Ref No: CP238

Sheffield Children's NHS Foundation Trust

Corporate Policy

Data Protection Policy

Author and Contact Person	Date Approved By Finance and Resources Committee	Implementation Date	Version number	Issue Date	Review Date
Russell Banks Head of IM&T (Data Protection Officer)	October 2019	September 2019	8	September 2019	September 2022

REQUIREMENT	ACTION
Who should be aware of this policy and where to access it	Executive Directors, Clinical Directors, General Managers, Heads of Department, all staff
Who should understand the policy	Executive Directors, Clinical Directors, General Managers, Heads of Department, Information Asset Owners, Information Asset Administrators
Who should have a good working knowledge of the policy	Information Governance Committee, all above and staff who develop Trust documents.
Whether the policy should be included in the General Trust Induction Programme and/or departmental specific induction programme.	Awareness of policy update.
Where is the policy available	Trust Intranet
Copy to be sent to HR with a request for inclusion in induction documents	Yes
Copy to:	IT
Process for monitoring the effectiveness of this document	See section 8
Patient version.	Leaflet 049 PROTECTING INFORMATION ABOUT YOU AND YOUR CHILD
Groups/persons consulted	Information Governance Committee
Training	General Induction Programme Awareness raising with departmental managers
This Policy is subject to the Freedom of Information Act	

CONTENTS

1	INTRODUCTION	4
2	PURPOSE	5
3	ROLES AND RESPONSIBILITIES	5
4	DATA PROTECTION LEGISLATION	7
5	DATA PROTECTION PRINCIPLES	7
6	OVERSEAS TRANSFERS	14
7	STAFF ISSUES	14
8	PROCESS FOR MONITORING COMPLIANCE WITH THE DOCUMENT	15
9	COMPLAINTS	16
10	REFERENCES	16
11	ASSOCIATED DOCUMENTS	17
12	EQUALITY IMPACT ASSESSMENT	17
13	VERSION CONTROL	18

Appendix 1:
DEFINITIONS 19

Appendix 2:
GUIDELINES FOR TRANSFER OF PATIENT DATA OUTSIDE THE UK 23

Appendix 3:
LINKS TO ASSOCIATED TRUST PROCEDURES 24

1 INTRODUCTION

1.1 The Trust has a legal obligation to comply with all appropriate legislation in respect of data security and confidentiality and the Data Protection Act 2018 (GDPR). It also has a duty to comply with guidance issued by the Department of Health, other advisory groups to the NHS and guidance issued by professional bodies.

1.2 The 2018 General Data Protection Regulation (GDPR) replaces the Data Protection Act 1998 (DPA). Much of the 1998 DPA continues but the new regulation clarifies several points that had previously been the subject of debate, plus it sets out additional rights to individuals, tightens breach reporting responsibilities for organisations and identifies enhanced responsibilities for individuals involved in processing personal data. It also increases fines which can be imposed by the Information Commissioners Office (ICO).

1.3 As a Data Controller the Trust has followed many of the requirements of the new regulation, by virtue of complying with the previous Act. It is anticipated that there will be aspects of the new regulation that will over time be tested in the courts and additional guidance on interpretation will continue to be produced. As such, this Policy and associated processes that are put in place will adapt over time and these will be reflected in regular updates to this Policy and/or associated documented Procedures.

1.4 All legislation relevant to an individual's right of privacy and the ways in which that can be achieved and maintained are paramount to the Trust.

1.5 In the event of non-compliance with GDPR, penalties may be imposed upon the Trust as Data Controller or upon the Trust in circumstances where the Trust is a Data Processor to a third party Data Controller.

1.6 Information Commissioner's Office (ICO) has powers to impose fines of up to:

- 4% annual turnover or 20 million euros (whichever is greater) for breaching an individual's privacy; and/or
- 2% annual turnover or 10 million euros (whichever is greater) for failing to follow the correct procedure for breach notification and for not complying with the regulation, even if no breach has occurred.

1.7 Fines will take account of an organisation's previous management and compliance with Data Protection regulation. Fines may also be levied upon individuals who fail to comply with the law.

1.8 This policy relates to all staff and especially those who use, collect or process (manual or electronic processing) data/information relating to individuals.

1.9 This Policy sets out requirements for ensuring that Data Protection Impact Assessments (DPIA) are undertaken at the planning stage of any new process or project that includes the processing of personal data.

1.10 An effective DPIA will allow for the identification and remediation of data privacy issues at an early stage of a project, ensuring that principles of 'privacy by design' and 'privacy by default' are embedded across the Trust. The process and forms for completing a DPIA are signposted at Appendix 3.

1.11 Circumstances in which a DPIA will be required shall include:

- Procurement, implementation or use of technology, machines, devices or products which hold or process personal data or information, even if only used within a trial period.
- Publishing personal identifiable or sensitive information or data on the internet or in other publically available media types.
- De-commissioning or disposal of technology, machines or devices or products, paper records, etc. which hold or process personal data or information.
- A change to existing processes or technology, machines or devices and products which will significantly amend the way personal data or information is collected, stored, processed or accessed.
- Collection, retrieval, disposal, storage, recording or holding of new personal data or information.

2 PURPOSE

2.1 The purpose of this Data Protection Policy is to detail how the Trust meets its legal obligations and NHS requirements concerning confidentiality, privacy and the management of information systems and security/information management standards.

2.2 For the purpose of this Policy, key relevant legislation and appropriate guidance has been referenced. A brief summary of the General Data Protection Regulation, associated legislation and guidelines are detailed in Section 4.

3 ROLES AND RESPONSIBILITIES

3.1 Trust Board and Chief Executive

It is the role of the Trust Board/Chief Executive to ensure that the Trust's policies support the implementation, use and handling of person identifiable information and that processing is done transparently, lawfully, accurately, securely and with a lawful basis. The Trust Board is also responsible for ensuring that sufficient resources are provided to support the requirements of the Policy and the role of Data Protection Officer (described below).

3.2 Data Protection Officer (Head of IM&T)

The Data Protection Officer (DPO) has a statutory responsibility and is a legal role required by the Data Protection Act. The Data Protection Officer is responsible for overseeing implementation of data protection and security measures to ensure compliance with the GDPR requirements (and in accordance with this Policy).

The DPO will advise the Trust on matters relating to Data Protection regulation and will act as a contact and advice resource for Trust staff and the public.

GDPR is very clear that the Data Protection Officer must be able to act independently. Any overruling of DPO recommendations will be documented as an Incident.

3.3 Caldicott Guardian (Medical Director)

The Caldicott Guardian is the senior person responsible for protecting the confidentiality of personal information. This includes the key function of ensuring that partner and inter-organisation privacy is maintained.

3.4 Senior Information Risk Owner (Chief Information Officer)

The Senior Information Risk Owner (SIRO) owns the Trust's information risk and incident management framework, information governance policies and risk assessment processes, ensuring they are implemented consistently.

3.5 Information Governance Committee

The Information Governance Committee is responsible for ensuring the development and operation of an effective information assurance framework that covers the scope of the NHS Digital Data Security and Protection Toolkit.

The Information Governance Committee is the main forum within the Trust for considering and addressing the impact of changes to national NHS standards and any legal regulations in respect of information governance issues. Hence this primarily includes cyber security, data protection, data quality and records management.

3.6 Line Managers

Line Managers are responsible for ensuring that their permanent and temporary staff and contractors are aware of:-

- The Data Protection Policy as it relates to their work areas
- Their personal responsibilities for handling person identifiable information
- Compliance with reporting requirements
- How and where to access advice on handling person identifiable information.
- Ensuring their staff have undertaken the Trust mandatory training

Line Managers will be individually responsible for maintaining data protection compliance with in their departments/areas of responsibility.

3.7 All Trust Staff

All staff must be made aware of this policy and any procedures. All staff that process person identifiable information must comply with the Data Protection Policy. Failure to do so may result in penalty sanctions against the Trust, and potential disciplinary action against individuals.

The definition of staff is taken in its broadest sense and covers all individuals working for or in the organisation, including volunteers and contract personnel.

4 DATA PROTECTION LEGISLATION

Data Protection Act (2018) (DPA)

4.1 The EU General Data Protection Regulation (GDPR) has extended the rights of individuals in relation to the personal data that an organisation holds about them. In the UK, this right is governed by the Data Protection Act (DPA), in relation to living individuals. The DPA applies to all person identifiable information held in manual paper files, computer databases, videos and other digital and automated media about living individuals, such as personnel and payroll records, medical records, other manual files, microfiche/film, pathology results, biometric data and x-rays, data held on websites, etc.

4.2 The Act dictates that identifiable data/information will only be collected and/or disclosed with individuals' consent, or specified lawful basis where consent is not required.

4.3 The Trust must hold a register of the data it processes, identifying the purposes for holding the data, how it is used and to whom it may be disclosed (there are specific items to hold). It is also used to enable citizens rights in health called the National Data Opt-Out. The Trust registers annually with the Information Commissioners Office (ICO). This registration is maintained by the Trust's Data Protection Officer (Head of IM&T) on the required renewal basis.

4.4 The Trust must inform the ICO of any significant data confidentiality or security breach within 72 hours of the incident occurring. Breaches that result in a likely inappropriate disclosure will also require notification to the individuals affected, i.e. where there is a high risk of an individual's privacy being compromised. This is assessed by the DPO using the Trust matrix criteria and recorded within the Datix incident reporting system.

4.5 Further details of the legislation requirements are set out at Section 5.

5 DATA PROTECTION PRINCIPLES

It must be noted that the legal requirement to protect an individual's information is secondary to the protection of that individual. This is not a blanket exemption. It must be a defendable position whereby failure to disclose personal information would risk the safety of an individual.

5.1 The Trust as a Data Controller must comply with a number of Principles consistent with the Data Protection Act. These principles are that personal data shall:

- Be processed lawfully, fairly and in a transparent manner in relation to individuals.

- Be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes: further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

- Be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

- Be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

- Be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

- Be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

These Principles are set out in further detail through this Section 5.

5.2 Lawfulness, Fairness and Transparency

There is a requirement to make the general public, who may use the services of the NHS, aware of why the NHS needs information about them, how this is used and to whom it may be disclosed.

Specifically:

5.2.1 Processing Staff Information

There must be procedures to notify staff, temporary employees (volunteers, locums) etc. of the reasons why their information is required, how it will be used and to whom it may be disclosed and have a lawful basis for collection or gain consent where appropriate. This may occur during induction or by their individual manager.

5.2.2 Processing Patient Information

Patients will be made aware of this requirement by the publication of Privacy Notices and the use of information leaflets, statements in patient handbooks or on survey forms, as well as verbally by those health care professionals providing care and treatment. These communications must take regard of age and understanding.

Patient information leaflets will be produced and made available upon request via the Trust's Intranet and these will be sited in patient areas.

All newly referred patients receive the leaflet *"049 PROTECTING INFORMATION ABOUT YOU AND YOUR CHILD"* appended to their appointment letters.

Privacy Notice statements will be published on the Trust's website and will also be summarised in poster form, for prominent display in key areas.

5.2.3 Individual Rights

GDPR sets out the following individual rights, which are further expanded on below:

- The right of access
- The right to be informed
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

The regulation determines an age of 13 years as being a legal age for the application of these rights. In practice, this can be a difficult thing to determine in some circumstances, e.g. a child attending A&E without parents may claim to be 13. The DPO and Caldicott Guardian have determined that (until any firmer other guidance is received) the Trust will continue to follow the "Gillick" principle of competence where the age cannot be determined.

5.2.3.1 The Right to Access

Individuals whose information is held within the Trust have rights of access to their information, regardless of the media the information may be held/retained on. Individuals also have a right to complain if they believe that the Trust is not complying with the requirements of the Data Protection Act.

The Trust procedure for Disclosing Copies of Health Records can be found in the Subject Access Request Policy. Further details of this request process are provided at Appendix 3.

The Access to Health Records Act 1990 provides a specified cohort of people with a statutory right to apply for access to the health records of a deceased individual. These individuals are defined under Section 3(1)(f) of the Act as "the patient's personal representative and any person who may have a claim arising out of the patient's death". A personal representative is the executor or administrator of the deceased person's estate.

5.2.3.2 The Right to be Informed

The Trust will notify individuals if a high risk breach occurs affecting their privacy or freedoms and this right to be enabled without delay within a period of 1 month and at no charge to the individual (certain exemptions may affect this right such as: if requests are excessive or manifestly unfounded).

A controller must, **within one month** of receiving a request made under those rights, provide any requested information in relation to **any of the rights of data subjects**. If the controller fails to meet this deadline, the data subject may complain to the relevant DPO and may seek a judicial remedy. Where a controller receives large numbers of requests, or especially complex requests, **the time limit may be extended by a maximum of two further months**, however, the data subject must be informed of this extension within the 1 month time period**.**
Requests about children are often complex and may span long time periods over numerous systems, it is likely that many requests will be deemed complex.

The Trust will also keep individuals informed of who they can contact at the Trust and what rights they have and how their data is used.

The Trust will maintain a leaflet of information to inform individuals of their rights and how the Trust manages their information. This will include (among other items)

- who we send/disclose their data to
- if we transfer this data outside the country/EU
- how long we keep it
- their rights
- how we manage consent and withdrawal
- ICO contact details
- DPO contact details
- what automated processing occurs and when we get information from third parties and from where
- Any automated processing including use of the “cloud”

5.2.3.3 The Right to Rectification

Individuals have the right to request that the Trust correct data inconsistencies and inaccuracies.
Rectification is often not black and white. The Trust’s main standpoint principle is a clinical record must not be altered by removing content from a request under this right. Errors must be corrected in a transparent manner and where there is a difference of opinion both opinions should be shown together and labelled appropriately.

5.2.3.4 The Right to Erasure

Individuals have the right to request that the Trust delete data and this is known as the right to be forgotten. In health care and for the safety of the child erasure is often exempt.

5.2.3.5 The Right to Restrict Processing

Data subjects have the **right to restrict the processing of personal data** if:

- the **accuracy of the data is contested**
- the **processing is unlawful** and **the data subject requests restriction**
- the controller **no longer needs the data for their original purpose**, but the data is still required to establish, exercise or defend legal rights.
- The National Data Opt-Out programme also gives the right to restrict processing.

5.2.3.6 The Right to Data Portability

Individuals have the right to receive their data in a format that they can use.

5.2.3.7 The Right to Object

Individuals have the right to object to the Trust about how their data is processed.

5.2.3.8 The Right in Relation to Automated Decision Making and Profiling.

Individuals have a right to be informed about the mechanism the Trust uses to process their data and, if profiling, how this is done.

5.2.3.9 Data Protection Requests.

The Data Protection Request process included at Appendix 3 sets out how individuals can exercise their individual rights as outlined at 5.2.3.3 to 5.2.3.8 inclusive.

5.3 Purpose Limitation

There is a requirement to ensure that personal data collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

All data stores which hold and/or process personal information about living individuals must be included within the registration with the Data Protection Officer and the Trust.

The Data Protection Officer will ensure that all relevant data stores, processing and who controls them are registered. A nominated person will be responsible as an Information Asset Owner/Record Manager for each registered data store. A log of data stores and nominated Information Asset Owners/Record Managers will be maintained by the Data Protection Officer for this purpose and to comply with the NHS data opt-out programme.

5.4 Data Minimisation

Personal data being processed must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

5.5 Accuracy

The Trust has to ensure that all information held on any media is accurate and up to date. The accuracy of the information can be achieved by implementing validation routines, some of which will be system specific and details must be provided of these validation processes to the system/information users.

Users of software will be responsible for the quality (i.e. Accuracy, Timeliness, and Completeness) of their data by carrying out their own quality assurance and participating as required by the Data Quality Policy.

Staff will check with patients that the information held by the Trust is kept up to date by asking patients attending appointments to validate the key information held. Errors and mistakes will be documented through the incident reporting process.

Staff information must also be checked for accuracy periodically and maintained to comply with the regulation – either by the manager or by the Human Resources department whoever maintains staff records.

If individuals feel that information recorded in their record is incorrect, they should first make an informal approach to the professional concerned to discuss the situation. This 'Data Protection Request' (DPR) must be recorded. Where both parties agree that information is factually inaccurate it should be amended to clearly display the correction whilst ensuring that the original information is still legible. An explanation for the correction should also be added.

Where there is disagreement about the accuracy of the entry, the Data Controller will allow the individual to include a statement within the record to the effect that they disagree with the content. This process will be overseen by the Data Protection Officer.

5.6 Storage Limitation

All records are affected by this requirement regardless of the media they may be held, stored or retained on. The Records Management Code of Practice for Health and Social Care provides comprehensive guidance.

If the information on the computer or manual record is not the main record, this is considered to be transient data, and procedures must be put in place to give guidance to these users that the information will be culled, archived or destroyed when no longer deemed to be of use in line with defined

retention/destruction schedules, which are signposted within the Trust's Clinical and Non-Clinical Records Management Policies.

5.8 Integrity and Confidentiality

All personal data processing must be managed in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss destruction or damage, using appropriate technical or organisational measures.

All information relating to identifiable individuals must be kept secure at all times. The Trust will ensure there are adequate procedures in place to protect against unauthorised processing of information and against accidental loss, destruction and damage to this information. Details of how this occurs are within the Information Security Policy.

Measures will be taken to ensure that:

- All data must be removed from hard drives/magnetic media before being disposed of. The Trust policy is physical destruction on site of such media.
- Confidential paper waste is cross cut shredded or is collected and held in a secure area prior to shredding/incinerating. A cross-cut shredder must be used for all shredding. Confidential waste is only by exemption taken off site for destruction.

The Trust has a legal obligation to maintain confidentiality standards for all information relating to patients, employees and Trust business. It is important that this information is disposed of in a secure manner. The NHS is most at risk in this area as there have been many occasions when personal information concerning patients has been discovered in public amenity waste disposal or in other public areas.

All employees will be made aware of how easy it is to breach confidentiality by incorrect use of waste paper, by using examples of 'real life situations' during training sessions. Staff will be informed how to dispose of person identifiable waste products.

The Data Protection Officer will have access to all personal data and processing operations in order to carry out the role as laid down by the regulation.

The Trust's incident management procedures must be followed for reporting and investigating potential and actual data breaches. Where necessary these must be formally reported to the Information Commissioners Office (ICO) within 72 hours of the incident occurring.

The Trust's information governance framework sets out requirements to ensure that all key information assets have a designated Information Asset Owner (IAO). The Information Governance Policy is the most specifically relevant reference point for staff. It sets out these IAO responsibilities in appropriate detail and also signposts all relevant documented Procedures that are to be followed in the management of these responsibilities.

For clarification a system may not necessarily be a computer system but may also be a paper based information system or process flow. All systems must be assessed using the pre DPIA check list prior to (if necessary) a full data protection impact assessment.

Where person identifiable information data/records need to be transported in any media, this process must be carried out to maintain strict security and confidentiality of this information. This may include magnetic tape, floppy disc, CD/DVD, memory stick or manual paper records. All portable electronic media must be encrypted.

Reliable transport couriers must be used at all times, sourced via the Supplies Department and will follow the Trust courier process. Packaging must be sufficient to protect the contents from any physical damage during transit, and will be in accordance with manufacturers' specifications.

Contracts between the Trust and third parties must include appropriate clauses setting out responsibilities for data security and confidentiality, consistent with GDPR requirements. If no such clause exists within the contract, the supplier must complete and sign a separate Confidentiality Agreement. Additionally, Data Sharing Agreements must be signed between the Trust and any third party Data Processor, where contracts involve access to or processing of Trust personal data.

6 OVERSEAS TRANSFERS

6.1 Transferring data outside the European Economic Area (EEA)

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

All person identifiable information sent outside the EEA must first be discussed with – and approved by - the Data Protection Officer and recorded in the Trust's Information Asset Register.

The use of "Apps", where individual's identifiable data is held outside the EEA is expressly forbidden, i.e. for recording or sharing person identifiable data.

Please refer to Appendix 2 for details of countries included within the European Economic Area, along with further procedural guidance.

7 STAFF ISSUES

7.1 Training

The Trust, as a Data Controller, has overall responsibility for maintaining awareness of confidentiality and security issues for all staff. Training for staff will be delivered through a number of means, including:

- personal responsibilities (Job Description)

- confidentiality of personal information (mandatory, annual, e-learning)
- relevant Trust Policies and Procedures (regular dissemination)
- registration of automated databases (initiated via Data Protection Impact Assessments)
- registration of data requests ('Data Protection Request' process – see information governance guidance for staff, set out on the Intranet)
- individuals rights, access to information and compliance with the principles (Privacy Notices, information leaflets)
- general good practice guidelines covering security and confidentiality (guidance for staff and FAQs will be maintained and regularly updated on the intranet, to serve as a central repository)
- promotion of the Data Protection Officer role and how they can be contacted for all problems which may occur in the areas of security and confidentiality of personal information (Privacy Notices, information leaflets, intranet guidance)
- As a result of incidents and events.

7.2 Induction

All new starters to the Trust will be given Information Governance (IG) awareness training as part of the Trust induction process. Extra training in these areas will be given to those who need it, e.g. training packages for specific clinical and business information systems. A register will be maintained of all staff attendance at training sessions.

All staff will also be required complete mandatory IG e-learning on an annual basis and awareness of the National Data Opt-Out will be provided. Periodic reminders will be targeted to all staff through the Trust Metacompliance policy tool.

7.3 Contracts of employment

Staff contracts of employment are produced and monitored by the Human Resources department. All contracts of employment include data protection and general confidentiality clauses. Agency and contract staff are subject to the same clauses.

All Trust employees will be made aware of their responsibilities in connection to this Policy through their Terms and Conditions, Job Descriptions, dissemination of Policies and targeted training activities as described at 7.2 above.

A breach of Data Protection requirements could result in a member of staff facing disciplinary action. A copy of these procedures is available from the Personnel/Human Resources Department and also published on the intranet.

8 PROCESS FOR MONITORING COMPLIANCE WITH THE DOCUMENT

8.1 This policy and associated appendices and procedures will be monitored and updated as necessary by the Data Protection Officer, under oversight through the Trust's Information Governance Committee.

8.2 Internal and External Audit may also review this and associated policies and procedures.

8.3 Evidence of compliance will be part of the Trust's annual NHS self-assessment audit process. This is set out in the NHS Data Security and Protection Toolkit requirements (previously NHS Information Governance Toolkit).

8.4 This Policy will be reviewed regularly to take into account changes to legislation that may occur, and/or guidance from the Department of Health and/or the Information Commissioners Office.

8.5 Breach notification and incident reporting procedures are set out on the intranet and can be accessed through the data protection officer.

9 COMPLAINTS

9.1 The Trust will ensure the Data Protection Officer is involved properly, and in a timely manner, with all issues relating to the protection of personal data complaints procedures. These are reviewed to take account of complaints which may be received because of a breach or suspected breach of the Data Protection Act.

9.2 Individuals have a right to seek compensation for any breach of the Act which may cause them damage and/or distress.

10 REFERENCES

The legislation listed below also refers to issues of security and or confidentiality of personal identifiable information/data:

Data Protection Act 2018
Access to Health Records 1990
Access to Medical Reports Act 1988
Human Rights Act 1998
Crime and Disorder Act 1998
Health and Social Care Act 2001 section 60
Lord Chancellors Code of Practice on the Management of Records 2002
Care Quality Commission Safe Data, Safe Care 2016
Care Quality Commission Policy statement on Information Security and Governance 2016
Department of Health Your Data: Better Security, Better Choice, Better Care 2017
DCB3058 Compliance with National Data Opt-Out 2019

Common Law and Administrative Law also produce judgements that affect the above legislation.

11 ASSOCIATED DOCUMENTS

The following are the main publications referring to security and or confidentiality of personal identifiable information/data (see section 4 for more information).

IMG:E5498	Ensuring Security and Confidentiality in NHS Organisations
HSG(96)18	The Protection & Use of Patient Information
HSC 1999/012	Caldicott Guardians
HSC 2002/003	Implementing the Caldicott Standard into Social Care
HSC1998/217	Preservation, Retention and Destruction of GP General Medical Services Records Relating to Patients
HSC2000/009	The Data Protection Act 2018
BS7799	Industry and adopted NHS IT security standards
July 2016	Records Management Code of Practice for Health and Social Care (replaced Records Management: NHS Code of Practice 2006. HSC 1999/053 For the Record)
February 2010	DOH: Guidance for Access to Health Records Requests
May 2018	Guidance from ICO on consent and for Data Protection Officers

Trust Policies:

CP38	Clinical Records Management Policy
CP39	Corporate (Non-Clinical) Records Management Policy
CP126	Policy for Investigation of Incident/ Complaints and Claims
CP931	Data Quality Policy
CP1526	Subject Access Requests Policy
CP242	Information Security Policy
CP204	Information Governance Policy

The documents referenced in section 10

12 EQUALITY IMPACT ASSESSMENT

12.1 This policy applies to all Trust employees irrespective of age, race, colour, religion, belief, disability, nationality, ethnic origin, sexual orientation or marital status, carer status, social and employment status, HIV status, gender reassignment, political affiliation or trade union membership. All employees will be treated in a fair and equitable manner.

12.2 The Trust will take account of any specific access or specialist requirements (e.g. Interpreter, documents in large print) for individual employees during the implementation of this policy.

13 VERSION CONTROL

Version	Date	Author	Status	Comment
1	February 2004	Russell Banks	Archived	Initial First Draft
2	May 2006	Russell Banks	Archived	
3	April 2009	Russell Banks	Archived	
4	October 2011	Russell Banks	Archived	Roles and Responsibilities added
5	December 2012	Russell Banks	Archived	Minimal changes throughout
5.1	April 2013	Russell Banks	Archived	Cosmetic changes to bring in line with Policy format
6	Feb 2017	Russell Banks	Archived	Updates for forthcoming GDPR, expanding DPO and other roles, PIA, subject rights, duty of candour, consent, breach
7	May 2018	Russell Banks	Archived	Full rewrite re GDPR
8	September 2019	Russell Banks	Approved	New references, National Data Opt-Out. Minor changes

Appendix 1

DEFINITIONS

Item	*Definition*
Anonymity	Information may be used more freely if the subject of the information is not identifiable in any way – this is anonymised data. However, even where such obvious identifiers are missing, rare diseases, drug treatments or statistical analyses which may have very small numbers within a small population may allow individuals to be identified. A combination of items increases the chances of patient identification. When anonymised data will serve the purpose, health professionals must anonymise data and whilst it is not necessary to seek consent, general information about when anonymised data will be used should be made available to patients.
Authentication Requirements	An identifier enables organisations to collate data about an individual. There are increasingly onerous registration processes and document production requirements imposed to ensure the correct person can have, for example, the correct access to a system or have a smartcard. These are warning signs of potential privacy risks.
Caldicott	Seven Caldicott Principles were established following the original reviewed in 1997 and further development in 2013. The principles include: 1. justify the purpose(s) 2. don't use patient identifiable information unless it is necessary 3. use the minimum necessary patient-identifiable information 4. access to patient identifiable information should be on a strict need-to-know basis 5. everyone with access to patient identifiable information should be aware of their responsibilities 6. understand and comply with the law 7. the duty to share information can be as important as the duty to protect patient confidentiality
Common Law Duty of Confidentiality	This duty is derived from case law and a series of court judgements based on the key principle that information given or obtained in confidence should not be used or disclosed further except in certain circumstances: • Where the individual to whom the information relates has consented • Where disclosure is in the overriding public interest; and • Where there is a legal duty to do so, for example a court order • The common law applies to information of both living and deceased patients.

Data Protection Act 1998 (fully applicable up to 25 May 2018)	The DPA defines the ways in which information about living people may be legally used and handled. The main intent is to protect individuals against misuse or abuse of information about them. The 8 principles of the Act state The fundamental principles of DPA 1998 specify that personal data must: 1. be processed fairly and lawfully. 2. be obtained only for lawful purposes and not processed in any manner incompatible with those purposes. 3. be adequate, relevant and not excessive. 4. be accurate and current. 5. not be retained for longer than necessary. 6. be processed in accordance with the rights and freedoms of data subjects. 7. be protected against unauthorized or unlawful processing and against accidental loss, destruction or damage. 8. not be transferred to a country or territory outside the European Economic Area unless that country or territory protects the rights and freedoms of the data subjects.
European Economic Area (EEA)	The European Economic Area comprises of the EU member states plus Iceland, Liechtenstein and Norway
Explicit consent	Express or explicit consent is given by a patient agreeing actively, usually orally (which must be documented in the patients case notes) or in writing, to a particular use of disclosure of information.
General Data Protection Regulation (EU) 2016/679 Principles of Lawful Processing of Personal Identifiable Information	The GDPR requires that data controllers ensure personal data shall be: a) processed lawfully, fairly and in a transparent manner in relation to individuals b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the

	appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
IAO (Information Asset Owner)	These are senior individuals involved in running the relevant service/department. Their role is to understand and address risks to the information assets they 'own' and to provide assurance on the security and use of those assets. They are responsible for providing regular reports regarding information risks and incidents pertaining to the assets under their control/area.
Implied consent	Implied consent is given when an individual takes some other action in the knowledge that in doing so he or she has incidentally agreed to a particular use or disclosure of information, for example, a patient who visits the hospital may be taken to imply consent to a consultant consulting his or her medical records in order to assist diagnosis. Patients must be informed about this and the purposes of disclosure and also have the right to object to the disclosure. Implied consent is unique to the health sector and may be revised under the GDPR.
Information Assets	Information assets are records, information of any kind, data of any kind and any format which we use to support our roles and responsibilities. Examples of Information Assets are databases, systems, manual and electronic records, archived data, libraries, operations and support procedures, manual and training materials, contracts and agreements, business continuity plans, software and hardware.
Personal Data	This means data which relates to a living individual which can be identified: 1. from those data, or 2. from those data and any other information which is in the possession of, or is likely to come into the possession of, the data controller. It also includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual
Privacy and Electronic Communications Regulations 2003	These regulations apply to sending unsolicited marketing messages electronically such as telephone, fax, email and text. Unsolicited marketing material should only be sent if the requester has opted in to receive this information.

Privacy Invasive Technologies	Examples of such technologies include, but are not limited to smart cards, radio frequency identification (RFID) tags, biometrics, locator technologies (including mobile phone location, applications of global positioning systems (GPS) and intelligent transportation systems), visual surveillance, digital image and video recording, profiling, data mining and logging of electronic traffic. Technologies that are inherently intrusive, new and sound threatening are a concern and hence represent a risk
Pseudonymisation	Where patient identifiers such as name, address, date of birth are substituted with a pseudonym, code or other unique reference so that the data will only be identifiable to those who have the code or reference.
Records Management: NHS Code of Practice	Is a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on current legal requirements and professional best practice. The code of practice contains an annex with a health records retention schedule and a Business and Corporate (non-health) records retention schedule.
Retention Periods	Records are required to be kept for a certain period either because of statutory requirement or because they may be needed for administrative purposes during this time. If an organisation decides that it needs to keep records longer than the recommended minimum period, it can vary the period accordingly and record the decision and the reasons behind. The retention period should be calculated from the beginning of the year after the last date on the record. Any decision to keep records longer than 30 years must obtain approval from The National Archives.
Special categories of personal data (sensitive data)	This means personal data consisting of information as to the: A. Concerning health, sex life or sexual orientation B. Racial or ethnic origins C. Trade union membership D. Political opinions E. Religious or philosophical beliefs F. Genetic data G. Biometric data

Appendix 2

GUIDELINES FOR TRANSFER OF PATIENT DATA OUTSIDE THE UK

Background

All person identifiable data processed outside of the UK must comply with the Data Protection Regulation and Department of Health guidelines.

Countries where the transfer of data is subject to the Data Protection Regulation and therefore deemed safe are:

The EU countries plus Iceland, Liechtenstein and Norway:

Austria	Germany	Malta
Belgium	Greece	Netherlands
Bulgaria	Hungary	Norway
Croatia	Iceland	Poland
Cyprus	Ireland	Portugal
Czech Republic	Italy	Romania
Denmark	Latvia	Slovakia
Estonia	Liechtenstein	Slovenia
Finland	Lithuania	Spain
France	Luxembourg	Sweden
		United Kingdom

Other countries not in the EU but are classed as having an adequate level of protection safeguards are:

Andorra	Guernsey	New Zealand
Argentina	Isle of Man	Switzerland
Canada	Israel	Uruguay
Faroe Islands	Jersey	

Further details can be found on the ICO website:
https://icosearch.ico.org.uk/s/redirect?collection=ico-meta&url=https%3A%2F%2Fico.org.uk%2Fmedia%2Ffor-organisations%2Fdocuments%2F1566%2Finternational_transfers_legal_guidance.pdf&index_url=https%3A%2F%2Fico.org.uk%2Fmedia%2Ffor-organisations%2Fdocuments%2F1566%2Finternational_transfers_legal_guidance.pdf&auth=nw0nzId9PdLz4hAUSiFwzg&profile=_default&rank=2&query=principle+8

Personal information can also be transferred to companies in the US that have signed up to the 'Safe Harbor' agreement this has been superseded by the 'EU-US Privacy Shield'. These companies have agreed to abide by a set of rules similar to those found in the Data Protection Act 2018.

Information on countries with an adequate level of protection and the 'EU-US Privacy Shield' agreements is available at:
https://ico.org.uk/for-organisations/data-protection-and-brexit/data-protection-if-there-s-no-brexit-deal/the-gdpr/international-data-transfers/

Appendix 3

LINKS TO ASSOCIATED TRUST PROCEDURES

A4.1 Subject Access Requests

http://nww.sch.nhs.uk/documents/14-trust-documents/2113-access-to-patient-records-application-form/latest/download

Further information is available on -
http://nww.sch.nhs.uk/departments/information-governance/subject-access-request

A4.2 Data Protection Requests

http://nww.sch.nhs.uk/documents/14-trust-documents/2117-data-protection-request-process/latest/download

Further information is available on -
http://nww.sch.nhs.uk/departments/information-governance/data-protection

A4.3 Data Protection Impact Assessment – Initial Screening

http://nww.sch.nhs.uk/documents/14-trust-documents/2108-data-protection-impact-assessment-screening/latest/download

Further information is available on -
http://nww.sch.nhs.uk/departments/information-governance/screening-for-data-privacy-impact-assessment

A4.4 Data Protection Impact Assessment – Full Detailed Process

http://nww.sch.nhs.uk/documents/14-trust-documents/2109-data-protection-impact-assessment/latest/download

Further information is available on –
http://nww.sch.nhs.uk/departments/information-governance/data-privacy-impact-assessment