Market Street Medical Practice

Data Protection Act Policy

1. Introduction

Summary & Aim

The Practice is committed fully to compliance with the requirements of Data Protection legislation and the General Data Protection Regulations (GDPR). The GDPR and the Data Protection Act 2018 (which provides the derogations (exemptions) to the GDPR) aims to balance the requirements of organisations to collect, store and manage various types of personal data in order to provide their services, with the privacy rights of the individual about whom the data is held.

Target Audience

This policy applies to:

- All Practice staff, including temporary staff and contractors, sub-contractors.
- Any individual using information "owned" by the Practice
- Any individual requiring access to information "owned" by the Practice

Training Requirements

Data protection act training is covered as part of the mandatory IG training package called ***Data Security Awareness - Level 1*** provided via NHS Digital
For 2018-19 the Practice will continue to use Bluesteam on-line learning, as approved by Yvonne Salkeld on the 18/12/2018.

Introduction

The General Data Protection Regulations and Data Protection Act (DPA) 2018 aims to balance the requirements of organisations to collect, store and manage various types of personal data in order to provide their services, with the privacy rights of the individual about whom the data is held.

The GDPR and DPA legislation covers both manual and computerised records in any format, where the record contains details that can identify, directly or indirectly data on a natural person or persons. The DPA sets out principles which must be followed by those who process data; it gives rights to those whose data is being processed.

To this end, the Practice endorses fully and adheres to the principles of data protection, as set out in Data Protection legislation.

- Data must be processed lawfully, fairly and in a transparent manner.

- Data must only be obtained for specified, explicit and legitimate purposes.

- Data must be adequate, relevant and limited to what is necessary for the purposes.
- Data must be accurate and up to date.
- Data must not be kept in a form that permits identification for longer than necessary for the purposes for which it is processed.
- Data must be processed in a manner which ensures appropriate security of the personal data.
- The Data Controller (the Trusts(s)) shall be responsible for, and be able to demonstrate compliance with the above principles (accountability).

2. Purpose

To provide guidance on how to ensure that the Practice complies with the latest Data protection legislation.

3. General Data Protection Regulations and Data Protection Policy Details

The Practice will handle personal data in accordance with the Act by:

- Obtaining and processing personal data in such a way that recognises the conditions for fair processing, for compliance with a legal obligation to which the Practice is subject, and for the exercise of statutory functions;
- Collecting and processing personal data on a 'need to know' basis, ensuring that it is fit for purpose, not excessive, is disposed of at a time appropriate for its purpose and that adequate steps are taken to ensure the accuracy and currency of data;
- Ensuring that for all personal data, appropriate technical and organisational measures are taken to prevent damage, loss or abuse;
- Ensuring that the movement of personal data is done in a lawful way – both inside and outside the organisation;
- Acknowledging the rights of individuals to whom the personal data relates and ensure that these rights may be exercised in accordance with the Act.

- Ensuring that the Information Commissioner is notified of all relevant processing and will conduct a periodic review and update of the register entries to ensure that they remain up to date;

- Ensuring that an active 'fair processing' framework is in place, through which patients and staff are informed about the kind of purposes for which information about them is collected, and the categories of people or organisation to which such personal information may be passed. Such a framework will ensure that an individual's consent to the use of their information is informed.

Compliance via this policy is delivered through the following initiatives:

3.1 Data Protection Compliance

Compliance will be achieved via three main areas:

- **Process** - A set of practices and policies that make sure compliant processes are followed which are aligned with the legal requirements. This provides a structured way of managing confidential.
- **People** - Aligning people in the organisation in terms of staff training and awareness with the end result of providing a competent staffing resource;
- **Technology** – supporting in providing the relevant tools for a competent workforce to use in line with agreed progress (management of systems, governance frameworks, best practice, audits).

3.2 General Data Protection Regulations and Data Protection Principles

The Practice will be responsible for compliance of the six privacy principles documented at Article 5 of the Regulation. The principles are as follows:

a) Lawfulness, fairness and transparency

b) Purpose Limitation

c) Data minimisation

d) Accuracy

e) Storage Limitation (retention periods)

f) Integrity and confidentiality

In addition, the Practice shall be responsible for, and be able to demonstrate compliance with principles – known as the seventh principle which asserts that the Practice is responsible for ensuring compliance with the previous six principles and for being able to demonstrate compliance (accountability).

The Practice will achieve this through the Data Protection Compliance Programme summarised above (ref 3.1).

Data Subjects have increased rights, to:

1. Information about how their information is being processed.
2. Access to their information.
3. Rectification when information is wrong.
4. Be forgotten; when it is appropriate to do so.
5. Restrict processing.
6. Data portability.
7. Object to processing.
8. Appropriate decision-making.

In health and social care the Caldicott Principles reflect these, that when using personal identifiable data:

1. Justify the purpose(s).
2. Don't use it unless it is absolutely necessary.
3. Use the minimum necessary.
4. Access should be on a strict need to know basis.
5. Everyone with access to it should be aware of their responsibilities.
6. Comply with the law.
7. The duty to share information can be as important as the duty to protect patient confidentiality.

The following indicates how the Data Protection principles will be achieved within the Practice:

3.2.1 Justifications for processing personal data

The Practice will ensure that all collections and regular flows of personal data are documented. This will ensure compliance with the requirement to have records of processing activities (under Article 30 of the General Data Protection regulation). These records will define the legal justifications for the processing of that data.

In any processing of data identified in the records of processing activity where the Practice can offer the data subject real choice and control of the use of their data for that purpose, then the processing will only be justifiable with the explicit, recorded consent of the data subject, i.e. the publication of a photo of the data subject in a publicity brochure. Where the processing of personal data also requires the processing of special categories of personal data (also known as sensitive personal data) then in addition the relevant justification to permit the processing of such data will also be documented.

The relevant retention periods for holding the information will be in line with the NHS Records Management Code of Practice.

As documented in the privacy notices the lawful conditions are documented which in the main will be under the public function condition.

3.2.2 Providing Information Notices to Data Subjects

The Practice will have responsibility for ensuring that they are informing data subjects of how their information is being used and in addition are expected to inform the Information Governance department of any changes and amendments so that the Team can update the Practice Privacy Notice.

The Practice will have one information notice which will be available on the public website.

The Practice will ensure that the same processes are in place for staff. This will be in the form of a separate privacy notice for staff.

3.2.3 Uses of Personal data by the Practice

The Practice will ensure that any existing uses of personal data comply with the data protection principles listed in the initial policy statement and the responsibilities of the Practice set out in this policy.

In developing any new services, projects or products, the Practice may be required to either collect new personal data, or use existing personal data for purposes it was not originally collected for.

In these circumstances the Practice will undertake a Data Protection Impact Assessment in order to ensure that the rights of individuals under this legislation are upheld.

3.2.4 Disclosure of personal data to external parties

Any request to disclose personal data of any individual whose data is held by the Practice will be considered carefully. Disclosures will only be permitted if an appropriate and necessary justification is established, in line with the requirements for lawful processing defined in data protection legislation. Any such disclosure will be recorded along with the reasons and justifications established to permit the disclosure. If a request to disclose is received, but no justification for disclosure other than consent would permit the disclosure, then disclosure will only be with the informed, explicit, recorded consent of the data subject.

Regardless of the justification for any disclosure, the data subject will be informed about the request and potential disclosure, unless to do so would prejudice any reasons for the request being made (such as prejudicing a police investigation or legal case). If the

decision is taken not to inform the subject the relevant justifications as defined in legislation will be noted.

3.2.5 Data processed by suppliers on behalf of the Practice

Where another organisation processes data on behalf of the Practice, such as a system supplier, then the Practice will ensure there is a contract in place that defines the boundaries and limitations of processing the data in terms of purposes and the requirements of the Practice to secure the personal data. This should include all the requirements put upon a 'data processor' as defined in Articles 28 & 29 of the General Data Protection Regulation.

3.2.6 Security of Personal Data

The Practice recognises that we are privileged to have personal identifiable information and through security policies and procedures will ensure appropriate technical and organisational controls in place.

3.2.7 Subject Access and other individual rights

Any data subject of the Trust(s) may exercise their rights under General Data Protection Regulations and Data Protection legislation. The Trust will set out procedures to manage these requests in line with legislative requirements. The rights are:

- A right of access
- A right of correction (rectification)
- A right to erasure (to be forgotten)
- A right to restrict processing
- A right to portability of data
- A right to object to the processing of data
- Rights with regard to automated decision taking and profiling of data subjects

All requests to exercise rights will be responded to within timescales laid down by the legislation, either by providing the information requested, or a response of the action taken by the Practice.

Where any request to exercise a right is to be denied, the response will detail the justification(s) put forward by the Practice in line with the exemptions and restrictions defined within the relevant data protection legislation.

3.2.8 Consent

Consent is one of the most important parts of ensuring compliance within GDPR. Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject must be able to withdraw consent at any time. The Practice as a public body is able to process data using the "public functions" conditions laid down in the legislation and therefore consent may not always be necessary.

3.2.9 Data Breaches

The Practice will report all high risk (see definition section) data breach to the Information Commissioner's Office. Where the Practice identifies that the data breach may result in a high risk to the data subject(s) then the individual will be informed.

Data Breaches will be handled in line with the overall Incident reporting policy of the Practice.

4. Training and Support

Employees will be made aware of their responsibilities under this policy through:

- Effective induction
- Circulation of this policy via the intranet and employee noticeboards
- Mandatory annual training.

5. Monitoring Compliance with this Policy

Aspect of compliance or effectiveness being monitored	Monitoring method	Individual responsible for the monitoring	Frequency of the monitoring activity	Group / committee which will receive the findings / monitoring report	Group / committee / individual responsible for ensuring that the actions are completed

6. References and Bibliography:

- A Manual for Caldicott Guardians (2017)
- Access to Health Records Act 1990
- Computer Misuse Act 1990
- Common Law Duty of Confidentiality
- CQC Safe Data, Safe Care (2016)
- Data Protection Act 1998 (until 24/05/2018)
- Data Protection Act 2018 (from 25/05/2018)
- Environmental Information Regulations
- Freedom of Information Act 2000
- General Data Protection Regulation / pending Data Protection Act (from 25/05/2018)
- Health and Social Care Act 2012
- Health and Social Care (Safety and Quality) Act 2015
- Confidentiality NHS Code of Practice (2003)
- Human Rights Act 1998
- Records Management Code of Practice for Health and Social Care (2016)
- Information Security Management Code of Practice (2007)
- Information: To Share or Not to Share (2013) (Caldicott2)
- Privacy and Electronic Communications Regulations
- Report on the Review of Patient-Identifiable Information (1997) (The Caldicott Report)
- Review of Data Security, Consent and Opt-Outs (2016) (Caldicott 3)

7. Duties (Roles & Responsibilities):

7.1 All staff

All staff are responsible for ensuring that:

- Keep up to date with IG training.

- Any personal or sensitive personal data that they hold is kept securely and only used for legitimate business of the Practice).

- Personal, sensitive personal data and or any other restricted data is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

- Reporting any near misses or incidents related to personal data, so they can be investigated and managed.

All staff are additionally responsible for:

- Checking that any information that they provide to the Practice in connection with their employment is accurate and up to date.

- informing the Practice of any changes to information that they have provided, including but not limited to changes of address, either at the time of appointment or subsequently. The Practice cannot be held responsible for any errors unless the employee has informed it of such changes.

Any member of staff, or other individuals who considers that the policy has not been followed in respect of personal data about himself or herself, should raise the matter with his or her line manager in the first instance and then to the Practice Data Protection Officer.

Staff should note that unauthorised disclosure of data deemed, personal, sensitive (special category) personal, confidential and restricted under the definitions in this policy will usually be a disciplinary matter, and may be considered gross misconduct in some cases. Therefore it is essential, if unsure, to check whether the disclosure is necessary or legally permissible by checking with the Data Protection Officer.

Staff will be required to report any incident related to data so that swift remedial and containment action can be applied.

8. Abbreviations / Definitions of Terms Used

Keep lists in alphabetical order

ABBREVIATION	DEFINITION
AHRA	Access to Health Records Act 1990
DPA	Data Protection Act 1998
DPIA	Data Protection Impact Assessment
DS&Ptk	Data Security and Protection Toolkit
GDPR	General Data Protection Regulation
HSCIC	Health and Social Care Information Centre
ICO	Information Commissioner's Office
IG	Information Governance
ISG	Information Sharing Gateway
MoU	Memorandum of Understanding
PID	Personal Identifiable Data
SAR	Subject Access Request
SIRO	Senior Information Risk Owner
SOP	Standard Operating Procedure
ToR	Terms of Reference

TERM USED	DEFINITION
Anonymised Information	This is information which does not identify an individual directly, and which cannot reasonably be used to determine identity. Anonymisation requires the removal of name, address, full postcode and any other detail or combination of details that

	might support identification.
Confidentiality	A duty of confidence arises when one person discloses information to another person, where it is reasonable to expect that information is to be held in confidence.
Data Controller	A Data Controller is 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 to be processed. By person it does not necessarily mean a living individual but refers to legal entity (i.e. organisation).
Data Erasure	**A**lso known as the Right to be Forgotten, it entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties cease processing of the data
Data Portability	The requirement for controllers to provide the data subject with a copy of his or her data in a format that allows for easy use with another controller
Data Processor	Any person (other than an employee of the data controller) who processes the data on behalf of the Data Controller.
Data Recipient	A recipient is any person who obtains a disclosure of data, this includes employees or agents who would not be regarded as third parties.
Data Subject	A natural person whose personal data is processed by a controller or processor
Disclosure	This is the divulging or provision of access to data.
Encrypted Data	Personal data that is protected through technological measures to ensure that the data is only accessible/readable by those with specified access
Health Record	Information about the physical or mental health or condition of an individual, made by or on behalf of a health professional in connection with the care of that individual.
Healthcare Purposes	These include all activities that directly contribute to the diagnosis, care and treatment of an individual and the audit/assurance of the quality of the healthcare provided. They do not include research, teaching, financial audit and other management activities.
Information Asset Administrator	Primary role is to support the IAO to fulfill their responsibilities. IAAs will ensure that policies and procedures are followed, recognise actual or potential security incidents, consult with their IAO on incident management and ensure that information asset registers are accurate and up to date.
Information Asset Owners	Senior members of staff who take responsibility for Information Assets such as information systems - further defined in the Trust's Information Risk Policy.
Information Sharing Protocols	Documented rules and procedures for the disclosure and use of patient information, which specifically relates to security, confidentiality and data destruction, between two or more organisations or agencies.
Medical Purposes	As defined in the Data Protection Act 1998, medical purposes

	include but are wider than healthcare purposes. They include preventative medicine, medical research, financial audit and management of healthcare services. The Health and Social Care Act 2001explicitly broadened the definition to include social care.
Personal Identifiable Information	Data that relate to a living individual who can be identified either from the data alone, or from combining the data with other information held by the data controller. It includes any recorded expression of opinion by or about the individual. Personal data may be held in electronic or manual form, or both.
Processing	Any activity that can be carried out concerning personal data.
Profiling	Any automated processing of personal data intended to evaluate, analyse, or predict data subject behavior
Pseudonymised Information	This is like anonymised information in that in the possession of the holder it cannot reasonably be used by the holder to identify an individual. However it differs in that the original provider of the information may retain a means of identifying individuals. This will often be achieved by attaching codes or other unique references to information so that the data will only be identifiable to those who have access to the key or index. Pseudonymisation allows information about the same individual to be linked in a way that true anonymisation does not.
Sensitive Personal Data / Special categories of personal data	**Under GDPR (article 9) "special categories of personal data" means personal data consisting of information such as:** a) racial or ethnic origin b) political opinions, c) religious or philosophical beliefs d) trade union membership, e) genetic data f) biometric data g) health data h) sex life i) sexual orientation The presumption is that, because information about these matters could be used in a discriminatory way, and is likely to be of a private nature, it needs to be treated with greater care than other personal data. The nature of the data is also a factor in deciding what security is appropriate
Third Party Information	Information relating to any person other than the data subject, the Data Controller or any data processor or other person authorised to process data for the controller or processor. Generally this would be one of the following: 1) Any individual who is identifiable from the records who is not the applicant. Note that this does not apply to healthcare professionals. 2) In an organisation context, a third party is any organisation /

	agency which is not the Practice, i.e. where the Practice holds information from other organisations, those other organisations remain organisationally responsible for their own records as the “data controller” and constitute third parties