GDPR Policy 2021 (last updated June 2023)

In effect from 25 May 2018

Includes Data Protection Act 2018

Applies to all individuals and organisations who have day-today responsibility for data protection.

**The data protection principles**

There are now six key data protection principles in the GDPR, rather than the eight in the DPA 1998. They can be summarised as follows:

1. Personal data should be processed lawfully, fairly and in a transparent manner.
2. Personal data should be collected for specified, explicit and legitimate purposes and be processed in a manner compatible with those purposes.
3. Personal data should be accurate, relevant and limited to what is necessary for purpose.
4. Personal data should be accurate and kept up to date, and inaccurate data should be rectified without delay.
5. Personal data, in a form that identifies the data subject, should be stored for no longer than is necessary for the purpose for which it is required. Exemptions in relation to the public interest and research may apply.
6. Personal data should be securely stored and protected against unlawful processing and accidental loss, destruction or damage.

‘Personal Data’ is defined as *“any information relating to an identified or identifiable natural person (the ‘data subject’)…. who can be identified, directly or indirectly, 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 natural person”.*

This Policy will include the following information:

* The data controller’s identity
* The data protection officer’s contact details
* The purpose of the processing
* The lawful basis for processing
* The categories of personal data concerned
* The potential recipients of personal data
* How long the data will be retained
* A list of the data subject’s rights
* Any safeguards that will be used if data is to be transferred to a country outside the EU.

Cliftonville Medical Practice GDPR Privacy Notice

YOUR INFORMATION, YOUR RIGHTS

*As your GP practice, we are a ‘****data controller’****for any information that we keep about you and your health.*

This Privacy Notice tells you what information we collect about you, how we store it, and who we share it with - and the reasons why.

The health care professionals who provide you with care maintain records about your health and any treatment or care you have received previously (e.g. hospital, GP surgery etc.). These records help to provide you with the best possible healthcare.

**What type of information do we keep about you?**

* **‘Personal data’.** This means any information that can identify who you are. This includes your name, date of birth, full postcode, address and next of kin;

***and***

* **‘Special category / sensitive data’.**This means any information about your medical history. It could be when you have come in for appointments, medication you have been given, notes about your care, or treatments. It could also be social care status, race or ethnic origin. The personal information we keep about you is to help us provide health or social care or treatment, under the Data Protection Act (DPA) 2018.

**Where do we keep your records?**

Your personal information is held in both paper and electronic forms for specific amounts of time. We will always make sure:

* Your records are accurate
* Your records are secure
* You can access your records

**What do we do with your information?**

Your records are used to manage and deliver your care. This helps us make sure:

* The practice staff has all of the information they need to help them provide you with the best care for your needs.
* The practice staff involved in your care has correct and up-to-date information about you.
* The right information is available in case you see another healthcare professional, or need to see a specialist, social care or health care provider.

**Who do we share your information with?**

We may need to share information with other organisations such as:

* HSCNI Trusts
* Public Health
* Other GP practices, hospitals or ambulance services
* Private Sector Providers
* Voluntary Sector Providers
* Independent contractors e.g. dentists, opticians
* Local Authorities
* Education Services
* Police & Judicial Services
* Social Services
* Other ‘data processors’ which you will be informed of

**What are your rights?**

You will be informed who your data will be shared with and in some cases asked for explicit consent for this to happen when it is required.

The DPA 2018 means that you or your parent(s) / guardian(s) **may** have the right to:

* Ask to see the personal data we hold about you, such as health records.
* Ask us to correct information in your health records that you think is wrong or incomplete.
* Refuse or take away consent for us to share your health records with others – an example could be using your information for research purposes.
* Ask us to send your personal information to other healthcare providers.

All our staff and members of other NHS organisations have a legal obligation to keep information about you confidential.

We will only ever use or pass on information about you if others involved in your care have a genuine need for it. We will not disclose your information to any 3rd party without your consent unless there are exceptional circumstances (i.e. life or death situations), or where the law requires information to be passed on for example Child/Adult Protection and Serious Criminal Activity.

**Access to personal information**

You have a right under the Data Protection Act 2018 to request access to view or to obtain copies of what information the surgery holds about you and to have it amended should it be inaccurate.  In order to request this, you need to do the following:

Go on to our practice website www.cliftonvillemedicalpractice. and print off and complete “Access to Notes” form. Your request can also be made in writing to the practice.

* There is no charge to have a printed copy of the information held about you. However, if requests for your record are excessive or manifestly unfounded, a reasonable fee for the administrative cost will be charged to comply with the request.
* We are required to respond to you within 30 days
* You will need to give adequate information (for example full name, address, date of birth, Health & Care number and details of your request) so that your identity can be verified and your records located

**Objections / Complaints**

Should you have any concerns about how your information is managed by your GP Practice, please contact the Practice Manager- Mrs Clarke.  If you are still unhappy following a review by the GP practice, you can then complain to the Information Commissioners Office (ICO) via their website ([www.ico.org.uk](http://www.ico.org.uk/)).

**Change of Details**

It is important that you tell the person treating you if any of your details such as your name or address have changed or if any of your details such as date of birth is incorrect in order for this to be amended.  You have a responsibility to inform us of any changes so our records are accurate and up to date for you.

**Notification**

The Data Protection Act 2018 requires organisations to register a notification with the Information Commissioner to describe the purposes for which they process personal and sensitive information.

This information is publicly available on the Information Commissioners Office website [www.ico.org.uk](http://www.ico.org.uk/)

The practice is registered with the Information Commissioners Office (ICO)

**Who is the data Processor?**

This is the person/people or organisation that is responsible for using and recording your information. All staff at Cliftonville Medical Practice act as individual Data Processors.

**Who is the Data Controller?**

The Data Controller, responsible for keeping your information secure and confidential is Cliftonville Medical Practice staff.

**Data Protection Officer (DPO)**

The Data Protection Officer has overall responsibility for GDPR within this area.  Our designated DPO is**Mrs Elizabeth Clarke.**

**Data Protection Policy**

|  |  |
| --- | --- |
| Last updated | 22.6.2023 |

Definitions

|  |  |
| --- | --- |
| **Practice** | means Cliftonville Medical Practice |
| **GDPR** | means the General Data Protection Regulation. |
| **Data Protection Act** | Means the Data Protection Act 2018 |
| **Data Protection Lead** | means Dr Emma-Sue Curran |
| **Register of Processing** | means a register of all systems or contexts in which personal data is processed by the Practice. |

**Introduction**

Cliftonville Medical Practice is a General Practitioner contracted by the Health and Social Services Board to provide General Medical Services. The personal data that Cliftonville Medical Practice processes to provide these services relates to its patients, relatives and Practice staff.

This policy sets out Cliftonville Medical Practice’s commitment to ensuring that any personal data, including special category personal data, which Cliftonville Medical Practice processes, is carried out in compliance with data protection law. Cliftonville Medical Practice is committed to ensuring that all the personal data that it processes is done in accordance with data protection law. Cliftonville Medical Practice ensures that good data protection practice is imbedded in the culture of our staff and our organisation.

‘Data Protection Law’ includes the General Data Protection Regulation 2016/679; the UK Data Protection Act 2018 and all relevant EU and UK data protection legislation.

This policy applies to all personal data processed by the Practice. All staff are expected to comply with this policy and failure to comply may lead to disciplinary action up to an including dismissal.

1. **Data protection principles**

The Practice is committed to processing data in accordance with its responsibilities under the Data Protection Act and General Data Protection Regulations (GDPR).

Article 5 of the GDPR requires that 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 purposes;
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 in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
6. 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.”

**2. General provisions**

1. This policy applies to all personal data processed by the Practice.
2. The Data Protection Lead shall take responsibility for the Practice’s ongoing compliance with this policy.
3. This policy shall be reviewed at least annually.
4. The Practice shall register with the Information Commissioner’s Office as an organisation that processes personal data.

**3. Lawful, fair and transparent processing**

1. The Practice will publish a Privacy Notice that provides details in relation to its processing of information.
2. The privacy notice shall identify:
   1. Details of the Data Controller
   2. Details of the Data Protection Officer
   3. Purpose of the processing
   4. Lawful basis for processing
   5. Recipients or categories of recipients of data
   6. Individuals rights.
3. The Practice privacy notice will be reviewed and updated annually or as required following any major changes to processing activities.
4. To ensure its processing of data is lawful, fair and transparent, the Practice shall maintain a Register of Processing.
5. The Register of Processing shall be reviewed at least annually.
6. Individuals have the right to access their personal data and any such requests made to the Practice shall be dealt with in a timely manner in accordance with the requirements of the legislation.

**4. Lawful purposes**

1. All data processed by the Practice must be based on the appropriate lawful basis for both personal and special category data.
2. Processing shall be based on at least on for the following:
   1. Legal basis for processing personal data;
      1. Consent
      2. Necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract.
      3. Legal obligation to carry out the processing.
      4. Necessary to protect the vital interests of the data subject or another individual.
      5. Necessary for the performance of a task carried out in the public interest.
      6. Necessary for the legitimate interests of the Practice or by a third party.
   2. Legal basis for processing special category data;
      1. Explicit Consent
      2. Necessary for the purposes of carrying out obligations in the field of employment, social security or social protection law
      3. Necessary to protect the vital interests of the data subject or another natural person where the data subject is physically or legally incapable of giving consent.
      4. The data subject has deliberately put the data within the public domain.
      5. Necessary for the establishment, exercise or defence of legal claims.
      6. Necessary for reasons of substantial public interest.
      7. Necessary for the purposes of preventative or occupational medicine, for the assessment of working capacity of an employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.
      8. Necessary for reasons of public interest in the area of public health.
      9. Necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

1. The Practice shall note the appropriate lawful basis in the Register of Processing.
2. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
3. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Practice’s systems.

**5. Data minimisation**

1. The Practice shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

**6. Accuracy**

1. The Practice shall take reasonable steps to ensure personal data is accurate.
2. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

**7. Archiving / removal**

1. To ensure that personal data is kept for no longer than necessary, the Practice shall put in place an archiving policy for each area in which personal data is processed and review this process annually.
2. The archiving policy shall consider what data should/must be retained, for how long, and why.

**8. Security**

1. The Practice shall ensure that personal data is stored securely.
2. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
3. When personal data is deleted this will be done safely such that the data is irrecoverable.
4. Appropriate back-up and disaster recovery solutions shall be in place.

**9. Confidentiality**

As an individual working for, on behalf of or within, the Practice you are subject to an obligation of confidentiality and must adhere to the Data Protection Act 2018 (DPA18) and General Data Protection Regulation (GDPR).

All employees have a duty of confidence to patients and staff under common law. Furthermore statute law imposes legal obligations regarding confidentiality of patient data whether it is manually documented or collected and held within computer systems.

To access patient identifiable clinical information, you must have a legitimate relationship with the individual service user to whom the information relates or be part of the team providing / supporting that care.  A legitimate relationship is created only when an individual is an active recipient of the service providing care. The relationship ends when the individual is discharged from that service.

At no time are you permitted to access your own or clinical information relating to friends or relatives without a legitimate relationship being in place. Access to confidential clinical information outside of a legitimate relationship is deemed unauthorised access and may be subject to disciplinary action by the Trust or in some circumstances legal action.

While you are at work you will have access to information about patients/colleagues and/or the Practice. You may come in to contact with this type of information during the course of your work or simply see, hear or read something while you are working. In these circumstances where a duty of care, either to the patient or the staff member potentially overrides the duty of confidentiality, you must discuss the matter with the Practice manager. Otherwise, you must keep this information confidential.

Professional bodies (e.g. Nursing & Midwifery Council (NMC), General Medical Council (GMC)) provide additional supplementary advice and guidance for their own disciplines. These guidelines are complimentary to this policy and do not conflict with this policy or legislation.

* All staff are responsible for: protecting the integrity, availability and confidentiality of patient information;
* acting to prevent the improper use or disclosure of information;
* following the guidance of set out in our GDPR policy – this should be reviewed and signed annually by all staff;
* reporting breaches of Confidentiality;
* ensuring the safe collection, storage, processing and disclosure of personal and confidential information;

**9. Data Subject Rights**

Cliftonville Medical Practice has processes in place to ensure that it can facilitate any request made by an individual to exercise their rights under data protection law. All staff have received training and are aware of the rights of data subjects. Staff can identify such a request and know who to send it to.

All requests will be considered without undue delay and within one month of receipt as far as possible.

**Subject access**: the right to request information about how personal data is being processed, including whether personal data is being processed and the right to be allowed access to that data and to be provided with a copy of that data along with the right to obtain the following information:

* the purpose of the processing
* the categories of personal data
* the recipients to whom data has been disclosed or which will be disclosed
* the retention period
* the right to lodge a complaint with the Information Commissioner’s Office
* the source of the information if not collected direct from the subject, and
* the existence of any automated decision making

**Rectification**: the right to allow a data subject to rectify inaccurate personal data concerning them.

**Erasure**: the right to have data erased and to have confirmation of erasure, but only where:

* the data is no longer necessary in relation to the purpose for which it was collected, or
* where consent is withdrawn, or
* where there is no legal basis for the processing, or
* there is a legal obligation to delete data

**Restriction of processing**: the right to ask for certain processing to be restricted in the following circumstances:

* if the accuracy of the personal data is being contested, or
* if our processing is unlawful but the data subject does not want it erased, or
* if the data is no longer needed for the purpose of the processing but it is required by the data subject for the establishment, exercise or defence of legal claims, or
* if the data subject has objected to the processing, pending verification of that objection

**Data portability**: the right to receive a copy of personal data which has been provided by the data subject and which is processed by automated means in a format which will allow the individual to transfer the data to another data controller. This would only apply if Cliftonville Medical Practice was processing the data using consent or on the basis of a contract.

**Object to processing**: the right to object to the processing of personal data relying on the legitimate interests processing condition unless Cliftonville Medical Practice can demonstrate compelling legitimate grounds for the processing which override the interests of the data subject or for the establishment, exercise or defence of legal claims.

**10. Breach**

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Practice shall promptly assess the risk to people’s rights and freedoms and if appropriate report this breach to the ICO ([more information on the ICO website](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/)).

11. **Responsibility for the processing of personal data**

The partners of Cliftonville Medical Practice take ultimate responsibility for data protection.

If you have any concerns or wish to exercise any of your rights under the GDPR, then you can contact the data protection lead in the following ways:

* 1. In writing address to Mrs Elizabeth Clarke, Practice Manager
  2. By email address to Mrs Elizabeth Clarke, Practice Manager- [Elizabeth.Clarke.Z00093@gp.hscni.net](mailto:Elizabeth.Clarke.Z00093@gp.hscni.net)
  3. By telephone requesting to speak to Mrs Elizabeth Clarke, Practice Manager on 02890747361.

Data Breach Policy

* 1. Data Officer is notified a breach has taken place
  2. A risk assessment takes place within 72hours- ICO website can be used to determine level of breach
  3. If high risk level patient should be informed immediately and reported directly to the ICO
  4. If risk is medium to low a decision should be made with DO and Partners in relation to being open and transparent with the patient and actions to be taken in the future.
  5. Any Breach needs to be recorded for future reference and written up as an SEA.

A breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised.

Data Mapping Process:

Awareness of personal data we hold in the practice

Electronic notes- VISION/ DOCMAN/ RAT/ 24hr BP monitor/ VMS/ ECR

Online prescription requests

Email – prescription requests/ photos

Repeat Telephone Line

Letters- hospital/ solicitors/ requests from patients

Handwritten requests for medications/ notes

Awareness of security processes

Daily backup of VISION and DOCMAN; all tapes stored when on-site in a fireproof safe

Individual passwords for all staff

Regular change of passwords

Awareness of how data is deleted

Paper is shredded in confidential waste; immediate shredding of any paper identifiable information

Deleted records on VISION