Data Protection & Personal Information Handling Policy

Version No. 9 : April 2023

First Issued: October 2016
Review date: April 2025

Contents

*(For quick access to a specific heading - **press CTRL and click your mouse** to follow the link for the below options)*

1. INTRODUCTION

The appropriate and secure handling of personal information about living individuals is a requirement of law, and also of NHS policy. The introduction of the General Data Protection Regulations (GDPR) in May 2018 introduced enhanced controls and protections for personal information which apply to all organisations. For ECCH there are additional requirements due to the confidential and sensitive nature of the information that is processed in the normal course of service delivery.

1Additionally, the NHS has in place requirements for the handling of Confidential Patient-Identifiable Information, that were outlined in the Caldicott Report of 1997, the recommendations of which have subsequently been implemented within all NHS Organisations and are known as the Caldicott Principles. Caldicott operates alongside and in addition to specific guidance and requirements of professional codes of conduct, such as the NHS Confidentiality Code of Practice.

In addition to these, the Common Law Duty of Confidentiality also places requirements on those who receive and use confidential information.

2. PURPOSE

The purpose of this policy is to provide employees and workers of ECCH with guidance as to the correct and lawful processing of information.

To ensure that all employees and workers of ECCH are aware of their legal and contractual obligations in terms of data protection.

This policy applies to personal information of both patients/clients of ECCH and its contracted service providers, and to personal information of employees and workers of ECCH.

3. SCOPE

This policy applies to any substantive/temporary employees and any contractor, agency, student, honorary and volunteer worker, where work is performed on behalf of ECCH.

4. DEFINITIONS

The following definitions are intended to provide a brief explanation of the various terms used within this policy.

Term	Definition
Policy	A policy is a formal written statement detailing an enforceable set of principles or rules. Policies set the boundaries within which we operate. They also reflect the philosophy of our organisation.
Data Protection Act (DPA)	The Data Protection Act 2018 controls how your personal information is used by organisations, businesses or the government. The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).
General Data Protection Regulation (GDPR)	The General Data Protection Regulation 2016/679 is a regulation in EU law on data protection and privacy in the European Union and the European Economic Area.
TPP	TPP is a healthcare technology company, dedicated to delivering world class healthcare software in the UK and internationally. TPP provides the SystmOne patient record keeping system to ECCH.
Personal Identifiable Information (PII)	Personally identifiable information is any data that can be used to identify a specific individual.
Sensitive Person Information	Any information relating to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life and criminal convictions.
Pseudonymisation	The process of replacing person identifiers in a dataset with other values (pseudonyms) from which the identities of individuals cannot be intrinsically inferred. Examples of this process are replacing an NHS number with another random number, replacing a name with a code or replacing an address with a location code.
Data Subject	An individual who is the subject of personal data / information.
Subject Access Request (SAR)	A subject access request (SAR) is a written request made by or on behalf of an individual for the information which they are entitled to ask for.
Accessible Record	(a) A health record. (b) An educational record. (c) An accessible public record. A health record is defined as; "any record which consists of information relating to the physical or mental health or condition and an individual, and has been made by or on behalf of a health professional in connection with the care of that individual".
Processing	Processing in relation to personal information means;

	obtaining, recording, holding or deleting information.
Data Controller	A person who either alone, 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.
Data Processor	Any person, other than an employee of the data controller, who processes information on behalf of the data
Third Party	Any person other than; (a) the data subject, (b) the data controller or (a) any data processor or other person authorised to process data for the data controller or processor.
Caldicott Principles	The Caldicott Principles are fundamentals that organisations should follow to protect any information that could identify a patient, such as their name and their records. They also ensure that this information is only used and shared when it is appropriate to do so.
Caldicott Guardian	The Caldicott Guardian is senior person responsible for protecting the confidentiality of personal confidential data and information. The Caldicott Guardian plays a key role in ensuring that ECCH and partner organisations abide by the highest level of standards for handling personal information and personal identifiable information.
Senior Information Risk Owner (SIRO)	The Senior Information Risk Owner (SIRO) on behalf of the Board. The SIRO owns the information risk and incident management framework, overall information risk approach and risk assessment processes, and is responsible for ensuring they are implemented consistently.
Data Protection Officer (DPO)	The Data Protection Officer is a legal role required by the GDPR. This person is responsible for overseeing the Information Governance (IG) Policy and Framework and the implementation of data protection and security measures to ensure compliance with the GDPR requirements; these measures should ultimately minimise the risk of breaches and uphold the protection of PII and special categories of data.

5. RESPONSIBILITIES

- **Chief Executive of ECCH –** Overall responsibility for the enforcement of this policy lies with the Chief Executive of ECCH. It is the responsibility of the Chief Executive to implement the policy within ECCH, and take appropriate action where misuse is discovered.

- **ECCH Employees –** Every employee and worker of ECCH is responsible for the implementation of this policy and following the requirements of the policy whilst processing personal-identifiable information**.**

- **ECCH Information Governance and Caldicott Group –** it is the responsibility of ECCH Information Governance and Caldicott Group overseen by the Integrated Governance Committee (IGC) to monitor the overall implementation of the policy on behalf of ECCH.

- **Data Protection Officer -** it is the responsibility of ECCH Data Protection Officer to maintain the policy, reviewing it on a regular basis or following any major organisational or legislation changes, to ensure that it remains applicable.

- **Senior Information Risk Owner (SIRO)** - it is the responsibility of Senior Information Risk Owner (SIRO) who will act as an advocate for information risk on ECCH's Board and will provide written advice on the content of the Statement of Internal Control with regard to information risk.

- **Head of IT – i**t is the responsibility of the Head of IT for implementing the IT security requirements of the organisation.

- **Caldicott Guardian - i**t is the responsibility of the Caldicott Guardian to protect the confidentiality of personal confidential data and information

6. POLICY STATEMENT

East Coast Community Healthcare regard the lawful and correct treatment of personal information as very important to successful operations, and to maintain confidence between those whom the Organisations deal with and themselves. East Coast Community Healthcare (ECCH) will ensure that information is treated lawfully and correctly, in accordance with the requirements of the GDPR, Caldicott, Common Law Duty and related NHS guidance.

ECCH will specifically ensure that:

1. Personal information is processed fairly and lawfully and shall not be processed unless the specific conditions of the GDPR are met.

2. Personal information shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with the purpose(s).

3. Personal information is adequate, relevant and not excessive in relation to the purpose(s) for which they are processed.

4. Personal information will be accurate and where necessary, kept up to date.

5. Personal information will not be kept for any longer than is necessary for the purpose or as is required by statute and NHS guidance

6. Personal information will be processed in accordance with the rights of the Data Subject.

7. That appropriate technical and organisational measures have been implemented to protect information against unauthorised or unlawful processing, accidental loss or destruction of or damage to personal information.

8. Personal information will not be transferred to a country or territory outside the European Union without the express consent of the Data Subject.

9. That patient-identifiable information is handled in accordance with the Caldicott Principles and the NHS Confidentiality Code of Practice.

In addition to the above, ECCH will ensure that:

1. An individual is identified with specific responsibility for Data Protection.

2. That all employees of ECCH and contractors, agency, student, honorary and volunteer workers, who manage or handle personal information are aware of the requirements of GDPR, and that they are contractually responsible for adhering to the Data Protection Principles, Caldicott and Common Law requirements for confidentiality and following good data protection practice.

3. That all employees and workers who manage or handle personal information are appropriately trained to do so and receive appropriate supervision.

4. That all data subjects about whom ECCH processes information are aware of how and to whom, to make a request to access their records.

5. That queries regarding data protection or the handling of personal information within the organisation are dealt with promptly and courteously.

6. That methods of handling personal information are clearly described in procedures relevant to the area(s) in which personal information is held and processed.

That regular audits are undertaken reviewing the way that personal information is managed within the organisation and that methods of information handling are regularly assessed and evaluated.

7. PROCEDURE

GENERAL DATA PROTECTION REGULATION (GDPR)

GDPR replaces the Data Protection Act 1998 and is designed to strengthen individual rights regarding the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information.

GDPR gives protection to individuals about whom data is recorded either manually or electronically. Any individual has the right to see what information is held about them and may challenge this information if they feel it is inaccurate or has caused damage to them.

GDPR places obligations on those who record and use information about individuals. They must register the use of that information (through the Information Commissioner) and they must ensure that they follow sound practices in recording and using the information, in line with the Data Protection Principles.

In addition to information that is processed automatically i.e. any information that is held on computers, the regulations also cover any structured set of manual information that references individuals or criteria relating to individuals in such a way that specific information relating to a particular individual is easily accessible.

GDPR therefore now covers all information that is recorded about individuals by employees of ECCH, and entered into a paper record, either clinical or non-clinical

GDPR PRINCIPLES

GDPR states that all Data Controllers and Data Processors must comply with the six data protection principles. Therefore ECCH must adhere to the following:

Personal data shall be:

1) Processed lawfully, fairly and in a transparent manner in relation to individuals

2) 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 purpose

3) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

4) 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

5) 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 or statistical purposes subject to implementation of the appropriate technical and organisational measures required by GDPR in order to safeguard the rights and freedoms of individuals

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

INFORMATION PROVIDED TO DATA SUBJECTS

GDPR requires that information regarding the nature of the information collected and its uses within ECCH is communicated to the individuals to whom the data relates. This is known as the 'Fair Processing' of information.

ECCH will ensure that the following minimum information is communicated to the individuals to whom the data they hold relates:

- The identity of the Data Controller.
- The identity of ECCH's nominated representatives, usually the Data Protection Officer.
- The purpose or purposes for which personal information is processed.
- Potential disclosures of personal information and who information may be disclosed to.
- Any further information, which is necessary to make the processing fair.

RIGHTS OF THE DATA SUBJECT

ECCH will ensure that personal information is handled in accordance with the rights of the Data Subject as defined by the legislation.

GDPR requires that information be processed in accordance with the rights of the Data Subject. Data subjects have the following rights in respect of the processing of their personal information:

1) The right to be informed
2) The right of access

3) The right to rectification
4) The right to erasure
5) The right to restrict processing
6) The right to data portability
7) The right to object
8) Rights in relation to automated decision making and profiling

SUBJECT ACCESS REQUESTS

ECCH may receive requests for subject access from a data subject or their legal representative. In all cases an access request must be dealt with within one month of receiving the request. (For advice and guidance please consult the either ECCH's Access to Health Records Policy or the Data Protection Officer)

CALDICOTT PRINCIPLES

The Caldicott Principles were first introduced by the 1997 Caldicott Report into the uses of patient-identifiable information within the NHS. The principles it devised are to ensure that access to and use of personal information is restricted to justifiable purposes and to authorised staff.

The current Caldicott Principles are:

1. Justify the purpose(s).
2. Don't use patient identifiable information unless it is absolutely necessary.
3. Use the minimum amount of patient identifiable information.
4. Access to patient-identifiable information should be on a strict need to know basis.
5. Everyone should be aware of his or her 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.
8. Inform patients and service users about how their confidential information is used

Caldicott also requires the establishment of *Information Sharing Protocols* to govern the sharing or patient information between partner organisations. This is to

ensure that each organisation receiving information will handle and protect that information in a similar way.

COMMON LAW DUTY OF CONFIDENTIALITY

Personal information given or received in confidence for one purpose may not be used for a different purpose or passed to anyone else without the consent of the provider of the information. This duty of confidence is long established in common law.

The Department of Health's guidance to the NHS is that, with proper safeguards, the duty of confidence need not be construed so rigidly that, when applied to NHS or related services, there is a risk of it operating to the disadvantage of a patient or to the public generally.

HANDLING PERSONAL INFORMATION

All employees and workers of ECCH, must ensure that they follow the data protection principles at all times when handling personal information.

Personal information collected by staff in the course of their duties must not be communicated to other persons or bodies unless required to do so by law, or to meet the requirements of the registered purposes of ECCH, or with the explicit consent of the individual concerned.

Any disclosures of information made by staff must be consistent with the Organisations registration under the GDPR, Caldicott requirements and Common Law Duty of Confidentiality.

It is the responsibility of all staff to ensure that:

- Appropriate measures are taken to prevent personal information from being accidentally disclosed to unauthorised persons, for example by the implementation of 'Clear Desk' or 'Clear Screen' policies.

- Appropriate care is taken in the storage and disposal of personal information held in whatever format. Personal data must be held securely and in confidence.

- Any guidance on handling personal information specific to your work area is followed in addition to the guidance in this policy.

- That any planned use of personal information that does not fall within the organisations data protection registration is notified to the individual within the organisation who has responsibility for data protection compliance.

- Personal data is only collected for the purposes identified within the organisations data protection registration.

- That they only access personal information of individuals where required to in connection with the duties they perform.

All personal information must be stored securely and access to the information restricted to only those personnel who require access as part of their duties. This is especially important in relation to any sensitive data held. Access to personal information that falls into this category as defined by the Act requires stricter access controls, to ensure that unauthorised access and disclosure is prevented.

Appropriate precautions must be taken when transporting personal information, both within and outside the organisation, to ensure that it is protected from unauthorised access, loss or destruction. The protection of information is the responsibility of the member of staff who is in possession of the information. Failure to take adequate measures to protect information may lead to disciplinary and or legal action being taken against the individual.

Where appropriate, personal information must be kept accurate and up to date. Personal information must not be modified or destroyed without the authorisation of the data owner.

The organisation must have in place up to date procedures to handle subject access requests made by individuals, or on the individual's behalf, to ensure that information is only disclosed to those who have a right to the information, and that the information is provided within one month of receiving the request as specified by the legislation.

ECCH must have in place procedures for dealing with requests to disclose personal information by other organisations not covered by the Information Sharing Protocols, and for dealing with requests for access by the courts. The procedures must detail what action staff are to take in these circumstances and also place specific arrangements on obtaining approval from ECCH's Caldicott Guardian prior to disclosure.

DISCLOSING PERSONAL INFORMATION

Extreme care must be taken to prevent the unauthorised disclosure of personal information by ensuring staff are aware of the implications of not positioning equipment carefully, using time-out and screen-blanking features, poor password management, not securing paper-based information in locked cases, filing cabinets or drawers and conducting sensitive telephone conversations away from a communal office environment.

When sharing personal information between departments or outside organisations e.g. Social Services, consent must be obtained from the data subject where appropriate. Refer to the Data Protection Officer for further guidance in this area.

USING PSEUDONYMISATION FOR PERSONAL INFORMATION

Pseudonymisation is a method which disguises the identity of patients by creating a pseudonym for each patient identifiable data item. The pseudonym must be constant for each record, that is generated and the same pseudonym used across all reporting. It must also be reversible so that the record can be linked back to the original record should that be necessary.

Pseudonymisation should be used when patient data is used by ECCH for secondary purposes (e.g. research, audit, reporting and service evaluation) not involving the direct care of the patient, the patient should not be identified unless other legal means hold, such as the patient consent. This ensures that personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Data items to be Pseudonymised - All data items (or combinations of Data items) that could be used to identify an individual are classed as Sensitive Personal Data and therefore must be removed, or anonymised, or pseudonymised. The data items in question are listed below:

- NHS Number(or other local system) ID – TPP provide pseudonymised alternative patient id, traceable through SystmOne reporting extracts only. Is pseudonymised by TPP by applying an algorithm in the data warehouse to create an alias for reporting.
- Name - To be removed from all reports.
- Address - To be removed from all reports.
- Postcode - Anonymised by removing the second part of the record. For example the Trust postcode NW3 5BA would become simply NW3.
- DOB - To be anonymised by converting to age at referral. For example, a DOB of 1/6/90 would be shown as age 21.
- GP Code - To be included as long as all the above have been actioned

Warehouse Data
Warehouse Data used for secondary purposes by the Business Intelligence (BI) Team will be pseudonymised and anonymised correctly as above, this makes certain patient confidentiality and privacy is maintained. Before any data is released the BI Team ensure strict rules and procedures are applied to the data in accordance with best practice and governance protocols.

Non-Warehouse Data:
Where the data is not recorded on SystmOne (and thus not available via the data warehouse), or provided via other systems, or is simply collated from clinical notes, the compiler of the data is responsible for ensuring that the data items above are suitably anonymised or pseudonymised.

Those responsible for such data should liaise with the DPO and BI Team who will ensure arrange for the data to be properly pseudonymised, ready for l distribution.

INCIDENTS & REPORTING

Incidents or any near miss that affects the confidentiality, integrity or availability of information, and lead to the unauthorised destruction, denial of access, disclosure or modification of information, must be reported as either a Serious Incident for any actual data loss or an Adverse Incident for any near misses. This will aid in improving awareness, eliminating poor practice and carelessness, rather than apportioning blame.

Details of any incidents or near miss must be reported via ECCH's Incident Reporting system and the Data Protection Officer notified, who will investigate and report to the Caldicott Guardian (for cases involving patient information).

GDPR introduced new requirements for reporting of incidents and a mandatory reporting timescale of 72 hours from the time the incident is identified. All staff must be aware of this requirement and ensure that incidents are promptly recorded in the incident recording system, and appropriately coded to identify them as relating to a breach of patient confidentiality.

8. MONITORING AND REVIEW

The Information Governance and Caldicott Group will have overall responsibility for overseeing the implementation of this policy and its associated procedural guidelines, taking forward any action relating to information governance and data protection within the Organisation.

9. REFERENCES

https://ico.org.uk/for-organisations/
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data/

10. ASSOCIATED POLICIES & PROCEDURES *(To include but not limited to)*

- Information Governance Policy& Framework
- Data Protection Impact Assessment (DPIA) Policy & Procedure
- Confidentiality Policy
- IG Handbook
- Incident Reporting Policy
- Serious Incident Reporting Policy
- Information Security Incident and Incident Investigation Policy

11. AUTHOR

Data Protection Officer

12. APPENDICES

Appendix 1. Conditions for Processing of Personal Data

1. Legal Basis

GDPR defines the following as legal basis for processing personal information of which at least one must apply:

A. Consent; the individual has given clear consent for you to process their personal data for a specific purpose.

B. Contract; the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

C. Legal obligation; the processing is necessary for you to comply with the law (not including contractual obligations).

D. Vital interests; the processing is necessary to protect someone's life.

E. Public task; 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.

F. Legitimate interests; the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

2. Special Category Data

GDPR specifies additional conditions that apply to the processing of special category data and it is necessary to meet both a legal basis condition *and* at least on special category condition for processing of special category data (which includes health information) to be legal. The conditions for processing special category data are:

A. The data subject has given explicit consent to the processing of those personal data for one or more specified purposes.

B. Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law.

C. Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.

D. Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for

profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.

E. Processing relates to personal data which are manifestly made public by the data subject.

F. Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

G. Processing is necessary for reasons of substantial public interest.

H. 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 and social care systems and services.

I. 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.

J. Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

3. Special Category Data

Special category data consists of the following:

(a) Racial or ethnic origin of the data subject
(b) Political opinions
(c) Religious beliefs or beliefs of a similar nature
(d) Trade union membership
(e) Genetics
(f) Biometrics (where used for ID purposes)
(g) Health
(h) Sexual life or
(i) Sexual orientation

13. EQUALITY & DIVERSITY IMPACT ASSESSMENT

In reviewing this policy, the Reviewer considered, as a minimum, the following questions:

- Are the aims of this policy clear?
- Are responsibilities clearly identified?
- Has the policy been reviewed to ascertain any potential discrimination?
- Are there any specific groups impacted upon?
- Is this impact positive or negative?
- Could any impact constitute unlawful discrimination?
- Are communication proposals adequate?
- Does training need to be given? If so is this planned?

Adverse impact has been considered for age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion and belief, sex, sexual orientation.

14. DOCUMENT CONTROL

Version Date	Version No.	Author/ Reviewer	Comments
April 2019	7	Heather Howman – DPO	No changes required
April 2021	7.1	Hannah Lewis – DPO	Added Caldicott Principle 8
April 2021	8	Hannah Lewis – DPO	• Added to updated policy template • Added reference table • Added section on **Pseudonymisation** • Added references and associated policies *(Sent for virtual review and comments to IG Caldicott Group*
April 2023	9	Hannah Sewell – DPO	Policy transferred to new template Replaced Datix references

DOCUMENT CONTROL SHEET

Name of Document:	Data Protection & Personal Information Handling Policy
Version:	No. 9
File Location / Document Name:	ECCHO – Intranet
Date Of This Version:	April 2023
Produced By (Designation):	Data Protection Officer
Reviewed By:	Information Governance & Caldicott Group
Synopsis And Outcomes Of Consultation Undertaken:	Changes relating to relevant committees/groups involved in ratification processes.
Synopsis And Outcomes Of Equality and Diversity Impact Assessment:	No adaptions required as document has no direct impact on specific groups listed in the Impact Assessment
Ratified By (Committee):-	Information Governance & Caldicott Group
Date Ratified:	April 2023
Distribute To:	ECCHO – Intranet
Date Due For Review:	April 2025
Enquiries To:	DPO
Approved by Appropriate Group/Committee	☐ Date: April 2023