Data protection
& Medical Confidentiality policy

VERSION CONTROL

Version No.	Date Edited	Edited By	Summary of Changes
1.0	29.3.19	Dawn Hambly	Created
1.1	29.8.19	Marina Edwards	Update surgery Name + add version control, update page numbering
1.2	01.09.2020	Dawn Hambly	Checked & Updated

CONTENTS

CLAUSE

March 2019

1. POLICY STATEMENT

1.1 Everyone has rights with regard to how their personal information is handled. During the course of our activities we will collect, store and process personal and special category personal data about our staff and patients and we recognise the need to treat it in an appropriate and lawful manner.

1.2 The types of information that we may be required to handle include details of current, past and prospective employees, suppliers and of course patients. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in Data Protection legislation (the EU General Data Protection Regulation and UK Data Protection Act 2018) and other regulations. The legislation imposes restrictions on how we may use that information.

1.3 In addition to Data Protection legislation, all Practice members are reminded that Patient and staff information is held under legal and ethical obligations of confidentiality. Information provided in confidence should not be used or disclosed in a form that might identify an individual unless the individual is aware and not objecting, or there is a legal duty or overriding public interest reason.

1.4 Although this policy does not form part of any employee's contract of employment and it may be amended at any time, any breach of this policy, the legislation or Patient Confidentiality will be taken seriously and will result in disciplinary action. A breach of confidentiality will almost always be treated as gross misconduct and may result in dismissal without notice.

2. STATUS OF THE POLICY

2.1 Any questions or concerns about the operation of this policy should be referred in the first instance to a Partner.

2.2 If you consider that the policy has not been followed in respect of personal data about yourself or others or patients you should immediately raise the matter with the Practice Manager or a Partner.

3. DEFINITION OF DATA PROTECTION TERMS

If there is any debate then the reference point will be the definitions in the current applicable data protection legislation in the UK.

3.1 **Data** is information which is stored electronically, on a computer, or in structured paper-based filing systems.

3.2 **Data subjects** for the purpose of this policy include all living individuals about whom we hold personal data (including employees and patients). A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

3.3 **Personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in anyone's possession). Personal data can be factual or it can be opinion.

3.4 **Data controllers** are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the legislation. We are the data controller of all personal data used in our business.

3.5 **Data users** include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.

3.6 **Data processors** include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it includes suppliers which handle personal data on our behalf.

3.7 **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

3.8 **Special categories of personal data** (previously sensitive data) includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings (as set out in UK DP Act 2018).

4. DATA PROTECTION PRINCIPLES

Anyone processing personal data must comply with the enforceable principles of good practice. These provide that personal data must be:

(a) Processed lawfully, fairly and in a transparent manner.

(b) Collected for specific, explicit and legitimate purposes and not further processed in a manner that is not compatible with those purposes.

(c) Adequate, relevant and limited to what is necessary for the purpose.

(d) Accurate and where necessary kept up to date.

(e) Not kept longer than necessary for the purpose.

(f) Processed in a manner that ensures appropriate security.

In addition the organisation will maintain 'records of it's processing activities' in addition to this policy as follows:

- Overview of the types of data collected
- How the data is stored
- The purposes it is used for – linked to the lawful basis in Article 6 and 9 of the GDPR
- Regular disclosures of data to other agencies

It will also have records of staff training on data protection and audits done to ensure that it is complying with legislative requirements (such as the Data Security & Protection Toolkit).

The above is set to meet the principle of accountability in the GDPR.

5. LAWFUL, FAIR AND TRANSPARENT PROCESSING

5.1 The legislation is intended not to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is (in this case Dr Glen Micklethwaite (the Data Protection Officer), the purpose for which the data is to be processed by us, and the identities of anyone to whom the data may be disclosed or transferred. They should also be able to access detail on the lawful basis for processing, the retention period of their data and be made aware of their rights and the option to raise concerns with the Information Commissioner's Office.

5.2 For personal data to be processed lawfully, certain conditions have to be met. For the provision of care to patients, the general lawful basis is the 'exercise of official authority' and the 'provision of health and social care services and treatment'. Detailed guidance on lawful basis has been published by the Information Governance Alliance: https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga/general-data-protection-regulation-gdpr-guidance

5.3 To process data on staff, then data is processed on the basis of the contract of employment with staff.

5.4 Where there is no other lawful basis to process data, then for other uses of data, the explicit consent of the individual will be gathered and recorded and they will have full choice over the use of their data in these circumstances.

5.5 All Employees and Partners shall observe strictly the requirements of the Data Protection Act and observe at all times the duty of confidentiality owed to patients. The Sensitive Personal Data

6. PROCESSING FOR LIMITED PURPOSES

In general personal data must not be collected for one purpose and then used for another, unless the other process is closely related and 'compatible' with the main purpose. A way to

review that is to ask if a reasonable person would be surprised by the data being used for a subsequent purpose. If they would be then the data subject must be informed of the new purpose before any processing occurs and an appropriate lawful basis for processing established.

7. ADEQUATE, RELEVANT AND LIMITATIONS ON PROCESSING

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

8. ACCURATE DATA

Personal data must be accurate and kept up to date. Information which is incorrect or out of date is potentially misleading and carries risk of incorrect care provision. Steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Any issues of accuracy or out of date information must be corrected as soon as possible. In health records inaccurate information is likely to be kept, but marked in error and linked to the correct information, it should not be erased without careful consideration of all potential impacts.

9. TIMELY PROCESSING

Personal data should not be kept longer than is necessary for the purpose it was originally collected for. This means that data should be destroyed or erased from our systems when it is no longer required. Before any data is erased or destroyed the appropriate retention period from the NHS Records Management Code of Practice must be checked. A record of destruction of any records should be kept, so that if required to confirm to a regulator then destruction can be documented.

10. PROCESSING IN LINE WITH DATA SUBJECT'S RIGHTS

Data must be processed in line with data subjects' rights. Data subjects have a right to:

(a) Request access to any data held about them by the practice (as Data Controller) – see section 12

(b) Have incorrect data amended or incomplete data completed

(c) Have data erased (forgotten)

(d) Request restrictions on how their data is processed and/or object to processing

(e) Request copies of their electronic data to transfer to another organisation (portability)

(f) Not be subject to decisions made solely by automated means (including profiling)

It should be noted that the above rights are not absolute and there can be valid reasons why a request will not be responded to in the manner expected by the patient. Each case must

be judged on its own merits and specific guidance about reasons for either refusal or a different response checked before the response is given.

All requests must be fully responded to within one calendar month of receipt. However where there is significant complexity in dealing with a request, then the time period can be extended to three months provided the data subject is informed of this and reasons why within the first month. Complexity may arise where there are multiple rights being requested or where there are many complexities in the record in determining whether changes should be made or whether certain data can be released.

11. DATA SECURITY

11.1 We must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.

11.2 Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

(a) **Confidentiality** means that only people who are authorised to use the data can access it.

(b) **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.

(c) **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual PCs.

11.3 Security procedures include (not an exhaustive list):

(a) **Encryption.** This should be used wherever possible, but particularly on mobile devices (laptops, memory sticks etc) and for any transfers of personal data via electronic means

(b) **Psuedonymisation.** Identifying factors in any use of personal data should be kept to a minimum and replaced with a pseudonym where the specific identity does not need to be used.

(c) **Regular reviews of security.** Many security controls can become ineffective if they are not used appropriately, so there should be regular reviews of the effectiveness of security controls.

(d) **Entry controls.** Any stranger seen in entry-controlled areas should be reported.

(e) **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

(f) **Methods of disposal.** Paper documents should be disposed of securely. Floppy disks and CD-ROMs should be physically destroyed when they are no longer required.

Hardware that contains or processes data should be destroyed via an appropriate secure mechanism via a reputable contractor (ideally to ADISA standard)

(g) **Equipment.** Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

12. DEALING WITH SUBJECT ACCESS REQUESTS

If an individual makes a request for information that we hold about them, then this is a Subject Access Request. Any member of staff who receives a request should forward it to the practice manager immediately. Fees cannot be charged unless the requestor is asking for a copy of information they have already received. As with any data subject request, response must be given within one calendar month, unless the request is deemed complex.

Data that may cause harm or distress to the data subject or another party can be redacted before it is provided. Additionally data related to a third party (but not care professionals or staff in their professional role) must be carefully checked before the response is provided. Third party data with any degree of confidentiality should either be removed or only disclosed with the consent of the third party.

For more guidance see: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

13. PROVIDING INFORMATION OVER THE TELEPHONE

Any member of staff dealing with telephone enquiries should be careful about disclosing any personal information held by us. In particular they should:

(a) Check the caller's identity to make sure that information is only given to a person who is entitled to it.

(b) Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.

(c) Refer to the Practice Manager or a Partner for assistance in difficult situations. No-one should be bullied into disclosing personal information especially medical records or details of treatment about any patient.

14. MONITORING AND REVIEW OF THE POLICY

14.1 We will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives.