Surrey and Sussex Healthcare NHS Trust

Data Protection and Confidentiality Policy

Status (draft/ratified):	Final
Date ratified:	05/07/2018
Version:	2
Ratifying Board:	IG Steering Group
Approved sponsor group:	IG Steering Group
Type of procedural document	Policy
Owner:	Dipa Bhella
Job title:	Information Governance / Data Protection Officer
Author:	Dipa Bhella
Author's job title:	Information Governance / Data Protection Officer
Equality analysis completion date:	August 2018
Date issue:	August 2018
Review date:	31 July 2021
Replaces:	1.1
Unique document number:	2018/064

Equality statement

This document demonstrates commitment to create a positive culture of respect and equal opportunities for all individuals, including staff, patients, their families and carers as well as community partners**.** The intention is, to identify and remove unlawful discriminatory practice contrary to the Equality Act 2010 on the grounds of age, disability, sex, gender reassignment, pregnancy and maternity; race; sexual orientation; religion or belief; marriage and civil partnership.

It is also intended to use the Human Rights Act 1998 to promote positive practice and value the diversity of all individuals and communities. This document is available in different languages and formats upon request to the head of corporate governance.

Contents

Policy summary

It is important that all staff are aware of how to access this policy either via the Trust intranet or via their line manager in the area they work. All staff need to be aware of their responsibilities regarding Data Protection and Confidentiality.

This summary sheet highlights the key things you need to know:

Action	Policy page	✓
The Data protection Act (2018) and General Data Protection Regulation sets the legal framework by which we can process personal information.	5	
The Data protection Act (2018) defines six Data Protection Principles, which all processors or personal information must abide by.	5	
The Trust is required to register annually with the Information Commissioner as a Data Controller the registration is Z720627X	6	
Under GDPR each controller of personal information must decide what basis it is processing personal information.	6	
The Caldicott Report provides staff with a series of principles to adhere to when handling patient identifiable information	7	
The Medical Director is the Trusts Caldicott Guardian and advises the Trust on all matters of patient confidentiality	7	
A fair processing notice also known as a privacy notice informs patients about the way we handle and use their personal data. This is published on the Trust public website.	8	
A Data Protection Impact Assessment (DPIA) should be completed on all projects, proposals or business changes that involve personal information.	8	
Procedures for obtaining access to or copies of personal information held by the Trust about individuals are explained in the Access to Health Records Policy	9	
The Trust carries out audits of access to personal data inappropriate access may lead to disciplinary action.	10	
The Information Commissioner's Office regulates data protection and has a wide range of powers to enforce compliance which includes the imposition of a financial penalty of up to £20,000,000	12	
The Information Governance Manager is the Data Protection officer and is responsible for managing data protection issues throughout the Trust	13	
All staff are responsible for ensuring they keep up to date with Data Security Awareness Training	13	

1 Rationale

The NHS cannot operate effectively if the patients we need to treat do not trust us to provide confidential and effective care. Part of this trust is being able to provide confidential information to clinicians and other staff and be confident that it will remain confidential and only be shared when necessary.

The Data Protection Act (2018) and the General Data Protection Regulation sets the legal framework, by which we can process personal information. It applies to information that might identify any living person. The common law duty of confidentiality governs information given in confidence to a health professional (about a person alive or deceased) with the expectation it will be kept confidential. The Human Rights Act (1998) article 8 provides a person with the right to respect for private and family life. The key rights provided by this legal Framework are also set out in the NHS Constitution (section 3A).

The Data Protection Act (2018) defines six Data Protection Principles; which all processors of personal information must abide by. The 6 principles are:

1. Processing shall be lawful, fair and transparent
2. The purpose of processing shall be specified, explicit and legitimate
3. Personal data processed shall be adequate, relevant and not excessive
4. Personal data shall be accurate and kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary
6. Personal data shall be processed in a secure manner

2 Scope

This policy provides guidance to ensure that information processed by Trust staff is handled in a safe and secure manner which complies with current legislation and best practice relating to data protection and confidentiality.

It will apply to all areas of the Trust and all staff who handle information. It will be of particular relevance to staff members who handle personal and sensitive information relating to both patients and staff.

Data Protection and Confidentiality is a component of Information Governance and as such this policy and associated procedures form part of the Trust's overall Information Governance Framework.

3 Data Protection Act 2018 and GDPR

The Data Protection Act (2018) (DPA) and the General Data Protection Regulation (GDPR) sets out the legal requirements and duties placed on data controllers (i.e. the Trust), and data processors (anyone the Trust uses to process data on our behalf) and explains the 'information rights' held by data subjects (people we hold information about).

The Trust is required to register annually with the Information Commissioner as a Data Controller. The Trust's unique registration number is **Z720627X.**

The DPA sets out 6 data protection principles which describe legal requirements in relation to data processing. These principles are the key 'rules' for data handling and any processing of data which breaches one or more of the 6 data protection principles is unlawful.

Although the Data Protection Act (2018) does not apply to deceased persons, the NHS has issued guidance which states that, where possible, the same level of confidentiality should be provided to the records and information relating to a deceased person as one who is alive.

3.1 Legal basis for processing personal information

Under GDPR each controller of personal information must decide under what basis it is processing personal information. If there is no relevant basis, then the processing is likely to be illegal.

- Under Article 6 the Trusts basis for processing personal information is:
    - "the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law".
- As the Trust processes special category information – which includes health data then it must have a second basis (under Article 9), which are:
    - processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards

- processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy

- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Further guidance on lawful processing is available from the Information Governance Alliance (IGA).

3.2 NHS caldicott report

The Caldicott Report was published in 1997 (updated in 2013 and 2016) and focused on the protection and processing of patient identifiable information within the NHS. The reports provided the NHS with a series of principals to adhere to:

- Justify the purpose for collecting or holding patient-identifiable information
- Do not use patient-identifiable information unless it is absolutely necessary
- Use the minimum necessary patient-identifiable information
- Access to patient-identifiable information should be on a strict need to know basis
- Everyone should be aware of their responsibilities
- Understand and comply with the law
- The duty to share information can be as important as the duty to protect patient confidentiality

The Trust appointed Caldicott Guardian (Medical Director) advises the Trust Board on matters of patient confidentiality and promotes the safe and secure handling of patient data. The Trust Caldicott Guardian will consider and approve, as appropriate, applications for the disclosure or processing of patient data which fall outside routine procedures.

3.3 Data processing

Data processing covers the obtaining, recording, using, storing, disclosure and disposal of data. The lawful and safe processing of data is important to successful business operations and to maintaining confidence between the Trust and its patients, staff and others with whom we deal.

The DPA requires that processing of any personal information held by the Trust must be both fair and lawful. This requires that the processing meets fair processing criteria and satisfies one or more 'conditions for processing' set out in the DPA.

To ensure 'fair processing' we must be lawful, fair and transparent about the way we will use the personal data we hold. We must demonstrate that we:

- are open and honest about our identity
- tell people how we intend to use any personal data we collect about them
- usually handle their personal data only in ways they would reasonably expect
- do not use their information in ways that unjustifiably have a negative effect on them
- help people to understand their rights

To meet this requirement the Trust publishes a fair processing notice also known as a privacy notice to inform patients about the way we handle and use their personal data. This is made available in hard copy format in public facing areas and published on the Trust public website.

Routine data processing for the purposes of patient care will normally be conducted for a purpose that satisfies one of the processing conditions in the DPA. When sharing takes place for non-care reasons (often referred to as secondary purposes) it can be more challenging to satisfy a condition for processing and demonstrate it is lawful processing. This is particularly the case when sharing sensitive information or when sharing personal information without consent.

A Data Protection Impact Assessment (DPIA) should be completed on all projects, proposals or business changes that involve personal information. This could be patient information or staff information. Please contact the Data Protection Officer for a copy of the pro-forma.

The Data Protection Officer (DPO) must be consulted to ensure
that data protection principles such as data minimisation are integrated into the new processing to protect the privacy rights of data subjects.

3.4 Access to IT systems

It is essential that IT systems holding personal data have adequate controls in place to prevent loss, unlawful processing or inappropriate access.

The ICT Security and Acceptable Use Policy provides detailed guidance on the security of Trust IT systems including minimum standards of access controls.

Staff should not attempt to access or use electronic record systems they have not been trained to use or authorised to access. Existing system users should not allow others to access systems using their login credentials. Sharing system passwords is a disciplinary offence and viewed as a serious breach of Trust procedure.

3.5 Access to records

The Trust holds over a million individual patient records in a variety of formats. In addition it holds personal records for present and former members of staff and others it does business with. While it is clearly necessary for many members of staff to routinely access and use these records to carry out their work, it is important staff know that any access to records which is not legitimate or authorised is prohibited and may be unlawful.

Many of our digital clinical systems will allow a user to access any individual record held in that system. Users should only access individual personal records for those data subjects (patients, staff etc) that they have authorisation to access for specific purposes or in the case of patient records where they have a 'legitimate relationship' with the patient.

Staff have no right to access personal information held in records about their relatives, friends or colleagues.

While some Trust staff are in a position to potentially access personal data held about them in Trust records (e.g. their personal medical records) this is not a facility available to members of the public. NHS policy is that NHS staff should follow the same procedure as members of the public to access their data. Therefore **Trust staff should not access their own data held in any Trust records without specific authorisation**.

Procedures for obtaining access to or copies of personal information held by the Trust about individuals are explained in the Access to Health Records Policy.

The Trust carries out audits of access to personal data and any member of staff who is found to be in breach of this guidance by inappropriately accessing their own or other peoples' record data may face disciplinary action.

3.6 Communicating personal information

In order to provide effective care services there is a need to transfer information between organisations and individuals. In order to comply with the DPA principles it is important that any transfer or communication of personal data is carried out securely and safely and the risk of accidental disclosure or loss in transit is minimised.

Any data containing identifiable information transferred by the Trust outside the Trust for processing must be securely encrypted during transit. Any transfer outside the European Economic Area must only be carried out if appropriate security controls are in place.

The Code of Conduct Policy provides guidance to staff on the transfer or communication of personal data by post, fax, by hand and e-mail and the use of portable media.

3.7 Disclosure and sharing of personal information

3.7.1 Sharing personal information for care purposes

In order to provide safe and effective care, personal information about patients will need to be shared with all those caring for an individual. In addition to the clinical team providing care, the direct care team may include laboratory staff, social care staff, specialist care teams and administrative staff supporting the care process.

In accordance with both DPA 2018, GDPR and Caldicott principles information shared for care purposes should be relevant, necessary and proportionate. In applying this principle care should be exercised to avoid compromising care. Confidentiality should not become a barrier to safe and effective care.

Caldicott principle 7 (Duty to share) emphasises the need to share information in certain circumstances where the duty to share information clearly outweighs the normal duty of confidentiality owed. This would be the case when there is a threat to the safety of others and the sharing of personal information about individuals (e.g. vulnerable adults or children) with the police or other agencies may prevent that threat materialising.

3.7.2 Sharing personal information for non-care purposes

Non care purposes (also known as secondary purposes) will include research, service development and improvement, billing and invoicing, service management and contracting. Where possible these activities should be carried out using anonymised or de identified data. This removes the need to consider consent issues.

In certain circumstances the law requires that confidential information should be disclosed when consent may not be provided. Examples of this include a direction within a court order to disclose confidential information or the requirement to notify Public Health officials when a patient is suspected of suffering from a notifiable disease.

Where a legal obligation to disclose does not exist there are some limited circumstances where the sharing of personal information without consent may be justified in the 'Public Interest'. Disclosures made without consent to support the detection investigation and punishment of serious crime and to prevent abuse or serious harm to others are examples of such circumstances. Such disclosures are considered on a case by case basis and can be complex. The public good that would be met by sharing the information has to be weighed against the obligation of confidentiality owed to an individual and the public good in maintaining trust in a confidential service.

3.7.3 Disposal of personal information

It is a principle of the DPA that data should 'not be kept for longer than necessary'. To assist staff in meeting this requirement the Records Management NHS Code of Practice for Health and Social Care provides detailed guidance to staff about the minimum retention periods applicable to Trust records and record disposal procedures.

All printouts, reports and printed copies of records containing personal data should be kept secure at all times. This particularly applies to handover sheets and documents used by staff working in ward areas.

Any documents containing personal data should be disposed of securely in the confidential waste bins provided and not discarded in domestic waste and recycling bins. The Trust waste management team operate a confidential waste disposal service and provide regular collections of confidential waste from all Trust areas.

The disposal of items of electronic equipment which may hold personal data (PCs, laptops and any other devices with information storage capabilities) should be carried out through the IT department to ensure all data is effectively removed before disposal.

3.7.4 Breach of policy and procedure

Any breach of data protection and confidentiality can have severe implications for the Trust, our patients and staff and, where significant numbers of patients are involved, can impact on the reputation of the NHS as a whole.

Breaches of confidentiality or unauthorised disclosure of any information subject to the Data Protection Act 2018 constitutes a serious disciplinary offence under the Trust Disciplinary Policy. Staff found in breach of this policy may be subject to disciplinary action.

The office of the Information Commissioner's Office (ICO) regulates data protection and is charged with upholding individual's information rights. The ICO has a wide range of powers to enforce compliance which includes the imposition of a financial penalty of up to £20,000,000.

Staff who wish to report incidents relating to data protection and confidentiality should follow the incident reporting procedures contained in the Trust Incident Reporting Policy and refer to the NHS guidance on the Notification of Data Security and Protection Incidents.

4 Responsibilities

4.1 Management responsibilities

As Accountable Officer the Chief Executive is responsible for overall leadership and management of the Trust and has the ultimate responsibility for ensuring compliance with the Data Protection Act (2018), the General Data Protection Regulation, Human Rights Act (1998) and the Common Law Duty of Confidentiality.

The **Director of Information and Facilities** has been appointed as the Trust **Senior Information Risk Officer (SIRO)** and is also the executive lead for information governance.

The Information Governance Manager is the Data Protection Officer and responsible for managing data protection issues throughout the Trust.

The Director of Information and Facilities chairs the **Information Steering Group,** where data protection issues should be discussed and escalated to the Executive Committee.

Day to day responsibility for data protection and confidentiality management is the responsibility of the **Trust Information Governance Manager.**

The Trust has appointed the **Medical Director** as the Trust Caldicott Guardian with specific responsibility for the confidentiality agenda and the collection, use and sharing of patient information.

Divisional managers are responsible for the local implementation of this policy in their areas of responsibility.

4.2 Individual responsibilities

Everyone working for the NHS has a legal duty to keep information about patients and clients and other individuals such as staff or volunteers confidential. They are required to adhere to confidentiality agreements i.e. common-law duty of confidentiality, contract of employment, NHS Confidentiality Code of Practice.

All staff are responsible for ensuring they keep up to date with Data Security Awareness Training in accordance with the Trust Statutory and Mandatory training policy as this training covers relevant data protection, security and confidentiality requirements.

This requirement also applies to workers (including agency, bank workers and fixed term contracted staff), volunteers and contractors working at the Trust who may have access to personal information.

5 Compliance monitoring arrangements

The purpose of monitoring is to provide assurance that the agreed approach is being followed – this ensures we get things right for patients, use resources well and protect our reputation. Our monitoring will therefore be proportionate, achievable and deal with specifics that can be assessed or measured.

What will be monitored	Responsible	Frequency	Reported to
Breaches of Incidents	IG Manager	Quarterly	IG Steering Group
Compliance with Subject Access Requests	Medical Records Manager	Quarterly	IG Steering Group
Compliance with Freedom of Information Requests	Head of Communications	Quarterly	IG Steering Group
Audit access to personal data	Privacy Officers	Ad-hoc	IG Steering Group
Spot checks	IG Manager	Ad-hoc	IG Steering Group
Compliance with Data Security Awareness Training	IG Manager	Quarterly	IG Steering Group
Compliance with standards set in Data Security and Protection Toolkit	IG Manager	Annual assessment	IG Steering Group

6 Training to ensure compliance with this policy

Annual Data Security Awareness training must be completed by all staff in accordance with the Data Security and Protection Toolkit and the Trust training needs analysis for all staff groups. Reference to the existence of this policy is made during face to face IG training sessions.

7 References and associated documents

References

Information Commissioner's Officer
https://ico.org.uk/for-organisations/guide-to-data-protection/

Guidance on lawful processing

Records Management NHS Code of Practice

Surrey & Sussex Healthcare NHS Trust privacy notice (fair processing notice)

Data Privacy Impact Assessments

Associated documents

Staff Code of Conduct Policy in respect to Confidentiality
Email Policy
Internet Policy
Information Governance Policy
ICT Security and Acceptable Use Policy
Access to Medical Records Policy
Incident Reporting Policy
Disciplinary Policy
Guide to the Notification of Data Security and Protection Incidents

8 Glossary

Acronym/abbreviation/term	Meaning
Personal Data	Any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.
Data controller	The person (or company) who determines the purposes for which and the manner in which any personal data are, or are to be, recorded. In our case, the Data Controller is the Trust
Data flow	A continuing or repeated flow of information which takes place between individuals or organisations and includes personal data.
Data processor	Any person who processes data on behalf of the data controller.
Direct care	The provision of clinical services to a patient that require some degree of interaction between the patient and the health care provider. Examples include assessment, performing procedures and implementation of a care plan
Duty of confidence	A duty of confidence arises when one person discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence. It arises from common law.
Explicit consent	A form of consent normally given orally or in writing and is where a patient makes a clear and positive indication that they understand the consequences of what they are agreeing to and are content with these consequences. For data protection purposes, this must clearly set out how the information is going to be used and how the person can withdraw that consent.
Information governance	Information governance is a combination of legal requirements, policy and best practice designed to ensure all aspects of information processing and handling are of the highest standards.

Legitimate relationship	A relationship that exists between a patient and an individual or group of record users involved in their treatment which provides the justification for those users to access a patient record.
Processing	This term covers the collection, recording or holding of information or data, or carrying out any operation or set of operations on the information or data, including but not restricted to alteration, retrieval, disclosure and destruction or disposal of the data
Non care or secondary purpose	Purposes other than direct care such as healthcare planning, commissioning, public health, clinical audit and governance, benchmarking, performance improvement, medical research and policy development.

9 Document control

This procedural document supports:

Standard(s)/key lines of enquiry	Paragraph/ID no	Standard/title
NHS Litigation Authority (NHSLA)		
Care Quality Commission (CQC)		
NICE Guideline		
Other national guidance (eg Royal College Guidance) - please list		

Consultation record

Relevant service	Speciality, sponsor or user group name	Individual's name	Job title	Date consulted	Date feedback received
SASH	IG Steering Group	IG members	IG members	05 July 2018	

Change history

Version	Date (DD/MM/YYYY)	Author / Lead	Job title	Details of change	Ratification body	Archiving location
1.1	Sept 2014	Dipa Bhella	IG Manager / DPO	Minor changes to all sections, new policy template	IG Steering Group	Intranet
2	July 2018	Dipa Bhella	IG Manager / DPO	Policy revised to reflect new changes in legislation DPA 2018 and GDR	IG Steering Group	Intranet

Appendices

Appendix 1 Equality analysis

By completing this document in full you will have gathered evidence to ensure, documentation, service design, delivery and organisational decisions have due regard for the Equality Act 2010. This will also provide evidence to support the Public Sector Equality Duty.

Name of the policy/function/service development being assessed	DPA and Confidentiality	
Date last reviewed or created and version number	August 2018	
Briefly describe its aims and objectives:	This policy provides guidance to ensure that information processed by Trust staff is handled in a safe and secure manner which complies with current legislation and best practice relating to data protection and confidentiality	
Directorate lead	Dipa Bhella	
Target audience (including staff or patients affected)	All staff	
Screening completed by (please include everyone's name)	**Organisation**	**Date**
Colin Pink	SASH	August 2018

Equality group *(or protected characteristic)*	What evidence has been used for this assessment?	What engagement and consultation has been used	Identify positive and negative impacts	How are you going to address issues identified?	Lead and Timeframe
Age	*				
Disability	*				
Gender reassignment	*				
Marriage and civil partnership	*				
Pregnancy and maternity	*				
Race	*				
Religion and belief	*				
Sex	*				
Sexual orientation	*				
Carers	*				

*This policy follows best practice guidance described in the references no adverse equality impact was identified.