Data Protection Policy

Author:	Information Governance Officer - Rachel Adams
Document Owner:	Trust Secretary and Director of Corporate compliance and Legal service - Sheila Murphy
Revision No:	8
Document ID Number	POLCGR007
Approved By:	Information Governance Group
Implementation Date:	May 2018
Date of Next Review:	April 2019

Data Protection Policy

Document Control / History	
Revision No	**Reason for change**
7	
8	Revised review date

Consultation
Information Governance Group members
Caldicott Guardian

Data Protection Policy

Table of Contents

Data Protection Policy

To be read in conjunction with any policies listed in Trust Associated Documents.

1 Introduction

1.1 For the purposes of the General Data Protection Regulation (**GDPR**) and the Data Protection 2018, Medway Foundation Trust (the **Trust**) acts as the data controller when obtaining and processing personal and special categories of personal data. A data controller is an organisation who determines the purposes for which, and the manner in which, personal data is to be processed. Such processing may be carried out jointly or in common with other organisations.

1.2 The Trust and its appointed data processors have a legal obligation to comply with all appropriate legislation with regard to processing personal data. They also should reflect guidance issued by the Department of Health, NHS England, advisory groups to the NHS and any guidance issued by professional bodies such as the Information Governance Alliance. A data processor is responsible for processing personal data on behalf of a controller.

1.3 All staff have a duty to patients and other staff to ensure that all the relevant statutory requirements that relate to this policy are complied with. The Trust expects all employees to comply with this policy and all Data Protection legislation in force from time to time.

1.4 Failure to comply with GDPR legislation can lead to enforcement action from the Information Commissioners Office (ICO), including monetary penalty notices, claims for compensation or even criminal prosecution. The ICO enforces and oversees the GDPR and the Freedom of Information Act 2000.

2 Purpose / Aim and Objective

2.1 The Trust must comply with its statutory obligations as laid down under the GDPR. The Act establishes seven principles (see Appendix 1) for which this policy provides a framework for the Trust to ensure compliance with GDPR.

2.2 This policy establishes how compliance with GDPR will be monitored and that Information Asset Owners (IAO) will provide the Senior Information Risk Officer (SIRO) with timely, reliable and fit for purpose information to meet reporting requirements, to support legislative and regulatory compliance and to assist management in decision making.

2.3 The GDPR requires all public authorities to appoint a Data Protection Officer (DPO). The role of the DPO is to assist the Trust in monitoring internal compliance, inform and advise the Trust on its Data Protection obligations, provide advice regarding Data Protection Impact Assessments (of a which a policy can be found via QPulse and will act as a contact point for data subjects and the supervisory authority e.g. ICO. The Trust has appointed the Trust Secretary and Director of Corporate compliance and Legal service as the DPO. Should you need to contact the DPO please email medwayft.dpo@nhs.net or 07788916897

2.4 Assurances will be provided to the Caldicott Guardian, DPO and Trust Board through reports produced by the Information Governance Team. These reports will promote openness and transparency on how the Trust is complying with statutory duties and deadlines, and highlight key areas of risk and non-compliance.

2.5 The Trust aims to 'Be the BEST' in everything it sets out to do, and this extends to embedding Information Governance (IG) at the heart of how it protects, manages and uses patient, staff and corporate data.

3 Definitions

3.1 **Data** – this is not defined under GDPR but the Regulation applies to the processing of personal data wholly or partly by automated means and to processing other than by automated means of data, which forms part of a filing system or which is intended to form part of a filing system. This can be in both written and electronic form

3.2 **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, 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 person.

3.3 **Special C**ategories of personal data - this was previously known as "sensitive data". To process this category of data the Trust is required to comply with one of the conditions set out in Article 9 of the GDPR. This includes processing personal data about someone's:

- Race and ethnicity
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Processing of genetic data and biometric data for the purpose of identification
- Health
- Sex life
- Sexual orientation

3.4 **Pseudonymisation** – the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

3.5 **Filing System –** means any structured set of personal data which is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

3.6 **European Economic Area (EEA) -** The member States of the European Union, together with Iceland, Liechtenstein, and Norway.

3.7 A '**health record**' is any record which consists of information relating to the physical or mental health or condition of an individual, and has been made by or on behalf of a

health professional in connection with the care of that individual. This can be processed and stored in manual or in electronic format and will also include genetic data as defined under GDPR.

This data includes material held in Trust systems, letters, emails and text messages, but also other media including an X-ray, MRI scan, photographs or video.

3.8 **Medical Purposes** information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test. (GDPR)

3.9 **NHS Organisations** all organisations providing health care services, including NHS trusts, NHS Foundation Trusts, general medical and dental practices, NHS commissioners.

3.10 **Data Controller** - means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by European Union law or the laws of a Member State, the controller or the specific criteria for its nomination may be provided for by Union or Member State law

- 'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
- 'Personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
- 'Filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

3.11 **Subject Access Request**:

- A request by an individual or third party for copies of information held by the Trust about a person. Requests can be made either in writing or orally. The Trust must reply to a valid request promptly and, at the latest, within one month. Any requests made orally must be documented.

- A person who asks for their personal information may require the Trust to search all Departments where such information may be held. It may be limited to health records or it may include administrative records (e.g. personnel, occupational health, financial).

- The information must be provided free of charge and no fee can be charged.

- If you consider the request to be manifestly unfounded or excessive or a repeated request there are two options available:

- You can request a "reasonable fee" to deal with the request, which should be based on the administrative costs of complying with the request; or
  - Refuse to deal with the request.

- If we decide to charge a fee we must notify the individual promptly.

  [http://www.medway.nhs.uk/about-the-trust/access-to-information/subject-access-requests/]

- In general, an individual may gain access to their personal data however it is held and whenever it was created provided it has not been destroyed in accordance with the retention periods applied by the Information Governance Alliance Records Management Code of Practice. This normally involves providing applicants with copies of their records. However if providing copies would disclose information about third parties which it would be unfair to disclose, the third party personal information may either be redacted or extracted or the applicant's information transposed to a new document in order to appropriately disclose the requester's information.
- Requesters must also be given a description of the data, a description of the purpose/s for which the data is being or is to be processed, and a description of those to whom the data is disclosed.
- In addition, requesters must also be given any information available to the controller about the source of the data, and an explanation of any automated decision taken about the data subject.

3.12 **Exemptions to complying with a** Subject **Access Request:**

The main exceptions to the obligation to respond to a data subject access request are:

- Where information is being or has been processed for scientific research and the results cannot identify the person.
- Where disclosing the personal data would reveal information about someone else who has not consented to that disclosure - where the third party would reasonably be expected to give consent to this disclosure, it can (in some cases) be presumed.
- Where permitting access to information about a person's physical or mental health or condition would be likely to cause serious harm to the physical or mental health or condition of that person or another individual.

- Where a request for information about a person's physical or mental health or condition is made by another person (such as the parent of a child), on behalf of the data subject, access can be refused if the data subject had:
  - either provided the information in the expectation it would not be disclosed, or
  - had indicated it should not be disclosed to the applicant;
  - or if the data was obtained as a result of an examination or investigation to which the data subject consented on the basis that information would not be so disclosed.

3.13 **Individual Rights under GDPR**

There are 8 rights which every individual has under GDPR in relation to their personal data:

- The right of access – this is exercised by a person making a Subject Access Request. For further information please contact medwayft.sars@nhs.net
- The right to be informed – this is provided using privacy notices. The Trust's privacy notices can be found here [https://www.medway.nhs.uk/about-us/privacy-policy.htm.
- The right to rectification – this allows individuals to have inaccurate personal data (a "statement of fact") rectified or completed if it is incomplete.
- The right to erasure – this allows individuals to have personal data erased, which rarely applies to the data held by the Trust. For further information please contact medwayft.dpo@nhs.net
- The right to restrict processing – this allows individuals to request to restrict or suppress their personal data. For further information please contact medwayft.dpo@nhs.net. The right to data portability – this allows individuals to obtain and reuse their personal data for their own purposes across different services. For further information please contact medwayft.dpo@nhs.net
- The right to object – this allows individuals to object to the processing of their personal data in certain circumstances. The national opt-out programme may result in this right being actioned by individuals. For further information please contact medwayft.dpo@nhs.net
- Rights in relation to automated decision making and profiling. This allows individuals to request for their personal data to not be used in automated decision making and profiling. For further information please contact medwayft.dpo@nhs.net
- More information on the Rights can be found via the Information Governance intranet page Right Intranet page

3.14 **Third party** – any person other than:

- The data subject
- The data controller or
- Any data processor or other person authorised to process data for the data controller or processor

4 (Duties) Roles & Responsibilities

4.1 The Chief Executive has overall responsibility for the Data Protection Policy within the Trust.

The implementation of and compliance with this policy is delegated to the Data Protection Officer (DPO) who is the Trust Secretary and Director of Corporate Compliance and Legal services; Senior Information Risk Officer (SIRO) who is the Director of Finance and Business Services; the Information Governance Manager; Information Asset Owners (system Managers) and other designated personnel.

4.2 **Management responsibilities:**

The Medway NHS Foundation Trust will:

- Ensure conditions for the fair collection and use of personal information is met by proactively informing patients and service users of how we collect, share, process, and protect their information (the confidentiality, integrity and availability of their information) and confirm to them the purpose for which their information will be used. This will mainly be done using the Trust's various privacy notices.
- Collect and process only relevant and necessary personal information, to the extent that it is needed to fulfil operational needs or to comply with legal requirements.
- Establish systems and processes to ensure that information is only kept for as long as lawfully required and in compliance with the Information Governance Alliance Records Management Code of Practice and the Trust Records Management Policies and SOP available via QPulse.
- Ensure people whose information is held can fully exercise their rights under GDPR.
- Take appropriate technical and organisational security measures to safeguard personal information whether using the existing Trust systems, or in transit to third parties.
- Ensure personal information is not transferred outside the European Economic Area without suitable safeguards being evidenced via risk assessments and due diligence such as a Data Privacy Impact Assessment and a 'managing risks when outsourcing' document.
- Ensure that there is a nominated person, the Data Protection Officer, with specific responsibility for data protection.

- Ensure that there is a nominated person, the Caldicott Guardian, with specific responsibility for internal protocols governing access to the Trust's identifiable information.
- Ensure that everyone managing and handling personal information is aware of their responsibilities.
- Ensure that anyone who wants to make enquiries about handling personal information knows what to do and that clear procedures on handling personal information are in place.
- Ensure that all staff who manage and handle personal information understand that they are contractually responsible for following good data protection practice.
- Ensure that all staff who manage and handle personal information maintain awareness of their responsibilities and obligations to respect patient confidentiality.
- Ensure that all staff who manage and handle personal information are appropriately trained to do so, and supervised where necessary.
- Ensure that all staff who manage and handle personal information are aware that they are also personally legally liable if they breach legislation relating to gathering, storage or processing of data at all times.
- Ensure that the performance of these procedures is regularly monitored and evaluated.

4.3 **The Data Protection Officer:**

Must ensure the Trust is GDPR compliant at all times and takes into consideration any new legislation that might take effect from time to time.

- Has responsibility to ensure requests under the GDPR, including Subject Access and the other Individual Rights are completed in a timely manner.
- Is responsible for internal oversight of data security and protection breach investigations, and liaising with the ICO on serious breaches.
- Is responsible for liaising with external organisations on GDPR
- Is responsible for ensuring the Board is kept up to date with progress or concerns in relation to the GDPR and Information Governance.

4.4 **The Head of Legal services**

- Holds management responsibility for ensuring requests under the GDPR in relation to the right of Subject Access are completed in a timely manner and arranges for updates and escalation to be sent through to the Information Governance Manager.

4.5 **The Head of Corporate compliance, Risk and Information Governance**

- Provides strategic overview of the Information Governance function within the Trust.

4.6 **The Information Governance Manager**

- Is responsible for advising users of their responsibilities under GDPR, Individual Rights (excluding the right of access)
- Is responsible for internal oversight of data security and protection breach investigations, and liaising with the ICO on serious breaches.
- Is responsible for liaising with external organisations on GDPR.

4.7 **The Caldicott Guardian**

- Is responsible for agreeing, monitoring, and reviewing internal protocols governing access to personal-identifiable information by staff within the organisation, in compliance with UK and EU legislation and national and international policy and guidance.
- Is responsible for agreeing, monitoring, and reviewing protocols governing the use of personal-identifiable information across organisations, e.g. with other NHS and local authority services, and other partner organisations contributing to the local provision of care.

4.8 **Senior Information Risk Owner**

- Is responsible for the management and accountability of information risk.

4.9 **Information Asset Owners**

Are responsible for ensuring the confidentiality, integrity and availability of that asset for which they are responsible. This includes ensuring that:

- only authorised staff may access the information
- that where processing of patient (or staff) information is contracted out to third parties, the contract remains valid and that security credentials tendered by contractors remain appropriate for the classification level of personal information being processed
- that an annual review of the asset is conducted in relation to supporting business continuity plans and Data Mapping spreadsheets are updated monthly
- that new information assets are registered on the Trust's Information Asset Database
- that where personal identifiable information is to be shared not for providing direct care, a lawful basis for doing so applies, for example:
    - Informed patient consent is explicitly obtained, or

- There is a statutory duty on the Trust to share the information for example under the Children Act 1989 (duty to disclose) or where a girl under 18 appears to be subject to genital mutilation, or
- Where there is no statutory duty (for example a request from the police) where refusal to disclose would undermine the investigation and potential prosecution of a crime[1]

- Where information is to be shared on a routine basis, appropriate information sharing agreements are established before information is shared with a third party
- The Trust will ensure that when working with processors all contracts will detail the requirements on how to manage and report a breach.
- Under GDPR the Trust is now liable for a breach that originates from an organisation processing the information we provide to them, as it would be if the incident occurred on-site.

4.10 Project Managers

- Where new projects are planned:
  - a Data Privacy Impact Assessment (DPIA) is conducted as part of the Project Implementation Document (PID) and risk process, and discussed with the IG team prior to implementation
  - where processing of patient (or staff) information is contracted out to third parties, the security credentials tendered by contractors are appropriate for the classification level of personal information being processed
  - where contractors propose to sub-contract information processing, the integrity and confidentiality of information is protected throughout the supplier chain
  - Where a proposed contractor plans to process personal information outside the UK or in a Cloud server, a risk assessment is carried out to confirm the security of the information at rest and in transit to the supplier together with the 'managing risks when outsourcing ' documentation

4.11 All Staff

- are contractually and legally responsible to follow good data protection practice and are legally liable if they breach legislation.

5 The Principles of the GDPR

[1] See http://systems.digital.nhs.uk/infogov/iga/consultations/policedisc.pdf for more information

Article 5 of the GDPR requires that personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for a 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, in accordance with Article 89(1)[2], not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is 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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject.
- 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.

The controller shall be responsible for, and be able to demonstrate compliance with, the above principles.

[2] Article 89(1): Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

6 Monitoring and Review

What will be monitored	How/Method/ Frequency	Lead	Reporting to	Deficiencies/ gaps Recommendations and actions
The Policy	Every two years or more frequently if appropriate to take into account changes to legislation that may occur and/or guidance from the Department of Health, the Information Commissioner's Office and/or any relevant case law	Information Governance Manager	DPO	Information Governance Group

7 Training and Implementation

7.1 All staff are required to complete their annual Data Security and Protection training either on-line or through classroom based sessions. Bespoke training is also available upon request.

7.2 Compliance with this policy is monitored via:

- The percentage level of staff completing training
- Monthly management information on the level of subject access requests completed within the statutory deadline
- The level of data breach incidents reported via Datix
- The level of data breach incidents escalated to the ICO via the IG Toolkit

8 Equality Impact Assessment

All public bodies have a statutory duty under The Equality Act 2010 (Statutory Duties) Regulations 2011 to provide "evidence of analysis it undertook to establish whether its policies and practices would further, or had furthered, the aims set out in section 149(1) of the [Equality Act 2010]"; in effect to undertake equality impact assessments on all procedural documents and practices. Authors should use the Equality Impact Toolkit to assess the impact of the document.
In the first instance this will mean screening the document and, where the screening indicates, completing a full assessment. The Toolkit can be found on the Trust

website http://www.medway.nhs.uk/our-foundation-trust/publications/equality-and-diversity/equality-impact-assessments/

A document will not be considered approved until the author has confirmed that the screening process has been carried out and where required a full impact assessment has been completed. Where a full assessment is completed this should be submitted along with the document for approval.

9 References

Document	Ref No
References:	
• Public Records Act 1958 • General Data Protection Regulations (**GDPR**) • Data Protection Act 2018 Freedom of Information Act 2000 • Access to Health Records Act 1990 • Regulation of Investigatory Powers Act 2000 (**RIPA**) • Records Management Code of Practice for Health and Social Care 2016 • NHS Information Governance: Guidance on Legal and Professional Obligations	
Trust Associated Documents:	
Information Security Policy	POLCGR018
Remote Access Policy	POLCGR084
Network Security Policy	POLCGR082
Acceptable Use of Trust Information Assets	POLCGR113
Secure Transfer of Information Policy	POLCGR077
Information Governance Policy	POLCGR017
Information Governance Strategy	STRCGR013

END OF DOCUMENT