PHGH Doctors

Data Protection and Cyber Security Policy

Version 1 Revised Sep 2022

CONTENTS

1. Introduction

1.1 The practice is required as part of its overall information governance structure to ensure that appropriate controls are implemented and maintained in relation to the collection, use and retention of personal information pertaining to its patients, workforce, contractors and others upon whom we retain personal data; and that these are in accordance with the requirements of the current data protection law as enacted. The Data Protection Act 2018 and the UK General Data Protection Regulations 2016 form the key portions, although other legislation also applies.

1.2 This document provides a framework for the practice workforce to meet legal and corporate requirements in relation to information requests that fall within the scope of the legislation.

1.3 The Policy applies to all personal information created, received, stored, used and disposed of by the practice irrespective of where or how it is held.

1.4 The regulations noted above mandate that the practice protects its data appropriately against cyber security risks as well as general data risks.

1.5 It must be noted that compliance is a **legal** requirement and that the practice and individuals can face prosecution for breaches of its Principles.

2 Aim of the Policy

2.1 The aim of this document is to clarify the practice's legal obligations and requirements for the processing of personal data and to ensure that all such data is:

- collected, stored and processed for justifiable reasons under the law
- has appropriate legal basis or informed consent for use, and is not combined with other data or used for other purposes without appropriate legal basis or consent
- used only by those persons with a legitimate reason for access
- stored safely and securely
- retained only for the defined time period
- not disclosed to unauthorised persons, and transfers to authorised persons recorded

2.2 The practice will actively seek to meet its obligations and duties in accordance with the law and in so doing will not infringe the rights of its workforce, patients, third parties or others.

2.3 The practice will ensure it remains compliant with the Data Security and Protection standards required by the NHS, along with (when published) the UK Minimum Cyber Security Standards.

3 Scope

3.1 The scope of this policy requires compliance with the principles defined in law. These are summarised below.

Personal Data is defined as: personal data relating to an identifiable living individual and includes the 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.

Special category personal data is defined as personal data consisting of information as to:

- racial or ethnic origin
- political opinions
- religious or other beliefs
- trade union membership
- biometric data for the purposes of uniquely identifying a living individual
- Genetic data
- physical or mental health or condition
- sexual life
- commission of criminal offences or alleged offences.

3.2 Special category personal data may only be stored or processed for a limited variety of purposes. All processing of special category personal data without a legal basis for use must be cleared by the Information Commissioner's Office.

3.3 All personal data must be protected, and special category personal data may require stronger protection measures.

3.4 Changes to use or new uses of personal data require consultation with the Data Protection Officer. Their advice must be recorded and if dissented from, the dissent and alternate action taken recorded.

4 Data protection principles

4.1 The UK GDPR includes principles which must be adhered to whenever personal data is processed. Processing includes obtaining, recording, using, holding, disclosing and deleting personal data.

4.2 All personnel processing personal information in the course of their business functionality must ensure they adhere to the principles in the UK GDPR Article 5 which require that:

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject **('lawfulness, fairness and transparency');**

(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, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes **('purpose limitation');**

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed **('data minimisation');**

(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 **('accuracy');**

(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 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 **('storage limitation').** Note that there are additional requirements on location of storage and processing elsewhere in the laws**;**

(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 ('**integrity and confidentiality').**

2.The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 **('accountability').**

Further information on the principles can be found on the Information Commissioner's Office website

5 The Information Commissioner's Office

5.1 The Information Commissioner administers Data Protection in the UK. The role and duties of the Commissioner include:

- ensuring compliance with the law
- ensuring that individuals rights to privacy are respected
- ensuring that individuals have access to data held about themselves
- establishing and maintaining a Register of data users and making it publicly available
- investigating complaints, serving notices on registered data users who are contravening the principles of the Act, and where appropriate prosecute offenders.

5.2 The law gives the Information Commissioner wide powers to ensure compliance, including warrants to search and seize documents and equipment.

6 Access and use of personal data

6.1 This policy applies to everyone that has access to personal data, and includes any third party or individual who conducts work on behalf of The practice or who has access to personal data for which The practice is responsible and who will be required contractually or otherwise to comply with this policy.

6.2 Deliberate unauthorised access to, copying, disclosure, destruction or alteration of or interference with any computer equipment or data is strictly forbidden and may constitute a criminal and/or a disciplinary offence.

6.3 It is an offence for any person to knowingly or recklessly obtain, procure or disclose personal data, without the permission of the data controller (The practice) subject to certain exceptions.

6.4 It is also an offence for someone to sell or offer to sell personal data.

6.5 All data subjects are entitled to:

- Know what information the practice holds and processes about them and why it is held
- Know who can gain access to it, who it is shared with and where it is stored
- How to keep this data up-to-date
- Know what action the practice takes to comply with its obligations

6.6 All data subjects may request erasure of data which they feel is no longer relevant. This is not an absolute right and all requests will be considered individually.

6.7 The practice will ensure that compliance with this Policy is monitored and the practice is able to evidence that it is complying with its legal responsibilities.

7 Practice commitment

7.1 To achieve the overall aim of the Data Protection Policy the practice will:

- Provide adequate resources to support an effective corporate approach to Data Protection.
- Respect the confidentiality of all personal information irrespective of source.
- Publicise the practice's commitment to Data Protection.
- Compile and maintain appropriate procedures and codes of practice.
- Record all data protection incidents on the Data Security and Protection Toolkit
- Promote general awareness and provide specific training, advice and guidance to its workforce at all levels and.

- Monitor and review compliance with legislation, national policy and guidance and introduce changes to policies and procedures where necessary.

8 Roles and responsibilities

8.1 The **Data Subjects** are those natural persons about whom the practice retains information.

8.2 Ultimate accountability for all decisions made relating to Data Protection lies with the **Practice Board**.

8.3 The **Practice Board** are responsible for ensuring that sufficient resources are provided to support the requirements of this policy as well as making strategic level decisions which impact on how the practice carries out its obligations under the legislation. The **Practice Manager** is responsible for monitoring compliance and taking any necessary corrective action.

8.4 The **Practice Board** monitors, oversees, reports and makes decisions on all strategic level DP issues.

8.5 The **Senior Information Risk Officer (SIRO)** has the delegated responsibility for the day-to-day risk management and acceptance for the practice.

8.6 The **Caldicott Guardian** has the statutory responsibility to ensure that patient data is used and shared appropriately, and with monitoring compliance with the Caldicott Guidelines.

8.7 The **Practice Manager** has the role of handling requests for data (Subject Access Requests, Freedom of Information Requests, etc.) and complaints about the use of data. The **Practice Manager** will also maintain and provide reporting to the **Practice Board** on these issues.

8.8 The **Data Protection Officer** (DPO) will provide advice and guidance in on legal compliance and best practice. Advice of the DPO must be sought for all new or changed data uses; this advice must be formally recorded and if not followed, this fact must also be recorded. The DPO acts as the liaison between the ICO and the practice, as well as the public and the practice if required. The DPO also acts as independent reviewer/advisor on complaints and provides a lead for raising awareness of Data Protection issues.

8.9 **The Practice Workforce** (permanent/fixed-term staff, temporary staff, volunteers) have a responsibility to ensure that they have sufficient awareness of the data protection law so that they are able to comply with the requirements of the law.

9 Responsibilities of Practice Workforce

9.1 The processing of personal data is to be compliant with legal, industry, regulatory and business requirements; it is the responsibility of each individual to be aware of and conversant with these requirements for the processing and management of personal data in an appropriate manner.

9.2 Some data supplied by others will have handling requirements beyond the practice's normal criteria. Workforce involved must be made aware of this by the Practice Manager and are then responsible for handling it correctly.

9.3 The following minimum requirements are applied to everyone who comes into contact with personal data and / or uses practice data systems:

- Workforce are to ensure that personal data is to be processed accurately
- When not required for immediate use personal data is to be secured from unauthorised viewing and access
- All devices in the practice are subject to protection from malicious software, and staff must not bypass this protection. Staff may not install software on any device without the authority of the IT supplier to the practice or the SIRO.
- Staff must take great care when opening emails to ensure that they do not introduce risks by clicking on links or opening attachments where the source is not well-known and expected. In the event of an incident, staff must report it immediately to the practice manager, SIRO or in their absence the DPO.
- Personal data must not be sent to/from personal (non-work) email accounts
- Personal data may be shared with other NHS bodies as appropriate via internal systems and via NHS.NET mail
- Personal information can only be distributed externally if it is:
    - being sent to someone with an appropriate data sharing or processing agreement with the practice, a legal right to access and a need to know
    - sent via NHS.Net mail with "[SECURE]" in the subject line (unless otherwise agreed with the data subject
    - otherwise securely distributed as agreed with the DPO.
- Computer systems that process, access or store such data are to have password protected screen savers activated when left unattended, and all data should be encrypted at rest.
- The carrying of personal, special category or confidential information outside practice environments should be avoided wherever possible. If this is unavoidable, then encryption of the device and device management by the practice or their appointed contractor is required. Paper based documents holding personal or special category information must be concealed from public view in transit and held securely when stored.
- Personal devices e.g. mobile phones may only be used where allowed by the SIRO and must be password protected and encrypted. Such devices must be kept up-to-date with software and malware protection. Devices where the software is unsupported (e.g. older versions of operating systems / packages) must not be used.

- When no longer required to be retained all personal data is to be disposed of securely, i.e. by shredding or via secure waste disposal.

- Personal data may not be stored on removable media devices without explicit management approval and appropriate encryption controls. Such data is to be removed from the removable media as soon as practically possible.

- The discussion of personal data with unauthorised persons either inside or outside the practice is expressly prohibited. This also includes, but is not limited to, email, social networking sites, blogs, forums, instant messaging services, chat rooms etc.

- Staff are required to report any breaches of personal data to management immediately on discovery. A "no-blame" approach will be taken to such reports.

- Staff are required to complete the training on NHS data management on joining the organisation and as required thereafter.

10 Data Controller

10.1 In accordance with the law, the practice as a corporate body is the Data Controller and is therefore ultimately responsible for the implementation of this policy.

10.2 The responsibilities of data controllers are laid out in the law, in particular Chapter IV of the UK GDPR.

10.3 The responsibilities of data controllers include, but are not limited to:

- Using appropriate organisational and technical measures to ensure and demonstrate that processing is within the law. This will include privacy notices, records of processing activities, data protection impact assessments and contractual documentation.

- Ensuring "data protection by design and default" including appropriate measures to ensure that measures are in place to provide necessary safeguards and protect the rights of individuals. This may include, where needed, Data Protection Impact Assessment. The appropriate measures will include those in the Data Security and Protection Toolkit, and, when published, the Minimum Cyber Security Standard.

- Ensuring that all processing with other controllers is done in a transparent manner including arrangements to designate roles and responsibilities. A suitable measure may include Data Sharing Agreements.

- Ensuring that any processors used provide sufficient guarantees to implement appropriate organisational and technical measures on behalf of the controller, and that the arrangement is clearly laid out in a contract (Data Processing Agreement)

- Ensure that any data breaches are recorded, and, if necessary, reported to the Information Commissioner within 72 hours.

11 Data Protection Officer

11.1 The DPO is responsible for fulfilling the role as documented in the data protection law.

11.2 The DPO must be involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

11.3 The DPO is invited to participate at the federation and CCG level regularly in meetings regarding data protection. Their presence is recommended where decisions with data protection implications are taken. All relevant information must be passed on to the DPO in a timely manner in order to allow them to provide adequate advice.

11.4 The opinion of the DPO must always be given due weight. In case of disagreement, the reasons for not following the DPO's advice must be recorded and formally communicated.

11.5 The DPO must be promptly consulted once a data breach or another incident has occurred which has a significant risk to the rights and freedoms of individuals.

11.6 The DPO will keep the practice informed of data protection issues pertaining to the practice and NHS in general, including any changes in legislation that might impact business processes.

12 Collection of Data

14.1 The practice collects and records personal data from various sources, including that obtained or provided by the data subjects themselves.

14.2 In some instances, data may be collected indirectly through monitoring devices, including but not limited to: door access control systems, CCTV, personal recording devices and physical security logs or electronic monitoring systems. For further detail refer to practice privacy notice.

13 Accuracy and relevance

15.1 It is the responsibility of those who receive personal information to ensure so far as possible, that it is accurate and up to date. Personal information should be checked at regular intervals, to ensure that it is still accurate.

15.2 If the information is found to be inaccurate, steps must be taken to rectify it. Individuals who input or update information must also ensure that it is adequate, relevant, unambiguous and professionally worded. Data subjects have a right to access personal data held about them and have inaccuracies corrected.

14 Rights to access, correct and remove information

14.1 Data subjects have the right to access any personal information (data) about them that is held.

14.2 Data subjects also have the right to have data about themselves corrected or erased subject to certain conditions.

14.3 The practice aims to comply with requests as quickly as possible but will ensure that it is provided within one calendar month unless there is a good reason for any delay. In such cases the reason for a delay will be explained in writing to the person making the request.

15 Fair and Lawful Processing

15.1 When the practice processes personal data, it must have a legal basis for doing so or a freely given, positive consent. The law provides a list of conditions to ensure that personal information is processed fairly and lawfully:

- Personal information is only processed where it is justified, and this is transparent to the data subject.
- Information on the processing is easily accessible and easy to understand, in clear and plain language.
- That data subjects are aware of risks, rules, safeguards and rights in respect of processing and how to exercise their rights.
- That the minimum amount of personal data is kept, and for as short a period as possible.
- That special category personal information is processed only where necessary and justified, and with permission for this from the ICO unless a legal basis for processing is used.

15.2 Individuals that supply the practice with personal information are provided with a 'Privacy Notice' (or online privacy statement) at time of data collection, repeated at time of SAR, which communicates the following:

- Purposes, categories, recipients (esp. outside country)
- Period of storage
- Existence of the right to request rectification, erasure and to object to processing
- Right to complain to supervisory authority and contact
- Information on communication and source
- Information on significance and consequences of processing

16 Data Sharing

16.1 Where the practice shares personal information with any third party a 'Data Sharing Agreement' or 'Data Processing Agreement' must exist as part of a formally documented written agreement or contract.

16.2 A 'Data Sharing Agreement' is required if the information supplied is being used to fulfil requirements of the recipient.

16.3 A 'Data Processing Agreement' is required if the information supplied is being used only to fulfil The practice requirements and not used otherwise by the recipient.

16.4 Where the other party uses the personal information for its own purposes (Data Sharing):

- The agreement or contract will clearly describe the purposes for which the information may be used and any limitations or restrictions on the use of that information
- The other party is to provide an undertaking or provide other evidence of its commitment to process the information in a manner that will not contravene the law

16.5 Where the processing of personal information with a third party is required by law, procedures are to ensure that the protocols and controls for the sharing of the data are documented, regularly reviewed and verified.

16.6 Requests for personal information from the Police or other enforcement agencies can be considered where the purpose is for the prevention or detection of a crime and other legal basis to which the data we hold is subject to exemption. It should be noted however that the practice is not generally under an obligation to provide data. Before providing the information, the requesting agency must provide a sufficient explanation of why the information is necessary to the extent that not providing it may prejudice an investigation. This is to satisfy the relevant information holder that the disclosure is necessary. The request must be on letter headed paper OR via a valid email address (pnn.net for example) and authorised by a senior officer from the requesting agency (Police Inspector or equivalent). If the information is to be disclosed, the disclosure must be authorised by the Practice Manager or a member of the practice board and a note for the record should be made of the details about the disclosure with an explanation of why the disclosure is appropriate. It is recommended to consult the DPO in all such cases.

17 Data retention and disposal

17.1 The practice must ensure that personal information is not kept for any longer than is necessary; this is to adhere to any legal, regulatory or specific business justification.

17.2 The practice will retain some forms of information longer than others, but all decisions are to be based upon business requirements; details can be found in the NHS guidance on Record Retention.

17.3 When disposing of information, equipment or media, the NHS procedures on confidential waste disposal policy and procedures should be adhered to.

17.4 The retention criteria must be imposed on third parties with who data is shared.

18 National Data Opt-Out for Health and Care Data

18.1 A system of opt-out for use of health and care personal data (including pseudonymised data) has been implemented by the NHS. We are required to comply with this. We will therefore:

- Ensure that all data extracts for non-direct care purposes are filtered to remove patients who have opted out
- Ensure that we make patients aware of their rights.
- Where data is being manually extracted for non-care purposes, we will ensure that records are manually checked for opt-out

19 Transfer outside of the UK

19.1 To ensure an adequate level of protection is applied to personal information transferred or processed outside the UK contracts are to include conditions relating to the specific requirements for the protection of the information.

19.2 The practice is responsible for ensuring that 'due diligence' is conducted on the other party, and that adequate and appropriate controls and safeguards are applied for the transfer of the personal information.

19.3 Companies outside the UK are to be required to apply the same controls and requirements as applied within the UK unless they can demonstrate other adequate procedures are implemented to protect the personal information as part of the 'due diligence' process. Periodic reviews of the same are to be conducted to ensure adherence is maintained.

19.4 Specific issues with cloud processing should be recorded by the practice and NHS cloud policy and procedures should be followed.

19.5 Data received by the practice from third parties may have specific storage and use rules that may further restrict where it can be stored or processed.

20 Violations

20.1 Where a cyber or data leakage incident occurs, and are reported in a timely, whistle-blower rules will apply. Not reporting incidents is regarded as a disciplinary matter.

20.2 Unauthorised disclosure of personal data is a disciplinary matter that may be considered a gross misconduct and could lead to termination of employment.

20.3 In the case of third parties unauthorised disclosure could lead to termination of the contractual relationship and in certain circumstances this could give rise to legal proceedings.

20.4 Any failure to follow this Policy must be treated as an incident and investigated in accordance with the NHS Security Incident Reporting Procedure.

21 Supporting Policies

This policy should be read in conjunction with the following policies and procedures:

- NHS Contract and Acceptable Use Policy

- Subject Access Policy and Procedure
- Data Security and Protection Toolkit
- National Data Opt-Out Policy
- (Draft) Minimum Cyber Security Standards