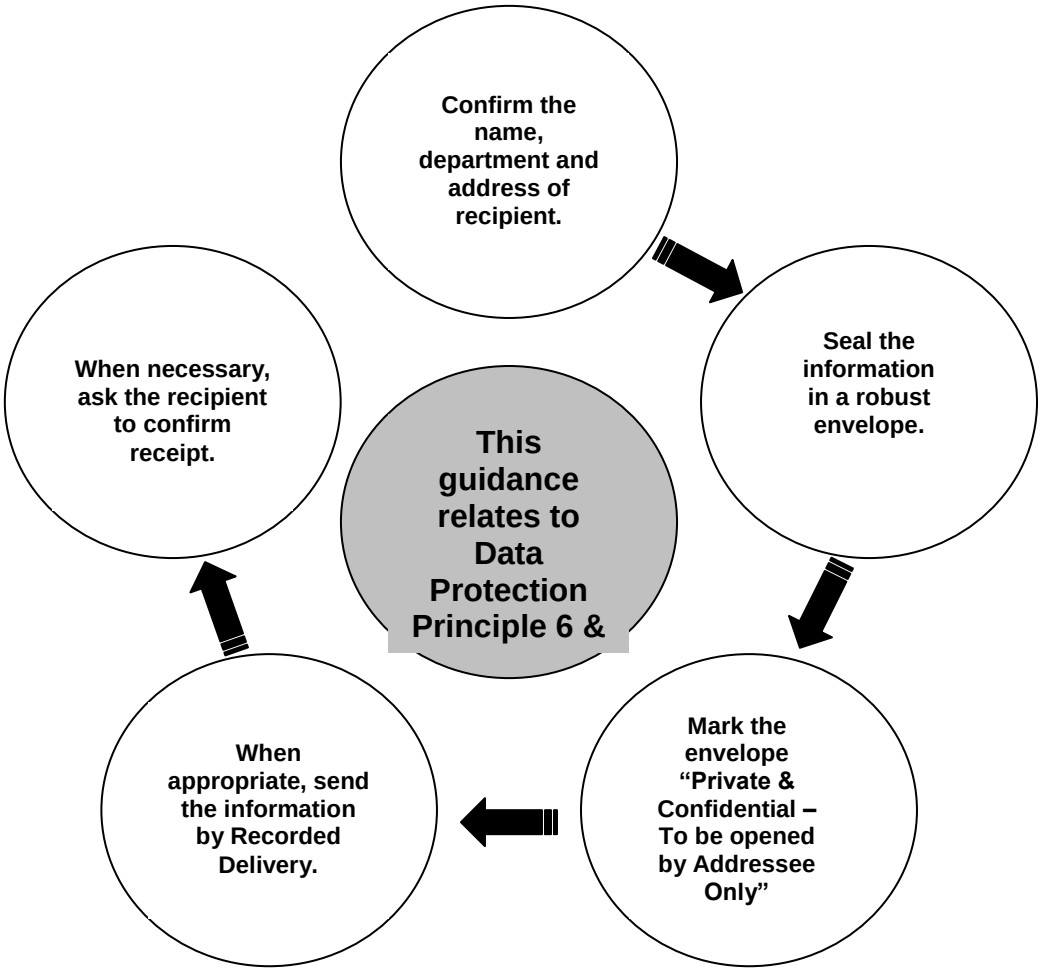
Guidance for Disclosing Confidential Information by Phone



If in doubt, please contact Information Governance on 020 3228 5174
or e-mail: DataProtectionOffice@slam.nhs.uk

South London and Maudsley NHS
NHS Foundation Trust

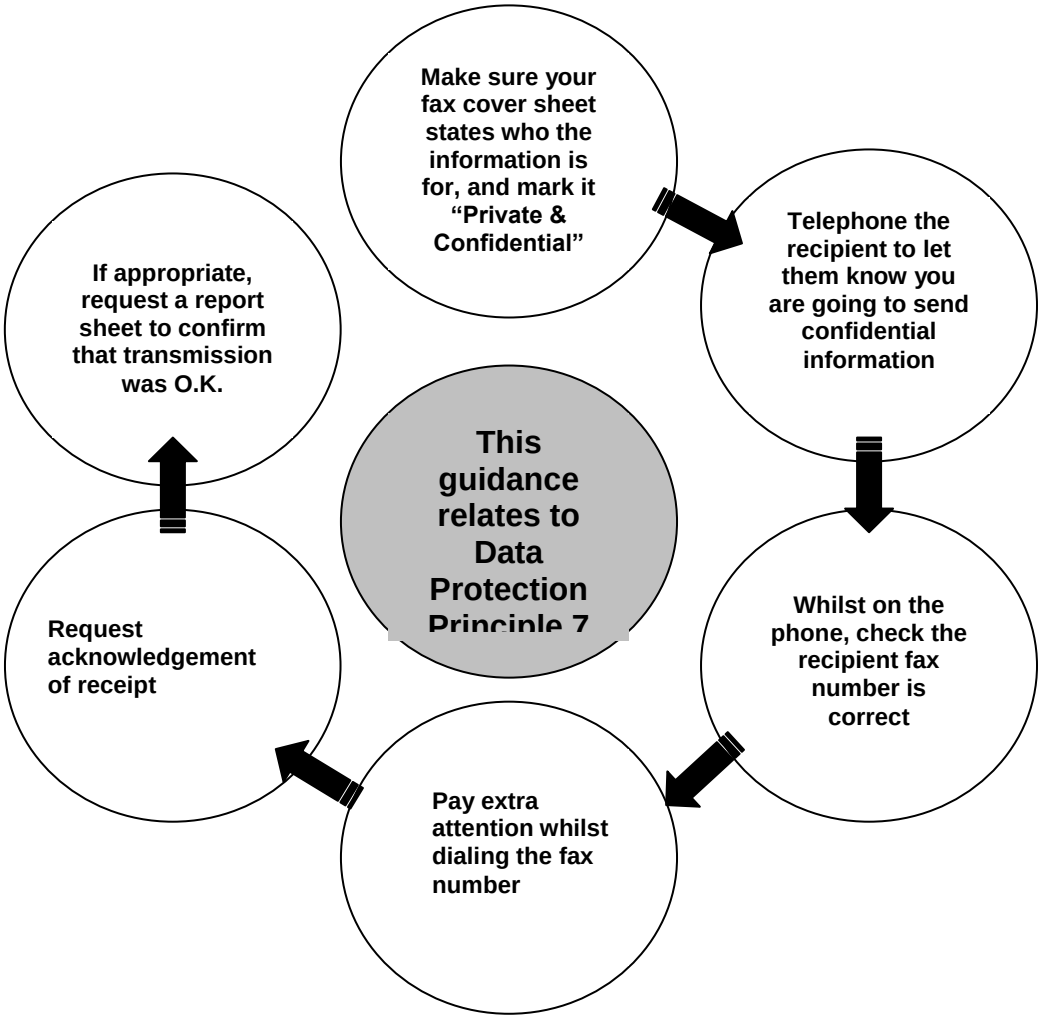
Guidance for Disclosing Confidential Information by Post



If in doubt, please contact Information Governance on 020 3228 5174
or e-mail: DataProtectionOffice@slam.nhs.uk

Guidance for Disclosing Confidential Information by Fax

.

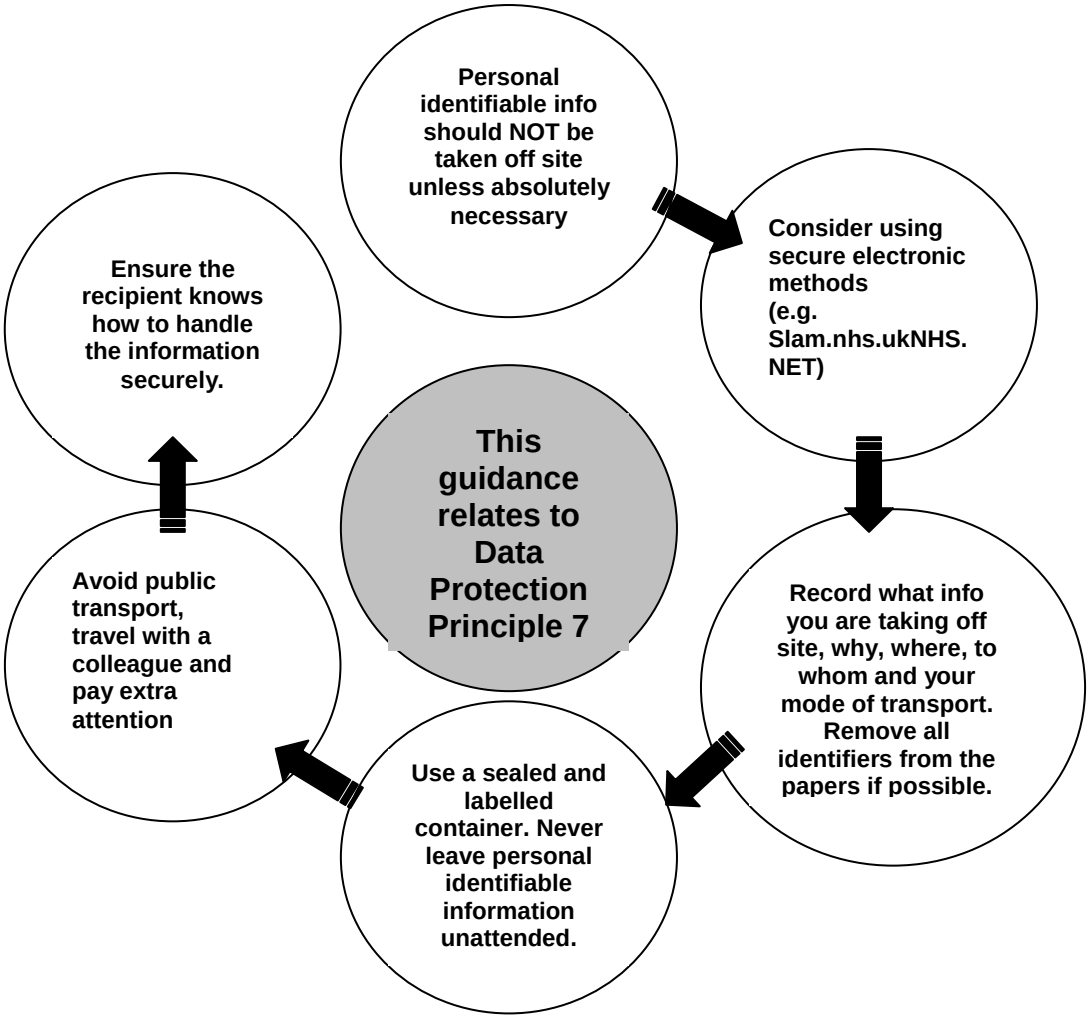


If in doubt, please contact Information Governance on 020 3228 5174
or e-mail: DataProtectionOffice@slam.nhs.uk

Guidance for Transporting Confidential Information [1] [2]

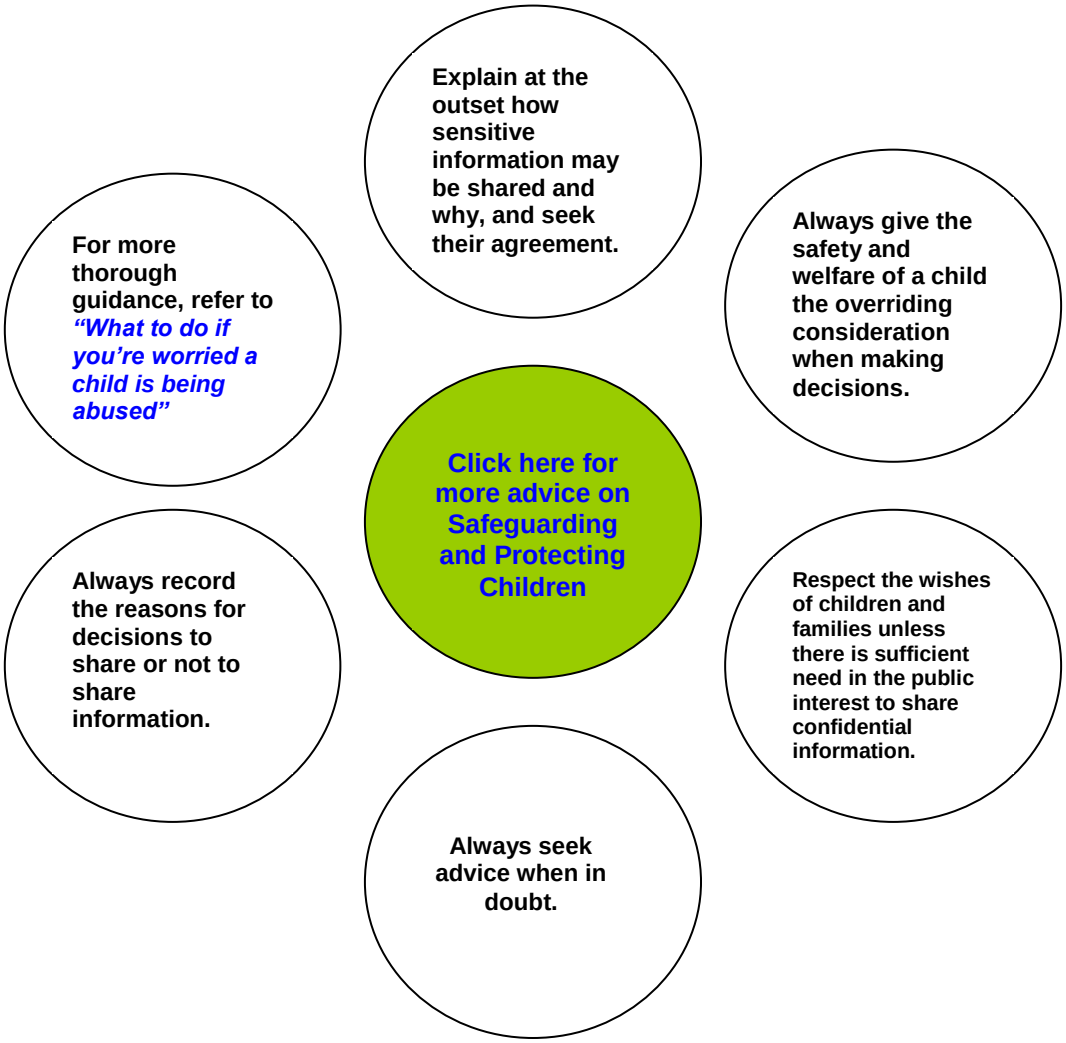
[1] Electronic transfers using SLAM.NHS.UK & NHS.NET is the most secure method.

[2] Avoid physical transportation of personal identifiable information.



If in doubt, please contact Information Governance on 020 3228 5174 or e-mail: DataProtectionOffice@slam.nhs.uk

Guidance on disclosing information where there are concerns about a child



If in doubt, please contact SLaM Advice Line on 07659 152233