Elsenham Surgery

Policy Name:

General Data Protection Regulation Policy

Last Reviewed:

25.6.19

Next Review:

25.6.20

See Intradoc for Full Version Control History

ELSENHAM SURGERY
General Data Protection Regulation Policy

1. Introduction

The General Data Protection Regulation (GDPR) came into force on 25th May 2018. The aim was to strengthen the previous Data Protection Act and to offer more control to individuals over what happens to their data, who is it shared with and the right to delete data. The GDPR covers personal data held manually and electronically.

The GDPR is closely linked to the Freedom of Information and Human Rights Acts. It focus is on promoting the rights of individuals in respect of their privacy and the right to confidentiality of their data. The responsibility to maintain the confidentiality of data resides with the Data Controller[1], even if an agent or subcontractor performs the processing[2].

The Practice has a legal obligation to comply with all appropriate legislation in respect of data, information and IT Security. It also has a duty under the establishment order to comply with guidance issued by The Department of Health, the NHS Executive, and other advisory groups to the NHS and guidance issues by professional bodies. The Practice believes individual's right of confidentiality are paramount.

All legislation relevant to an individual's right of confidence and the ways in which that can be achieved and maintained are paramount to the Practice. This relates to roles that are reliant upon computer systems such as patient administration/payment, purchasing, invoicing and treatment planning. Recent legislation also regulates the use of manual records relating to patients, staff and others whose information may be held within the Practice.

This document is a statement of the policy and principles adopted by Elsenham Surgery governing the processing of personal data as specified in the GDPR (2018). Conformance with the GDPR is part of the Practice's overall duty of confidentiality towards its patients, staff, and all other individuals with whom it deals, and this policy should be read in conjunction with the Practice's policies towards:

- The Caldicott recommendations,
- IT security,
- Personal and HR records,
- Payroll records,
- Supplier relationships

[1] The Data Controller is the person who in nominated by the Practice who determines the purposes for which and the manner in which any personal data are, or are to be, processed.
[2] Data Processing is anything that happens to data from when it is obtained until it is destroyed.

Noncompliance with the relevant legislation could result in individual employees and the Practice being prosecuted for offences under the GDPR:

- Processing personal data without notifying the Information Commissioner.
- Processing personal data for any purpose other than that covered by the Practice's notification.
- Unauthorised disclosure of personal data e.g. disclosure to a person/organisation not entitled to receive it.
- Failure to comply with the information/enforcement notice issued by the Information Commissioner.
- Modifying personal data subject to a subject access request.
- There are some offences around misinformation when registering with the information commissioner.

The Practices' GDPR Policy (The Policy) aims to detail how the Practice meets its legal obligations and NHS requirements concerning confidentiality and information security standards. The requirements within the Policy are primarily based upon the GDPR that is the key piece of legislation covering security and confidentiality of personal information.

Any confidentiality issues, should be addressed to:

The Practice Manager
Elsenham Surgery
Station Road
Bishops Stortford
Herts CM22 6LA

2. Data Protection

The 2018 GDPR defines data as any information which:

- is processed using equipment operating automatically in response to instructions,
- is recorded with the intention of being processed,
- is recorded as part of a relevant filing system,
- forms part of an accessible record, including health records.

Data Protection under the 2018 Act is about ensuring that personal data about an individual is processed fairly and lawfully in order to protect the rights of an individual

Personal Data, within the Practice, is taken to include:

- All identifiable patient information, including health records,
- all identifiable staff information,
- Any other identifiable personal information held on suppliers, contractors etc.

Whether held in electronic or paper form.

Certain types of data are regarded as sensitive, and the Act stipulates that special measures must be taken in the processing and protection of this type of data. Sensitive data includes:

- Racial or ethnic origins,
- Political opinions,
- Religious other similar beliefs,
- Membership of a trade union,
- Physical or mental health condition,
- Sexual life,
- The commission of any offence, or
- Any proceedings for any offence, or the sentence of any court in such proceedings.

The Practice collects and uses information about identifiable individuals in the course of its operations. These include current, past and prospective patients, employees, suppliers, contractor clients/customers, and others with whom it communicates. In addition, it may occasionally be required by law to collect and use certain types of personal information to comply with the requirements of government departments. Under the GDPR 2018, all forms of personal information must be dealt with properly however it is collected, recorded and used - whether automatically, within accessible records or relevant filing systems - and there are safeguards to ensure this in the GDPR 2018.

3. Policy statement

The Practice regards the confidence and Practice of both its staff and service users as a crucial element in its role in delivering the highest quality health care services in West Essex. The lawful and correct processing of personal information is a key part of building and maintaining that Practice and confidence.

The Practice will fully implement all aspects the GDPR 2018 and the Freedom of Information Act 2000.

The Practice will make all patients, staff and other individuals fully aware of both their rights and obligations under the Act, by holding mandatory training courses.

The Practice will implement adequate and appropriate physical and technical security measures and organisational measures to ensure the security of all information contained in or handled by those computer systems managed by the Practice, or by other agencies on behalf of the Practice.

The Practice will transfer personal data outside the European Economic Area (EEA), only with the *explicit* informed consent of the individual concerned.

4. Aims of the Policy

The aims of the policy are to deliver fully the Principles of Data Protection, as stated in the GDPR 2018. The Principles require that:

First Principle: Personal[3] information shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met.

There is a requirement to make the general public, who may use the services of the NHS; aware of why the NHS needs information about them, how this is used and to whom it may be disclosed. The Practice is obliged under the GDPR and Caldicott to produce a patient information leaflet.

A clear policy of consent is needed to ensure the first principle is addressed. The Practice has formally adopted a policy on this subject.

Second Principle: 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 that purpose or those purposes.

Third Principle: Personal information shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Fourth Principle: Personal information shall be accurate and, where necessary, kept up to date.

Fifth Principle: Personal information shall not be kept for longer than necessary for that purpose or those purposes

All records are affected by this principle regardless of the media they be held, stored, retained. HSC 1999/053 provides comprehensive guidance and HSC 2018/217 the same for information for GP held patient records.

Sixth Principle: Personal information shall be processed in accordance with the rights of data subjects under the Act.

Under this principle of the GDPR individuals have the following rights

- Right of subject Access
- Right to prevent processing likely to cause harm or distress
- Right to prevent processing for the purposes of direct marketing
- Right in relation to automated decision taking
- Right to take action for compensation of the individual suffers damage
- Right to take action to rectify, block, erase or destroy inaccurate data

[3] Personal data is any information, held in any format that relates to a living individual and can identify the person uniquely.

- Right to make a request to the Information Commissioner for an assessment against an organisation to establish whether any part of the Act has been contravened

Seventh Principle: Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal information and against accidental loss or destruction of, or damage to, personal data.

Eighth Principle: Personal information shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects[4] in relation to the processing of personal data.

5. Scope of the Policy

The policy covers all aspects of business relating to personal information within the Practice and is not solely patient related. It includes information held by all areas such as:

- Healthcare, covering:
  Acute, Community & Intermediate Care
  Mental Health
  Learning Disabilities
  Primary Care
  Child Protection
- H.R. – including Criminal Records Bureau checks on staff
- Payroll & Finance
- Procurement

The policy covers all methods of holding information, and all media used to store information, including:

- manually stored paper data, e.g. card index files, medical records etc.,
- computer referenced paper data, e.g. health records, personnel records, etc.,
- computerised data held in computer applications and databases,
- tapes and other data from CCTV systems,
- data held offsite in archive storage,
- data held on CD ROMs, floppy disks, computer disks, memory sticks etc.

6. Responsibilities

Jane Marley –West Essex CCG is the Data Protection Officer for Elsenham Surgery.

She has responsibility for ensuring that personal information is processed in accordance with the rights of the individual resides at all levels within the Practice:

1. All staff associated with the Practice have a responsibility to ensure compliance with the GDPR 2018 and to actively respond to any concerns relating to confidentiality.

[4] The Data Subject is the individual who is the subject of personal data.

2. The Clinical Leads and Practice Manager have a responsibility to understand the Act, and other related guidance, to establish appropriate procedures to control and manage information accordingly, and to ensure that these procedures are followed.

3. The Data Protection Officer is responsible for facilitating the implementation of the policy and supporting Practice staff to understand their responsibilities.

4. The Caldicott Guardian has responsibility for advising Practice staff and for ensuring adequate arrangements are put in place to protect patient identifiable information. Within the Practice, the Practice Manager is the nominated Caldicott Guardian.

5. The Practice Manager / Caldicott Guardian are responsible for ensuring the effective integration of respective policies for control of clinical and non-clinical information.

6. The Practice will fully conform to the rules for notification. These include:

    - that a notification is lodged in its name with the Information Commissioner,
    - that the notification is lodged within the stipulated time period,
    - that the notification is full, correct and up-to-date,
    - that any changes are notified within the stipulated time period.

The Practice will fully discharge its responsibilities implied by the Principles contained with the GDPR by putting in place procedures, and by ongoing monitoring of these procedures:

- to observe fully conditions regarding the fair collection and use of information,
- to meet its legal obligations to specify the purposes for which information is used,
- to collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirement,
- to ensure the quality of information used,
- to apply strict checks to determine the length of time information is held,
- to ensure that the rights of people about whom information is held can be fully exercised under the Act, this includes monitoring the management of "rights of access".
- to take appropriate technical and organisational security measures to safeguard personal information,
- to ensure that the necessary measures are taken to safeguard all sensitive personal data,
- to ensure that the necessary measures are taken to ensure the proper disclosure of information between agencies
- to ensure that personal information is not transferred abroad without suitable safeguards.

7. Individual Rights

Individuals have rights under the GDPR 2018 in respect of their own personal data held by others. The Practice will ensure that all individuals are aware of their rights under then Act, and will fully comply with the delivery of these rights to individuals.

The rights of the individual are:

- to be informed about the use made of personal data,
- to be informed about the purpose of processing, the source and the recipients of the data,
- to be informed of any logic used in automated decisions,
- to be provided with a copy of his record, where the effort to provide such is reasonable,
- to have incorrect data corrected, blocked, erased or destroyed,
- to have previous recipients of such data informed,
- to object where substantial damage or distress may be caused,
- to object where personal data are used for direct marketing,
- to take action for compensation if an individual suffers damage,
- to make a request to the Commissioner for an assessment to be made as to whether any provision of the Act has been contravened.

The Practice will ensure that patients are aware of their rights and how to exercise these rights. Patient leaflets are readily available upon request.

8. Subject Access Requests

All data subjects, or someone acting on their behalf (with patient consent), can request to view their personal data held by the Practice. All SAR's will be processed within one month.

All applications regarding patient personal data must be made in writing to the Practice Manager.

If a member of staff requires a copy of their personal data, a request can be made via their line manager.

9. Disclosures to others

The Practice may receive requests to obtain personal data from sources other than the individual. N.B. Please refer to the Practice Safe Haven Procedures for guidance on how to handle person-identifiable information.

Statutory Requests – All statutory requests from courts or coroners offices etc. will be complied with by the Practice via the Practice Manager, if appropriate, the patient may be informed that the data has been disclosed unless this would prejudice a criminal investigations.

Medico-Legal – All requests from solicitors and healthcare providers will only be complied with if the Practice is in receipt of the written consent of the patient or their representative, again all of these requests will be handled by the Practice Manager.

Police – All requests from the police for personal data will be viewed on a case-by-case basis via the Practice Manager, and Caldicott Guardian (or other Partner on call) who will decide if the information can be disclosed:

All requests must be in writing using the documentation provided by the Police authority.

The most likely legal basis for disclosure (without the patient's consent) to the police are:

- Prevention of Terrorism Act 1989 and Terrorism Act 2000 – it is a statutory duty to inform the police about information gained (including personal information) about terrorist activity.
- The Road Traffic Act 1988 – It is a statutory duty to inform the police, when asked, the name and address (not clinical information) of drivers who are allegedly guilty of an offense.
- Court order – where the courts have made an order the information must be disclosed unless the Practice decides to challenge the order of the court.

10. Exemptions

There are specific reasons why access to personal data may be denied including:

- Where the data released may cause serious harm to the physical or mental or condition of the patient, or any other person.
- Where access would disclose information relating to or provided by a third party. (where consent had not been received by the third party to release their data). N.B. this does not include information recorded by Practice employees as part of their normal duties.
- Where it is assessed that a patient, under the age of 16, cannot understand the implications of accessing their records.

11. Cost and Timescales

An application for data access will incur no charge and will be complied within a one month period.

12. Training & awareness

The Data Protection Officer has overall responsibility for maintaining awareness of the GDPR to all staff. This will be carried out by the regular mandatory training sessions covering the following elements:

- Patients are aware of the policy and of their rights.
- Staff are aware of the policy and of their rights and obligations.
- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice,

- Everyone managing and handling personal information is appropriately trained to do so,
- Everyone managing and handling personal information is appropriately supervised,
- Anybody wanting to make enquiries about handling personal information knows whom to approach,
- Queries about handling personal information are promptly and courteously dealt with,
- Methods of handling personal information are clearly described,
- Methods of handling personal information are regularly assessed and evaluated,
- Performance with handling personal information is regularly assessed and evaluated,
- Awareness raising for staff is an ongoing process.

As well as mandatory training for existing staff, all new starters to the Practice will be given data protection and general IT security training as part of the induction process.

In addition, many staff are bound by their professional codes of conduct

13. Human Resources

All contract of employment include a data protection and general confidentiality clause, Agency and contract staff are subject to the same rules.

Any member of staff current, past or potential (applicants) who wishes to have a copy of their information under the subject access provision of the GDPR have the right to access information held on then.

A breach of the Data Protection requirements could result in disciplinary action. A copy of these disciplinary procedures is available to staff.

The Practice is required to undertake criminal records check on certain groups of staff. The DBS is fully committed to compliance of the GDPR 2018 and the Freedom of Information Act 2000.

14. Policy Reviews

This policy will be reviewed annually or whenever any change in circumstances requires it, by Karen Greaves the Practice Manager.

11. Contacts with the Practice

General enquires under the GDPR (2018) should be addressed to:

The Practice Manager
Elsenham Surgery
Station Road
Elsenham
Bishops Stortford
Herts CM22 6LA

12. Reference Documents

This policy should be read in conjunction with the following:

IT Security Policy
Department of Health Confidentiality Code of Conduct
Freedom of Information Act 2000
Freedom of Information Scheme
Incident Reporting Policy
Recruitment ad selection guidance
Disciplinary Policy
Record Retention Policy
HSG (96)15 The NHS IM&T Security Manual Ensuring Security and Confidentiality in NHS Organisations
HSG (96)18 The Protection & Use of Patient Information
HSC 1999/012 Caldicott Guardians
HSC 2002/003 Caldicott Guardians & Implementing the Caldicott Standard into Social Care
HSC 1999/053 For the Record BS7799 Information Security Standards
HSC 1999/217 Preservation, retention and destruction of GP General Services Records Relating to Patients
Protection of Children Act 1999
Police Act 1997

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 and Public Health (Infectious Diseases) Regulations 1985
Education Act 1944 (for immunisations and vaccinations to the NHS Practices from Schools)
Births and Deaths Act 1984
Police and Criminal Evidence Act 1984

Glossary

Personal Data

Personal Data means data which relate to a living individual, organised in such a way that the individual can be identified from the data; it includes factual data as well as any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Relevant filing system

Relevant filing system means any set of information relating to individuals structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

Processing

Processing, in relation to information or data, means obtaining, recording or holding the information or carrying out any operation or set of operations on the information, including:

- acquiring the data,
- organising and managing the information or data,
- retrieving and using the information or data,
- disclosing or sharing the information or data by fax, letter, e-mail, or any other means of transmission or dissemination,
- archiving, disposing of or destroying the information or data.

Data Subject

The Data Subject refers to the individual to whom the personal data relates.

Data Processor

The Data Processor refers to any person or organisation (other than an employee of the data controller) who processes (including storing or otherwise managing) the data on behalf of the data controller.

Recipient

The Recipient refers to any person or organisation to whom the data are disclosed, but does not include any person to whom disclosure is made as a result of, or with a view to, a particular inquiry by or on behalf of that person made in the exercise of any power conferred by law.

European Economic Area (EEA)

The European Economic Area (EEA) refers to the following European countries or territories: Austria, Belgium, Denmark (excluding the Faroe Islands), Finland, France, Germany, Gibraltar, Greece, Iceland, Ireland, Italy, Liechtenstein, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, United Kingdom (excluding the Isle of Man and the Channel Islands).

The Practice

The Practice refers to the ELSENHAM SURGERY