South East Coast Ambulance Service NHS
NHS Foundation Trust

Data Protection Policy

Contents

1 Introduction

1.1. The South East Coast Ambulance Service NHS Foundation Trust ('the Trust') has a legal obligation to comply with all relevant legislation in respect of Data, Information and IT Security. It also has a duty to comply with guidance issued by the Department of Health, the Information Commissioner, other advisory groups to the NHS and guidance issued by professional bodies.

1.2. For the purpose of this Policy other relevant legislation and appropriate guidance may be referenced.

1.3. A brief summary of the Data Protection Act 2018 (including the UK General Data Protection Regulation), associated legislation and guidelines is provided in Appendix 1.

2 Aims and Objectives

2.1. This Data Protection Policy aims to detail how the Trust will meet its legal obligations and NHS requirements concerning confidentiality and information security standards. The requirements within the policy are primarily based upon the Data Protection Act 2018 and UK General Data Protection Regulation which are key pieces of legislation covering information security and confidentiality of personal information.

3 Definitions

3.1. **Data protection principles**: The principles of good practice are detailed within the Data Protection Act 2018 (including the UK General Data Protection Regulation) which must be adhered to when processing personal data (see Section 5).

3.2. **Data controller:** means, "... a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed"

3.3. **Personal data**: means "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, email address, telephone number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

3.4. **Special Categories of Personal Data** means "personal data about an individual's:

- race;
- ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data (where this is used for identification purposes);
- health data;
- sex life; or
- sexual orientation"

4 Policy Statement

4.1. The Trust is committed to ensuring that it fully complies with the data protection principles of good practice within the Data Protection Act 2018 (including the UK General Data Protection Regulation), together referred to as Data Protection Law, when conducting its business, through adherence to robust procedures and the provision of guidance and training. It is also committed to ensuring accountability by demonstrating its complicance.

5 Responsibilities

5.1. The Trust Board is accountable to its members and governors. The role of the Trust Board is to effectively lead and govern the organisation by undertaking three key roles:

- Formulating strategy for the organisation.
- Ensuring accountability by holding the organisation to account for the delivery of the strategy and through seeking assurance that systems of control are robust and reliable.
- Shaping a positive culture for the board and the organisation.

5.2. Responsibility for formulating data protection strategy for the organisation and for providing assurance that systems of control are robust and reliable has been delegated to the Executive Team.

The Chief Executive Officer (CEO) as the Accountable Officer for the Trust is therefore ultimately accountable to the Board for ensuring the Trust complies with legal and regulatory requirements and that it is meeting its strategic objectives in relation to data protection.

5.3. Responsibility for Data Protection compliance, including the associated strategy and the policies and procedures which support the delivery of that strategy within the Trust is delegated to the Executive Director who has been nominated to act as the Senior Information Risk Owner (SIRO).

5.4. Information Governance Working Group chaired by the SIRO is responsible for bringing data protection issues to the Executive Management Team, and the Trust Board as appropriate.

5.5. Responsibility for implementing Trust strategy, policy and procedures is delegated to designated personnel, including (but not limited to):

- **The Data Protection Officer (DPO)** – An individual appointed on the basis of their personal and professional qualities and their expert knowledge of data protection. The DPO will be independent, an expert in data protection, have a good understanding of the way the organisation operates, be adequately resourced, and report to the highest management level. The DPO's role is to monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the Information Commissioner's Office (ICO) and data subjects.

- **The Head of Information Governance** – An individual with responsibility for delivering the organisation's information governance strategy including data protection policy and procedures.

- **Information Asset Owners (IAO)** – Senior/responsible individuals involved in running the relevant business and appointed by the SIRO. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result, they can understand and address risks to the

information and ensure that information is fully used within the law for the public good. They provide assurance to the SIRO.

- **Information Asset Administrators** – Individuals who support IAO in their activities.

- **The Caldicott Guardian** - A senior person responsible for protecting the confidentiality of people's health and care information and making sure it is used properly. All NHS organisations and local authorities which provide social services must have a Caldicott Guardian.

- **The SIRO –** Is an executive director who has responsibility for information risk at Board level. As an executive who is familiar with information risks and their mitigations; including risk assessment methodology, the SIRO provides briefings and reports to the Board on matters of performance and assurance.

6 Arrangements

6.1. **Principle 1: 'lawfulness, fairness and transparency'**. *Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.*

6.2. **Lawfulness**

6.3. There is a requirement to ensure that all processing of personal data undertaken by the Trust is lawful. For processing to be lawful the Trust must be able to identify at least one 'lawful basis' as defined within data protection law that permits personal data to be processed. Data Protection law provides six options which depend on the purpose of any processing and the relationship with the individuals whose data is being processed.

6.4. As a public authority the Trust's functions and activities are set out in law. It is this which conveys 'official authority' onto the Trust to operate and act and provides a basis in law (a 'legal basis') for the Trust to undertake the majority of its activities, including those which require the processing of personal data. One of the lawful bases provided within data protection law specifically enables those with 'official authority' established in law to process personal data lawfully when carrying out their public functions and tasks. Where the Trust can identify it's 'official authority' in law to undertake an activity it will rely on the 'public task' lawful basis within data protection law to

ensure its processing of personal data is lawful. Where the Trust cannot identify a legal basis which provides the 'official authority' to act it will ensure an alternative lawful basis under data protection law is applicable.

6.5. Lawfulness also means that the Trust must not do anything with personal data which is unlawful in a more general sense. This includes statute and common law obligations, whether criminal or civil.

6.6. **Examples of processing activities which may be considered unlawful include those which result in:**

- A criminal offence being committed;
- A breach of a duty of confidentiality;
- The organisation exceeding its legal powers or exercising those powers improperly;
- An infringement of copyright;
- A breach of an enforceable contractual agreement;
- A breach of industry-specific legislation or regulations; or
- A breach of the Human Rights Act 1998.

6.7. **To ensure all processing of personal data remain lawful the Trust will ensure that:**

- Personal data is processed for one or more specified purposes;
- It has identified a basis in law to process the personal data;
- It is necessary to process the personal data for those purposes (i.e. it is reasonable, proportionate and the objective cannot be achieved by some other reasonable means);
- It can point to a clear and foreseeable legal basis for those purposes under UK law (whether in statute or common law); and
- It does not do anything generally unlawful with personal data.

6.8. **Fairness**

6.9. There is a requirement for the Trust to consider how any processing of personal data may affect the individuals concerned and to justify any adverse impact there may be.

6.10. The Trust will only handle people's data in ways that individuals would reasonably expect or will explain why any unexpected processing is justified.

6.11. The Trust will not deceive or mislead people when it collects their personal data.

6.12. **Transparency**

6.13. There is a requirement to be open and honest, and to inform the general public, those who use NHS services, staff members and any other individual whose personal data is processed of the reasons why the Trust needs information about them, how this is used and to whom it may be disclosed. This must be provided in a way that is easily accessible and easy to understand using clear and plain language.

6.14. The Trust will adopt a layered approach to transparency using a variety of communication methods to ensure its processing of personal data is transparent. This will include:

- A Privacy Notice published on the Trust website;
- Information published on the Trust website;
- Information published on the Trust intranet;
- Information posters and leaflets provided or available in hard copy and on the Trust website and intranet;
- Verbal information provided directly to individuals by relevant staff members;
- Direct communications via letter, email and SMS messages.

6.15. **Principle 2: 'Purpose Limitation'.** *Personal data shall 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.*

6.16. To ensure the Trust complies with the 'purpose limitation' principle it will:

- Be clear from the outset why personal data is being collected and what it intends to do with it;
- Comply with its documentation obligations to specify its purposes for processing;
- Comply with its transparency obligations to inform individuals about its purposes for processing; and
- Ensure that if it plans to use or disclose personal data for any purpose that is additional to or different from the originally specified purpose, the new use is fair, lawful, and transparent.

6.17. The Trust will be clear about what purposes personal data will be processed for from the start. Specifying purposes of processing from the outset is necessary to comply with the Trust's accountability obligations and helps avoid 'function creep'. It also helps individuals understand how the Trust uses their data, make decisions about whether they are happy to share their details, and assert their rights over data where appropriate. Being clear about why the Trust is processing personal data will help ensure all processing is fair, lawful, and transparent. This is fundamental to building public trust in how the Trust uses personal data.

6.18. The Trust will record its purposes of processing as part of its documentation obligations and specify them within the privacy information developed for and provided to individuals. This will be recorded as part of the Trust's records of processing (documentation) and will be specified within privacy information provided to individuals.

6.19. The Trust will only use the personal data it holds for a new purpose if either this is compatible with the original purpose, consent is obtained, or there is a clear obligation or function set out in law - for example, a new function the Trust is required to perform as a public authority.

6.20. The Trust will consider the following to be compatible purposes:

- Archiving purposes in the public interest;
- Scientific or historical research purposes; and
- Statistical purposes.

6.21. For all other purposes the Trust will confirm that these are not incompatible with the original purpose taking into account:

- Any link between the original purpose and the new purpose.
- The context in which the personal data was originally collected - in particular, the relationship with the individual and what they would reasonably expect;
- The nature of the personal data – for example whether it is particularly sensitive.
- The possible consequences for individuals of the new processing; and
- Whether there are appropriate safeguards – for example encryption or pseudonymisation.

6.22. **Principle 3: 'Data Minimisation'.** *Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.*

6.23. The Trust will ensure that the personal data it processes is:

- Adequate - sufficient to properly fulfil the stated purpose;
- Relevant - has a rational link to that purpose; and
- Limited to what is necessary – only the minimum amount of personal data needed for the purpose will be processed.

6.24. Where the purposes of processing have been clearly determined the Trust will identify the minimum amount of personal data needed to fulfil each purpose. Where relevant and appropriate this will be considered separately for each individual, or for each group of individuals that share relevant characteristics.

6.25. The Trust will periodically review its processing to check that the personal data held is still relevant and adequate for its purposes and delete anything which is no longer needed, or revise data collection processes if personal data is deemed to be inadequate. When periodically reviewing the adequacy and relevance of the personal data held the Trust will consider any specific factors that an individual has brought to its attention – for example, as part of an objection, request for rectification of incomplete data, or request for erasure of unnecessary data.

6.26. The Trust will minimise the duplication of personal data and records (e.g. across multiple electronic or paper-based record keeping systems or through the use of 'convenience copies' of data or records held outside of primary record keeping systems).

6.27. **Principle 4: 'Accuracy'.** *Personal data shall 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.*

6.28. **The Trust will:**

- Take all reasonable steps to ensure the personal data held is not incorrect or misleading as to any matter of fact;
- Keep personal data updated where this is necessary and appropriate based on the purposes for which the data is used;
- Take reasonable steps to correct or erase personal data as soon as possible if this is discovered to be incorrect or misleading; and
- Carefully consider any challenges to the accuracy of personal data.

6.29. **To support the accuracy of information the Trust will:**

- Accurately record the information provided;
- Accurately record the source of the information;
- Take reasonable steps in the circumstances to ensure the accuracy of the information, for example through the creation of contemporaneous records, use of electronic data transfer interfaces to minimise the risk of transcription errors, the use of validation routines built into data collection or recording processes and the use of auditing processes to ensure the effectiveness of the controls;
- Carefully consider any challenges to the accuracy of the information; and
- Consider whether it is necessary to periodically update the information.

6.30. **Principle 5: 'Storage Limitation'.** *Personal data shall 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 UK GDPR in order to safeguard the rights and freedoms of individuals.

6.31. The Trust will:

- Maintain a record of the personal data it holds and why it is needed;
- Carefully consider and justify how long personal data needs to be retained which take account of the purposes for which the personal data is being processed;
- Take account of the NHSx Records Management Code of Practice 2021 when setting retention periods and adopt the standard retention periods this sets wherever possible;
- Not keep personal data for longer than required.
- Periodically review the data held and erase or anonymise it when it is no longer needed;
- Carefully consider any challenges to the retention of data and maintain appropriate processes to comply with individuals' requests for erasure under 'the right to be forgotten'; and
- Clearly identify any personal data that needs to be keep for public interest archiving, scientific or historical research, or statistical purposes and ensure this is retained subject to appropriate safeguards.

6.32. You can keep personal data for longer if you are only keeping it for public interest archiving, scientific or historical research, or statistical purposes.

6.33. Holding more personal data than needed is inefficient and there may be unnecessary costs associated with storage and security. Ensuring that personal data is erased or anonymised when it is no longer needed will also reduce the risk that it becomes irrelevant, excessive, inaccurate, or out of date. It will help the Trust to comply with the data minimisation and accuracy principles and reduce the risk that you will use such data in error to the detriment of all concerned as well as reducing the burden of dealing with request for information (e.g., by data subjects as part of a Data Subject Access Request or under

Freedom of Information), queries about retention and individual requests for erasure.

6.34. **Principle 6: 'Integrity and Confidentiality' (Security).** Personal data shall 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.

6.35. **The Trust will:**

- Process personal data securely by implementing appropriate technical and organisational measures which ensure the confidentiality, integrity and availability of the personal data it processes;
- Adopt a data protection by design and by default approach to all data processing activities and undertake an analysis of the risks presented by processing to assess the appropriate level of security we need to put in place;
- Take account of the state of the art and costs of implementation when deciding what measures to implement;
- Maintain policies and procedures which ensure information security controls are in place and take steps to make sure they are implemented;
- Regularly review information security policies, procedures and measures and, where necessary, improve them;
- Maintain a Data Security and Protection Toolkit submission to evidence technical and organisational controls.
- Implement privacy enhancing security measures such as encryption, pseudonymisation and anonymisation where it is appropriate to do so;
- Maintain business continuity and disaster recovery processes which ensure that access to personal data can be restored in the event of any incidents;
- Conduct regular testing and reviews of security measures to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement;

- Ensure that any data processor engaged to process personal data on its behalf also implements appropriate technical and organisational measures.

6.36. **The technical and organisational measures the Trust will adopt to ensure the security of personal data will seek to ensure that:**

- The data can be accessed, altered, disclosed or deleted only by those who have been authorised to do so (and that those people only act within the scope of the authority given to them);
- The data held is accurate and complete in relation to the purposes for which they are processed; and
- The data remains accessible and usable such that if personal data is accidentally lost, altered, or destroyed, it can be recovered in such a way as to prevent any damage or distress to the individuals concerned.

6.37. The Trust will ensure that both physical and computer/IT (cyber) security measures are considered and applied as necessary. Examples of the factors which will be considered include (but are not limited to):

6.38. **Physical security measures:**

- The quality of doors and locks, and the protection of premises by such means as alarms, security lighting or CCTV;
- Access controls to premises and how visitors are supervised;
- Secure disposal of paper and electronic waste; and
- Security measures to secure IT equipment, particularly mobile devices.

6.39. **Cybersecurity measures:**

- System security - the security of networks and information systems, including those which process personal data;
- Data security - the security of the data held within your systems, e.g., ensuring appropriate access controls are in place and that data is held securely;
- Online security - e.g., the security of websites and any other online service or application that are uses; and

- Device security - including mobile device management and the authorised or appropriate use of personal devices.

6.40. Where the Trust engages any organisation to process personal data on its behalf these will be classed as a data processor under data protection law. As the data controller the Trust will remain responsible for ensuring compliance with data protection law and this includes what any processor does with the data. To suitably protect personal data processed by any data processor the Trust will:

- Only choose data processors that can provide sufficient guarantees about their security measures;
- Engage data processors under a written contract which stipulates that the processor will implement the same or equivalent security measures that the Trust would employ if it were doing the processing itself; and
- Ensure that the contract includes a requirement that the processor makes available all information necessary to demonstrate compliance such as allowing for audits and inspections by the Trust or an authorised third party.

6.41. The Trust will ensure that anyone acting under its authority with access to personal data will only process that data where they have been instructed or authorised to do so. It is therefore vital that staff and other personnel understand the importance of protecting personal data, are familiar with organisational policies and procedures relating to data security and protection and put these into practice. To achieve this the Trust will ensure that:

- All contracts of employment will include a data protection and general confidentiality clause;
- Agency and non-contract staff working on behalf of the Trust will be subject to the same data protection and confidentiality obligations;
- Appropriate initial and refresher training is provided to all staff and other personnel acting under the authority of the Trust;
- Breaches of data protection law, confidentiality, contracts, Trust policy or procedures by those acting under the authority of the Trust will be fully investigated and may result in disciplinary action in accordance with Trust policy or the application of contractual sanctions as appropriate.

6.42. **Accountability**. The controller shall be responsible for and be able to demonstrate compliance with the data protection principles.

6.43. The accountability principle requires the Trust to take responsibility for what it does with personal data and how it complies with the other principles.

6.44. The Trust will appoint a Data Protection Officer (DPO) to monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs), act as a contact point for data subjects and the Information Commissioner's Office (ICO). The DPO will be independent, an expert in data protection, adequately resourced, and report to the highest management level.

6.45. The Trust will maintain appropriate measures and records to ensure it is able to demonstrate compliance with the data protection principles. These will include (but not limited to):

- Maintaining a current registration with the Information Commissioner's Officer (ICO) in accordance with the requirements of the UK Data Protection (Charges and Information) Regulation and Data Protection legislation.
- Policies and procedures;
- Transparency materials including a Privacy Notice;
- Records of processing activities which include:
    - The purposes of your processing;
    - A description of the categories of individuals and categories of personal data;
    - The categories of recipients of personal data.
    - Details of any transfers to third countries including documenting the transfer mechanism safeguards in place;
    - Retention schedules; and
    - A description of the technical and organisational security measures.
    - Records of consent (where this is the lawful basis relied upon to process personal data);
    - Data Protection Impact Assessments (DPIAs);
    - Employment Contracts;
    - Controller-Processor Contracts;
    - Controller-Controller Information Sharing Agreements and Joint Data Controller Agreements;
    - An annual satisfactory Data Security and Protection Toolkit submission;

- Training records; and
- Records of data breaches and near misses.

6.46. To ensure accountability and responsibility for the management and security of data is maintained the Trust will operate an Information Risk Management Framework headed by a Senior Information Risk Owner (SIRO). This will ensure that responsibility for information risk, including security, is formally assigned to appropriate individuals (Information Asset Owners) who will be accountable to the SIRO.

7 Data Subject Rights

7.1. Data protection law aims to protect the fundamental rights and freedoms of individuals and in particular their right to the protection of personal data. Where personal data is being processed, data protection law requires the Trust to uphold the following rights which are granted to the subjects of the personal data which is being processed (the data subject):

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object

7.2. To uphold data subject rights the Trust will maintain procedures which ensure data subject rights requests can be effectively recognised and responded to in accordance with the requirements of data protection law.

7.3. Although data protection law is limited to living individuals and does not extend to deceased individuals, the Access to Health Records Act 1990 provides access rights to personal representatives, or those who may have a claim arising from the individual's death, to deceased patients' records. The Trust will ensure that data subjects rights procedures which uphold the right of access (Subject Access Requests – SARs) extend to cover requests for information relating to deceased individuals.

8 Complaints

8.1. The Trust's complaints' procedures take account of complaints that may be received because of a breach or suspected breach of the Data Protection law.

9 Compensation

9.1. Individuals have a right to seek compensation for any breach of data protection legislation that may cause them damage and/ or distress.

10 Competence

10.1. All staff are required to complete Data Protection and Cyber Security Awareness training which covers data protection and cyber security as part of their induction on joining the Trust's employment and to undertake Statutory and Mandatory training on an annual basis through completing the training modules within SECAmb.

10.2. The Trust will offer more specialised in-house training on data protection to those whose role indicates that this is required. The Information Governance Working Group is expected to provide expertise in the application of the Data Protection legislation and will be able to provide advice and guidance.

10.3. A register will be maintained of all staff attendance at the training sessions. Non-contract staff and those on short or fixed term contracts will also receive appropriate induction.

11 Monitoring

11.1. The Information Governance Working Group is alerted to pertinent data protection issues or near misses through the incident reporting and formal reports issued by the Head of Information Governance.

12 Audit and Review

12.1. This policy will be reviewed every two years or more frequently if appropriate, by the Information Governance Working Group to take into account changes to national legislation that may occur, and/ or guidance from the Department of Health, the Information Commissioner and/ or any relevant case law.

12.2. When deemed appropriate, the Trust may commission internal audit to review compliance with these arrangements.

13 Equality Impact Appraisal

13.1. The Trust will undertake an Equality Impact Appraisal to determine whether any groups may be adversely affected by this policy; and if so, how this impact may be mitigated.

14 References

14.1. Primary Legislation

- Access to Health Records Act 1990
- Access to Medical Reports Act 1988
- Caldicott Principles
- Children Act 1989
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Crime & Disorder Act 1998
- Data Protection Act 2018
- UK General Data Protection Regulation
- Common Law Duty of Confidentiality
- Electronic Communications Act 2000
- Freedom of Information Act 2000
- Health and Social Care Act 2001
- Human Rights Act 1998
- Police and Criminal Evidence Act 1984
- Public Records Act 1958Regulation of Investigatory Powers Act 2000

14.2. Secondary Legislation

- The Data Protection (Processing of Sensitive Personal Data) Order 2000 [SI 2000 No. 417]
- The Data Protection (Subject Access Modification) (Health) Order 2000 [SI 2000 No. 413]

- The Data Protection (Subject Access Modification) (Education) Order 2000 [SI 2000 No. 414]
- The Data Protection (Subject Access Modification) (Social Work) Order 2000 [SI 2000 No. 415]
- The Data Protection (Miscellaneous Subject Access Exemptions) Order 2000 [SI 2000 No. 419]
- The Data Protection (Miscellaneous Subject Access Exemptions (Amendment) Order 2000 [SI 2000 No. 1865]
- The Data Protection (Subject Access) (Fees and Miscellaneous Provisions) Regulations 2000 [SI 2000 No. 191]

14.3. **NHS and Related Guidance**

- Confidentiality: NHS Code of Practice (August 2003)
- Employee Code of Practice (Information Commissioner)
- HSC2000/009: Data Protection Act 2018: Protection and Use of Patient Information
- HSC1999/053: For the Record (preservation, retention, and destruction of records under the Public Records Act 1958) and records management strategy
- HSC2002/3: Implementing the Caldicott Standard into Social Care
- BS7799: British Standard for Information Management and Technology.

Appendix 1: Overview of Legislation and NHS Guidance

1. Data Protection Act 2018 (DPA 18) / UK General Data Protection Regulation (UK GDPR)

The above are the key pieces of legislation and are therefore covered in detail. Summaries of other Acts mentioned above are shown at Appendix 2.

The Data Protection Act 2018 is an update to the former Data Protection Act 1998 and was implemented on the 25 May 2018. It is the UK's interpretation of the European wide General Data Protection Regulation 2016.

Following the UK's departure from the European Union (Brexit) the GDPR was incorporated into UK law to become the UK GDPR and is now implemented as part of the Data Protection Act 2018. Together they are referred to as 'data protection law'.

Data protection law applies to 'controllers' and 'processors'.

A controller determines the purposes and means of processing personal data.

A processor is responsible for processing personal data on behalf of a controller.

Data protection law applies to processing carried out by organisations operating within the UK.

Data Protection law does not apply to certain activities including processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/household activities.

Data Protection law applies to the processing of personal data that is:

- wholly or partly by automated means; or
- the processing other than by automated means of personal data which forms part of, or is intended to form part of, a filing system.
- personal data only includes information relating to natural persons who:
    - can be identified or who are identifiable, directly from the information in question; or who can be indirectly identified from that information in combination with other information.
    - personal data may also include special categories of personal data or criminal conviction and offences data. These are

considered to be more sensitive, and you may only process them in more limited circumstances.

- Pseudonymised data can help reduce privacy risks by making it more difficult to identify individuals, but it is still personal data.
- If personal data can be truly anonymised, then the anonymised data is not subject to the Data Protection Act 2018 or the UK GDPR. It is important to understand what personal data is in order to understand if the data has been anonymised.
- Information about a deceased person does not constitute personal data and therefore is not subject to the UK GDPR.
- Information about companies or public authorities is not personal data.
- However, information about individuals acting as sole traders, employees, partners, and company directors where they are individually identifiable, and the information relates to them as an individual may constitute personal data.

1 NHS and Related Guidance

1.1. Confidentiality: NHS Code of Practice

1.1.1. This provides detailed guidance for NHS bodies concerning confidentiality and patients' consent to use their health information. It also details the required practice the NHS must take concerning security, identifying the main legal responsibilities for an organisation and also details employees' responsibilities (www.dh.gov.uk).

1.2. Employee Code of Practice

1.2.1. This is guidance produced by the Information Commissioner detailing the data protection requirements that relate to staff/ employee and other individuals' information www.ico.gov.uk.

1.2.2. NHSx Records Management Code of Practice 2021

1.2.3. Provides guidance to improve the management of NHS records, explains the requirements to select records for permanent preservation, lists suggested minimum requirements for records retention and applies to all information, regardless of the media, applicable to all personnel within the NHS such as patients, employees, volunteers etc. It aids compliance with the Data

Protection and Freedom of Information Acts (www.dh.gov.uk search by circular details).

1.3. **ISO/IEC 17799 Information Security Standards**

1.3.1. This is the accepted industry standard for Information Management and Security. This standard has been adopted by all NHS organisations. It is also a recommended legal requirement under the Data Protection Act 2018.

Appendix 2: Other Relevant Acts of Parliament

1 Access to Health Records 1990

1.1. This Act gives patients' representatives right of access to their manually held health records, in respect of information recorded on or after 1 November 1991. This Act is only applicable for access to deceased persons' records. All other requests for access to information by living individuals are handled under the access provisions of the Data Protection Act 1998.

2 Access to Medical Reports Act 1988

2.1. This Act allows those who have had a medical report produced for the purposes of employment and/ or insurance to obtain a copy of the content of the report prior to it being disclosed to any potential employer and/ or prospective insurance company.

3 Human Rights Act 1998

3.1. This Act became law on 2 October 2000. It binds public authorities, including all Trusts and individual doctors treating NHS patients, to respect and protect an individual's human rights. This will include an individual's right to privacy (under Article 8) and their right to expect confidentiality of their information at all times.

3.2. Article 8 of the Act provides that 'everyone has the right to respect for his private and family life, his home and his correspondence'. However, this article also states 'there shall be no interference by a public authority with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'.

3.3. Each organisation must act in a way consistent with these requirements. It must take an individual's rights into account when sharing personal information about them.

4 Freedom of Information Act 2000

4.1. This Act came into force on 1 January 2005. It gives individuals right of access to corporate information held by the Trust such as policies, reports, and minutes of meetings. The Trust has a Freedom of Information Policy and a nominated officer to deal with requests and queries.

5 Regulation of Investigatory Powers Act 2000

5.1. This Act combines rules relating to access to protected electronic information as well as revising the 'Interception of Communications Act 1985'. The Act aims to modernise the legal regulation of interception of communications in the light of the Human Rights laws and rapidly changing technology.

6 Crime and Disorder Act 1998

6.1. This Act introduces measures to reduce crime and disorder, including the introduction of local crime partnerships around local authority boundaries to formulate and implement strategies for reducing crime and disorder in that local area.

6.2. The Act allows disclosure of person identifiable information to the Police, Local Authorities, Probation Service or the Health Service but only if the purposes are defined within the Crime and Disorder Act. The Act does not impose a legal requirement to disclose/ exchange person identifiable information and responsibility for disclosure rests with the organisation holding the information. There must be a Crime and Disorder Protocol governing the disclosure/ exchange and use of personal information within a local authority boundary agreed and signed by all involved agencies and organisations.

7 The Computer Misuse Act 1990

7.1. This Act makes it a criminal offence to access any part of a computer system, programs and/ or data that a user is not entitled to access. Each organisation will issue users an individual user id and password which will only be known by the individual they relate to and must not be divulged/ misused by other staff. This is to protect the employee from the likelihood of their inadvertently contravening this Act.

7.2. Each organisation will adhere to the requirements of the Computer Misuse Act 1990 by ensuring staff are made aware of their responsibilities regarding the misuse of computers for personal gain or other fraudulent activities. Any member of staff found to have contravened this Act will be considered to have committed a disciplinary offence and be dealt with accordingly.

Appendix 3: Disclosure of Personal Patient Information

1 Acts of Parliament that govern the disclosure / sharing of personal patient information are detailed below:

- **Legislation to restrict disclosure of personal identifiable information**
- Human Fertilisation and Embryology (Disclosure of Information) Act 1992
- Venereal Diseases Act 1917 and Venereal Diseases Regulations of 1974 and 1992
- Abortion Act 1967
- The Adoption Act 1976
- **Legislation requiring disclosure of personal identifiable information**
- Public Health (Control of Diseases) Act 1984 & Public Health (Infectious Diseases) Regulations 1985
- Education Act 1944 (for immunisations and vaccinations to NHS Trusts from schools)
- Births and Deaths Act 1984
- Police and Criminal Evidence Act 1984
- Sometimes a request may be received for patient information as part of a research project. Any such request would need to be assessed against requirements in the Data Protection Act 2018. In most circumstances it will be necessary to have any research proposal approved by the Local Research Ethics Committee (LREC). It is also necessary to obtain the patient's consent prior to using information for research purposes.