Steyning Medical Practice - Organisational statement on Accountability

Summary

Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in clinical governance, service planning and performance management.

It is therefore of paramount importance to ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability provide a robust governance framework for information management.

General Data Protection Regulations (GDPR)

Steyning Medical Practice recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. Steyning Medical Practice fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard both personal information about patients and staff and commercially sensitive information. Steyning Medical Practice also recognises the need to share patient information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and, in some circumstances, the public interest.

Steyning Medical Practice believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of all clinicians and managers to ensure and promote the quality of information and to actively use information in decision making processes.

The Organisation is aware of and will adhere to the **General Data Protection Regulations (GDPR)**

Article 5 of the GDPR states that *"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."* and that *"Personal data shall be:*

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

b) 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;

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

d) 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;

e) 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

f) 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."

Steyning Medical Practice has a responsibility to adhere to the principles of the General Data Protections Regulations and will demonstrate compliance by implementing the following measures:

- Contracts.
- Documentation.
- Data protection by design and default.
- Appointing a Data Protection Officer.
- Information Security, including physical security, cybersecurity, personal data breaches.
- Staff awareness and training.
- Retention.

Contracts

Steyning Medical Practice, as a data controller, are liable for our compliance with the GDPR and will only appoint processors that can provide 'sufficient guarantees' that the requirements of the GDPR will be met and the rights of data subjects protected. We will use a processor who adheres to an approved code of conduct or certification scheme.

Processors must only act on the documented instructions of a controller. They will however have some direct responsibilities under the GDPR and may be subject to fines or other sanctions if they don't comply.

Contracts will be revised to reflect the responsibilities and liabilities when GDPR comes into law. The revised contracts will include a standard clause to be provided by the ICO. In addition to this the contract will specify that the data processor in question will:

- Only act on the written instructions of the controller;

- Ensure that people processing the data are subject to a duty of confidence;

- Take appropriate measures to ensure the security of processing;

- Only engage sub-processors with the prior consent of the controller and under a written contract;

- Assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;

- Assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;

- Delete or return all personal data to the controller as requested at the end of the contract; and

- Submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

Responsibilities of the Data processor

A processor must only act on the documented instructions of a controller. If a processor determines the purpose and means of processing (rather than acting only on the instructions of the controller) then it will be considered to be a controller and will have the same liability as a controller.

In addition to its contractual obligations to the controller, under the GDPR a processor also has the following direct responsibilities:

- Not to use a sub-processor without the prior written authorization of the data controller;

- To co-operate with supervisory authorities (such as the ICO);

- To ensure the security of their processing;

- To keep records of processing activities;

- To notify any personal data breaches to the data controller;

- To employ a data protection officer; and

- To appoint (in writing) a representative within the European Union if needed.

If a processor fails to meet any of these obligations, or acts outside or against the instructions of the controller, then it may be liable to pay damages in legal proceedings, or be subject to fines or other penalties or corrective measures.

If a processor uses a sub-processor then it will, as the original processor, remain directly liable to the controller for the performance of the sub-processor's obligations.

Documentation/Data Flow Mapping

Steyning Medical Practice will comply with GDPR article 30(1) and will document in writing and maintain a record of our processing activities, covering areas such as processing purposes, data sharing and retention.

This will include

- A description of the categories of individuals and categories of personal data. The name and contact details of our organisation (and where applicable, of other controllers, our representative and the data protection officer).
- The purposes of our processing.
- The categories of recipients of personal data.
- Details of our transfers to third countries (if any) including documenting the transfer mechanism safeguards in place.
- Retention schedules.
- A description of our technical and organisational security measures.

This will include information that feeds into our 'Privacy notice' such as

- the lawful basis for the processing
- the legitimate interests for the processing
- individuals' rights
- the existence of automated decision-making, including profiling
- the source of the personal data;

The rights available to individuals

- the right to be informed.
- right of access.
- right to rectification.
- right to erasure.
- right to restrict processing.
- right to portability.
- right to object.
- rights related to automated decision making including profiling.

and additional information to comply with transparency

- Controller-processor contracts;
- The location of personal data;
- Data Protection Impact Assessment reports;
- Records of personal data breaches;

- Information required for processing special category data or criminal conviction and offence data under the Data Protection Bill, covering:
- The condition for processing in the Data Protection Bill
- The lawful basis for the processing in the GDPR
- Our retention and erasure policy document.

Data protection by Design and default

Under the GDPR, we have a general obligation to implement technical and organisational measures to show that we have considered and integrated data protection into our processing activities.

Privacy by design has always been an implicit requirement of data protection that the ICO has consistently championed.

We will ensure that privacy and data protection is a key consideration in the early stages of any project that is "likely to result in a high risk". and then throughout its lifecycle. For example when:

- Building new IT systems for storing or accessing personal data;
- Developing legislation, policy or strategies that have privacy implications;
- Embarking on a data sharing initiative; or
- Using data for new purposes.

Steyning Medical Practice will, when embarking on any of the above will complete the Data Protection Privacy assessment template supplied by the Information Commissioners office. Advice with be sought from the Data protection officer who will be informed at the start of the project the findings of which will be documented and will feed directly into asset registers/Documentation

Data Protection Officer (DPO)

Steyning Medical Practice is a 'public authority' for the purposes of the 'Freedom of Information act 2000' and GDPR. Our core activities mean we process special categories of data (health data). For that reason we appoint a data protection officer

Our Data Protection officer is Charlotte Barrie (cwsccg.steyning-steyning@nhs.net)

The role of the Data protection officer is;

- To inform and advise you and your employees about your obligations to comply with the GDPR and other data protection laws;
- To monitor compliance with the GDPR and other data protection laws, and with your data protection polices, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits;
- To advise on, and to monitor, data protection impact assessments;
- To cooperate with the supervisory authority; and
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.).

The Data protection Officer involved, closely and in a timely manner, in all data protection matters, and will report to the highest level of management of the organisation.

The GDPR requires the organisation to publish the contact details of our DPO via our Privacy notice and provide them to the ICO. This is to enable individuals, and employees and the ICO to contact the DPO as needed.

Codes of conduct and certification

Steyning Medical Practice will adhere to any codes of conduct or certification scheme that become available that cover our processing activity. Adhering to these codes of conduct and certification schemes will demonstrate with:

- Improve transparency and accountability - enabling individuals to distinguish the organisations that meet the requirements of the law and they can trust with their personal data.
- Provide mitigation against enforcement action; and
- Improve standards by establishing best practice.
- When contracting work to third parties, including processors, we will consider whether they have signed up to codes of conduct or certification mechanisms.

Information Security

Steyning Medical Practice will establish and maintain policies for the effective and secure management of its information assets and resources.

- The Organisation will undertake or commission annual assessments and audits of its information and IT security arrangements.
- We undertake an analysis of the risks presented by our processing, by completing the **Data Security and Protection toolkit** and use this to assess the appropriate level of security we need to put in place.
- We make sure that we regularly review our information security policies and measures and, where necessary, improve them.
- The Organisation will promote effective confidentiality and security practice to its staff through policies, procedures and training.
- The Organisation will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.
- We will report personal data breaches to the ICO within 72 hours of being aware of them.
- We will use encryption and/or pseudonymisation where it is appropriate to do so.

When considering physical security, the organisation will take into account

- the quality of doors and locks, and the protection of our premises by such means as alarms, security lighting or CCTV;
- how we control access to our premises, and how visitors are supervised;
- how we dispose of any paper and electronic waste; and
- how we keep IT equipment, particularly mobile devices, secure.

When considering cybersecurity, the organisation will take into account:

- system security – the security of our network and information systems, including those which process personal data;
- data security – the security of the data we hold within our systems, eg ensuring appropriate access controls are in place and that data is held securely;
- online security – eg the security of our website and any other online service or application that we use; and

Personal Data Breaches

Steyning Medical Practice will report certain types of personal data breaches to the relevant supervisory authority. We will do this within 72 hours of becoming aware of the breach, where feasible.

- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we will also inform those individuals without undue delay.
- We will ensure we have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not we will need to notify the relevant supervisory authority and the affected individuals.
- We will also keep a record of any personal data breaches, regardless of whether we are required to notify.

Staff awareness and training

The GDPR requires that when acting under our authority with access to personal data staff will not process that data unless we have instructed them to do so. It is therefore vital that our staff understand the importance of protecting personal data, and are familiar with our security policy and put its procedures into practice.

Steyning Medical Practice provides appropriate initial and refresher training either online, internally or will commissioning appropriate training, which will enable staff so that;

- They have knowledge on our responsibilities as a data controller under the GDPR;
- They know and understand their staff responsibilities for protecting personal data – including the possibility that they may commit criminal offences if they deliberately try to access or disclose these data without authority;
- They are informed of the correct procedures to identify callers;
- They are made aware of the dangers of people trying to obtain personal data by deception (eg by pretending to be the individual whom the data concerns, or enabling staff to recognise 'phishing' attacks), or by persuading our staff to alter information when they should not do so; and
- They are aware of and observe any restrictions you place on the personal use of your systems by staff (eg to avoid virus infection or spam).

Retention Policies

Information relating to individuals and staff will be held in accordance with the NHS Records Management Code of Practice for Health and Social Care.