SHAY LANE MEDICAL CENTRE DATA PROTECTION POLICY

Introduction

The Practice complies with the legal obligations of the Data Protection Act 2018 (the '2018 Act') and the EU General Data Protection Regulation ('GDPR'). The Practice gathers and uses data about workers, employees and consultants, both to manage our relationships with these individuals and in the course of conducting our business.

This Data Protection Policy applies to 'Data Subjects'; who are defined as the 'subject' of the data which include: employees, workers, volunteers, consultants, apprentices, patients or any other any other individual for whom records are created, held or processed by the 'Data Controller'.

The Practice is a ***'Data Controller'***[1] and any staff members, volunteers or associates who are provided with legitimate access to the 'data', electronic or paper, are referred to as '***Data Processors***'.

Supplementary Policies and documents

The following sub-policies and documents support the overarching Practice Data Processing Policy:

- Privacy Notices
- Data sharing agreements
- Privacy impact assessments
- Records retention policy
- Data security procedure
- Patient facing data protection policy information documentation / Data subjects rights
- Third party data processor agreements
- Asset register
- Records retention policy
- Staff and third party data processer responsibilities

In line with our **records retention policy** and **data security procedure**, the Practice has measures in place to protect the security of individuals' data. Policy documentation can be obtained from the Practice Manager.

The Practice will retain data in accordance with our records retention policy and data will only be held for as long as is necessary for the purposes it has been collected.

This policy has been created to be fully compliant with the 2018 Act. Where any conflict arises between those laws and this policy, the Practice will comply with the 2018 Act.

The Six Data Protection Principles

The Practice processes personal data in accordance with the six Data Protection Principles of the 2018 Act identified by the ICO, in that data will be:

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

- 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');

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

- 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');

- 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');

- 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').

Personal Data

The Practice processes Personal Data, within the authority of Article 6 1(e) of the '2018 Act'; in that data "*processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller*"

'Personal data' is defined as information relating to a living person ('data subject') that can be used to identify them on its own, **or** in combination with other information likely to be collected by the Practice. This applies whether the information is stored physically, electronically, or in any other format.

It **does not** include anonymised data, but **does** include any expression of opinion about the person, or any indication of the intentions of the Practice or others, in respect to that individual.

Personal data might be provided to the Practice by the individual (data subject), or third party (such as a previous employer, external primary or secondary care provider, NHS Spine, Social Services or other organisation) or it could be created by the Practice. It could be provided or created as part of a consultation, clinical referral or staff employment process.

Under the provision contained within Article 6,1(e) of the 2018 Act the Practice may collect and use the following types of personal data, within the constraints of the Six Data Protection Principles', without the requirement of the 'Data Subjects' explicit consent::

Patient Services:

- Patient demographic data which promotes local and national government Health and Social Care strategies.
- Any other category of personal data which we may notify you of from time to time Contact details and date of birth;
- Identification documents e.g. passport; information in relation to immigration status; driving licence;
- Images (whether captured on CCTV, by photograph or video);

Employment Records:

- Recruitment information e.g. application form, CV, references, qualifications etc.;
- Emergency contact details;
- Identification documents e.g. passport; information in relation to immigration status; driving licence; and right to work for the Practice staff;
- Gender, marital status and family status;
- Information regarding their contract of employment (or services) e.g. start and end dates of employment; working hours; role; location; pension; benefits; holiday entitlement; and salary (including details of previous remuneration);
- Bank details and information in relation to tax status, including National Insurance number;
- Information relating to disciplinary or grievance investigations and proceedings involving them (whether or not they were the main subject of those proceedings);
- Electronic information in relation to their use of IT systems/SMART cards/telephone systems;
- Information relating to an employee's performance and behaviour at work;
- Images (whether captured on CCTV, by photograph or video);
- Training records;

Special Categories of Personal Data

The Practice processes Personal Data, within the authority of Article 9 2(h) of the '2018 Act'; in that data "*processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3*.[ii]

These comprise personal data consisting of information relating to:

Patient Services & Employment Records:

- Racial or ethnic origin;
- Religious or philosophical beliefs;
- Trade union membership (Staff only);

- Genetic or biometric data;
- Health;
- Sex life and sexual orientation; and
- Criminal convictions and offences.

The Practice may hold and use any of these special categories of your personal data in accordance with the law.

Processing Personal Data

'Processing' means any operation which is performed on personal data such as:

- Disclosure by transmission, dissemination or otherwise making available;
- Alignment or combination;
- Collection, recording, organisation, structuring or storage (e.g. within a filing system);
- Adaption or alteration;
- Retrieval, consultation or use; and
- Restriction, destruction or erasure.

The Practice will process individuals' personal data (including special categories of personal data) in accordance with the obligations prescribed under the 2018 Act, including:

- Performing 'direct care' functions to patients[iii]
- Complying with any legal obligation; or;
- If it is necessary for the Practice's legitimate interests (or for the legitimate interests of someone else). The Practice can only do this in circumstances where the individual's interests and rights do not override those of the Practice (or their own). Individuals have the right to challenge the Practice's legitimate interests and request that this processing be halted.
- Performing the contract of employment (or services) between the Practice and the individual.

The Practice may process individuals' personal data for these purposes without your knowledge or consent. The Practice will not use your personal data for an unrelated purpose without informing you about it and the legal basis for processing it.

Please note that if individuals opt not to provide the Practice with some personal data, the Practice may be unable to carry out certain parts of the contract between us, e.g. the Practice needs staff members' bank account details in order to pay them and patient's personal, address and contact details.

When the Practice Might Process Personal Data

The Practice is required to process patients, staff and contracted associates personal data in various situations including: the provision of direct care and staff recruitment, employment (or engagement) and even following termination of their employment (or engagement) for reasons including but not limited to:
Patient Services:

- Provision and management of patient's direct care by the Practice;

- Patient's referral to trusted heath, mental health and social care partners;[iv]
- Monitoring and protecting the security (including network security) of the Practice, staff, patients and others;
- Preventing and detecting fraud or other criminal offences;

Employment Records:

- Facilitating legal obligations during staff recruitment;
- Processing contractual employment obligations;
- Fulfilling legal obligations during the processing and payment of staff pension tax and national insurance;
- Ensuring staff have the legal right to work for the Practice;
- Carrying out a disciplinary or grievance investigation or procedure in relation to them or someone else;
- Monitoring and protecting the security (including network security) of the Practice, staff, patients and others;
- Providing a reference upon request from another employer;
- Preventing and detecting fraud or other criminal offences;

The Practice may process special categories of personal data for reasons including but not limited to:

Patient Services:

- Provision and management of patient's direct care by the Practice;
- Patient's referral to trusted heath, mental health and social care partners;

Employment Records:

- Facilitating legal obligations during staff recruitment and subsequent employment;
- Carrying out a disciplinary or grievance investigation or procedure in relation to them or someone else;
- Facilitating legal obligations during staff recruitment and subsequent employment including, but not limited to: sickness absence, health and medical conditions to monitor staff absence, assess staff fitness for work, to pay you benefits, to comply with our legal obligations under employment law including making reasonable adjustments and provide a safe working environment;

The Practice will only process special categories of individuals' personal and special category data in certain situations in accordance with the law. If the Practice requires explicit consent to process data, the reasons for the request will be explained. Individuals do not need to consent and can withdraw consent later if they choose by contacting the Practice Manager.

The Practice does not need consent to process special categories of individuals' personal data when it is processed it for the following purposes:

- When data is being processed under Article 9 2(h) of the '2018 Act'
- Where it is necessary for carrying out rights and obligations under employment law;
- Where it is necessary to protect individuals' vital interests or those of another person where one or both parties are physically or legally incapable of giving consent;
- Where the individual has made the data public;
- Where processing is necessary for the establishment, exercise or defence of legal claims; and
- Where processing is necessary for the purposes of occupational medicine or for the assessment of the individuals' working capacity.

All staff employment checks, including those for criminal records, will be carried out in line with the guidance from NHS Employers, available at:

www.nhsemployers.org/your-workforce/recruit/employment-checks/criminal-record-check.

Sharing Your Personal Data

Your data held may be shared, within the constraints of Article 6 1(e) and Article 9 2(h) of the '2018 Act', with 'trusted' third parties within the limitation of a Data Sharing Agreement between the Practice and the third party without the requirement for explicit consent; details of such third parties will be published and be available on the Practice's website

Sometimes the Practice may recommend the use of patient's personal data in the promotion of clinical research and the use of the data cannot be categorised as 'direct care' of a patient. In these instances potentially affected patients will be contacted directly, through the use of approved encrypted mail distribution services, inviting the patient to provide their explicit consent to participate.

The Practice *does not* send your personal data outside the European Economic Area. If this changes you will be notified and the protections in place to protect the security of your data will be explained.

Processing Personal Data for the Practice – Staff Responsibilities

All staff who work for, or on behalf of, the Practice has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this Data Protection policy and the Practice's Records Retention Policy[*] and Computer and Data Security Procedure[*].

The Practice's Data Protection Manager is responsible for reviewing this policy and updating the Managing Partners on the Practice's responsibilities for data protection, and any risks in relation to the processing of data. Any questions related to this policy or data protection should be directed to the Practice Manager.

Handling Data Breaches

The Practice has robust measures in place to minimise and prevent data breaches from occurring. Should a breach of personal data occur, the Practice will make note of the relevant details and circumstances, and keep evidence related to that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals then the Practice will notify the Information Commissioner's Office within 72 hours.

If you are aware of a data breach you must contact [insert name and role] immediately and retain any related evidence to the breach that you may have.

Subject Access Requests

Data subjects can make a Subject Access Request ('SAR') to access the information the Practice holds about them. This request must be made in writing. If staff receive a SAR they should forward it immediately to the Practice Manager, who will prepare a response.

The Practice will respond within one month unless the request is complex or numerous – if this is the case, then the Practice will need more time to complete the request, and can extend the response period by a further two months.

A Subject Access Request does not incur a fee, however, if the request is deemed to be manifestly unfounded or excessive then Practice is entitled to charge a reasonable administrative fee, or refuse to respond to the request.

Data Subjects' Rights

In most situations the Practice will not rely on your consent as a lawful ground to process data. If the Practice does request your consent to the processing of your personal data for a specific purpose, you have the right to decline or withdraw your consent at a later time. To withdraw consent, you should contact the Practice Manager.

Data subjects have the right to information about what personal data the Practice processes, how it is processed and on what basis.

If you have a complaint about how your data is processed that cannot be resolved with the Practice, you have the right to complain to the Information Commissioner. You can do this by contacting the Information Commissioner's Office at www.ico.org.uk.

Where your personal data is being corrected or erased, or the Practice is contesting the lawfulness of the processing, you can apply for its use to be restricted while the application is made. In this case please contact the Practice Manager.

Resources

Information Commissioner's Office website
www.ico.org.uk
NHS Employers guidance on criminal checks
www.nhsemployers.org/your-workforce/recruit/employment-checks/criminal-record-check
Records Retention Policy [*]
Computer and Data Security Procedure [*]

Annexes

A. Privacy Notices
B. Data sharing agreements
C. Privacy impact assessments
D. Records retention policy
E. Data security procedure-
F. Patient facing data protection policy information documentation
G. Patient consent forms

H. Third party data processor confidentiality agreement
I. Data subjects rights
J. Asset register
K. Intentionally Left Blank
L. Staff responsibilities
M. Patient responsibilities

[i] https://gdpr-info.eu/art-24-gdpr/

[ii] Personal data referred to in ……point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

[iii] "activities that directly contribute to the diagnosis, care and treatment of an individual. The direct care team is made up of those health and social care professionals who provide direct care to the patient, and other, such as administrative staff who directly support direct care. "When healthcare professionals, or someone working or support the healthcare professional, is providing direct care they have a legitimate relationship with the patient. https://www.bma.org.uk/collective-voice/policy-and-research/ethics/protecting-patient-information

[iv] Details of the Practice's 'Trusted' Partners along with Data Sharing Agreements and Privacy Impact Statements are contained under separate cover.