Care Quality Commission (CQC) - FUNDAMENTAL STANDARDS

Policy title:	**GDPR Data Protection (Patient data).**

Outcome:	**All data relating to individual confidential health held within patients' healthcare records at Street Medical Practice is stored and handled securely and confidentially in line with current legislation.**
Target audience:	**All members of Street Medical Practice, whether employed full-time or part-time, paid or unpaid, granted practising privileges, volunteers, students, and external contractors.**
Authorised by:	**Dr Debbie Street, Medical Director** **(CQC Registered Manager)**
Date issued:	**1 August 2018**
Next review date:	**31 July 2019** (or before if there is a change in practice or circumstances)
Signature:	

Person responsible for data protection at Street Medical Practice:

Dr Debbie Street

1. Introduction.

1.1 This policy sets out the obligations of Street Medical Practice independent healthcare service regarding data protection and the rights of people who use its independent healthcare service.

People who use the service include:

- patients
- patients' relatives
- patients' carers, or
- patients' representatives

(also referred to as '*data subjects*) in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation ('*GDPR*').

1.2 The GDPR defines '*personal data'* as any information relating to an identified or identifiable natural person (*for the purposes of this policy, this is a* '*patient'*).

An identifiable natural person is one who can be identified, directly or indirectly, in particular 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.

1.2 This policy sets out Street Medical Practice's obligations regarding the collection, processing, transfer, storage, and disposal of patients' personal data.

1.4 The procedures and principles set out must be followed at all times by Street Medical Practice as an independent healthcare provider organisation, its employees, external contractors, or any other relevant parties working on behalf of Street Medical Practice.

1.5 Street Medical Practice is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all patients' personal data, respecting the legal rights, privacy, and trust of all patients with whom it deals.

2. The Data Protection principles.

2.1 This policy aims to ensure compliance with the GDPR. The GDPR sets out

the following principles with which any party handling patients' personal data must comply. All patients' personal data at Street Medical Practice must be:

- processed lawfully, fairly, and in a transparent manner in relation to patients
- collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that any personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay
- kept in a format which permits identification of patients for no longer than is necessary for the purposes for which their personal data is processed. *(Patients' 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 the patient.),* and
- 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.

3. The rights of patients.

3.1 The GDPR sets out the following rights applicable to patients as patients (please refer to the parts of this policy indicated for further details):

- The right to be informed (Part 12).
- The right of access (Part 13).
- The right to rectification (Part 14).
- The right to erasure (also known as the 'right to be forgotten') (Part 15).
- The right to restrict processing (Part 16).
- The right to object (Part 17).

4. Lawful, fair and transparent data processing.

4.1 The GDPR seeks to ensure that patients' personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the patient.

The GDPR states that processing of patients' personal data shall be lawful if at least one of the following applies:

- the patient has given consent to the processing of their personal data for one or more specific purposes

- the processing of the data is necessary for the performance of a contract to which the patient is a party, or in order to take steps at the request of the patient prior to entering into a contract with them

- the processing is necessary for compliance with a legal obligation to which the data controller is subject

- the processing is necessary to protect the vital interests of the patient or of another natural person

- the 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 data controller, or

- the processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the patient which require protection of personal data, in particular where the patient is a child.

4.2 If the patients' personal data in question is known as '*special category data*' (also known as '*sensitive personal data*') (for example, data concerning the patient's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation), at least one of the following conditions must be met:

- the patient has given their explicit consent to the processing of such data for one or more specified purposes (unless EU or EU Member State law prohibits them from doing so)

- the processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the patient in the field of employment, social security, and social protection law (insofar as it is authorised by EU or EU Member State law or a collective agreement pursuant to EU Member State law which provides for appropriate safeguards for the fundamental rights and interests of the patient)

- the processing is necessary to protect the vital interests of the patient or of another natural person where the patient is physically or legally incapable of giving consent

- the data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the patients

- the processing relates to patients' personal data which is clearly made public by the patient

- the processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity

- the processing is necessary for substantial public interest reasons, on the basis of EU or EU Member State law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the patient

- the processing is necessary for the purposes of:

    - preventative or occupational medicine

    - for medical diagnosis

    - for the provision of health or social care or treatment, or

    - the management of health or social care systems or services on the basis of EU or EU Member State law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the GDPR

- the processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of EU or EU Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the patient (in particular, professional secrecy), or

- the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the GDPR based on EU or EU Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the patient.

5. Specified, explicit, and legitimate purposes.

5.1 Street Medical Practice collects and processes patients' personal data set out in Part 18 of this policy. This includes personal data collected directly from patients from consultation or treatment appointments.

5.2 Street Medical Practice only collects, processes, and holds patients' personal data for the specific purposes set out in Part 18 of this Policy.

5.3 Patients are kept informed at all times of the purpose or purposes for which Street Medical Practice uses their personal data. *(Please refer to Part 12 for more information on keeping patients informed.)*

6. Adequate, relevant, and limited data processing.

6.1 Street Medical Practice will only collect and process patients' personal data for, and to the extent necessary, for the specific purpose of which patients have been informed as under Part 5, above, and as set out in Part 18, below.

7. Accuracy of data and keeping data up-to-date.

7.1 Street Medical Practice shall ensure that all patients' personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of patients' personal data at the request of a patient, as set out in Part 14, below.

7.2 The accuracy of patients' personal data shall be checked when it is collected. Patients will be asked to confirm that the information they have provided is correct and accurate. If any patients' personal data is found to be inaccurate, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

8. Data retention.

8.1 Street Medical Practice shall not keep patients' personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.

8.2 When patients' personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay. Paper records will be confidentially shredded; electronic records will be securely deleted.

8.3 For full details of Street Medical Practice approach to data retention, including retention periods for specific personal data types held by Street Medical Practice, please refer to the Data Retention Policy.

9. Secure processing.

9.1 Street Medical Practice shall ensure that all patients' personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. *(Further details of the technical and organisational measures which shall be taken are provided in Parts 19 to 24 of this policy.)*

10. Accountability and record-keeping.

10.1 The person responsible for data protection at Street Medical Practice is **Dr Debbie Street** (referred to as 'the person responsible').

10.2 The person responsible shall be responsible for overseeing the implementation of this policy, for monitoring compliance with this policy, Street Medical Practice other data protection-related policies, and with the GDPR and other applicable data protection legislation as it applies to Street Medical Practice independent healthcare service.

10.3 Street Medical Practice shall keep written internal records of all patients' personal data collection, holding, and processing, which shall incorporate the following information:

- the name and details of Street Medical Practice, person responsible for data protection, and any applicable third-party data processors
- the purposes for which Street Medical Practice collects, holds, and processes patients' personal data
- details of the categories of patients' personal data collected, held, and processed by Street Medical Practice, and the categories of patient to which that personal data relates
- details of any transfers of patients' personal data to non-EEA countries including all mechanisms and security safeguards
- details of how long patients' personal data will be retained by Street Medical Practice *(please refer to Street Medical Practice Data Retention Policy),* and
- detailed descriptions of all technical and organisational measures taken by Street Medical Practice to ensure the security of patients' personal data.

11. Data protection impact assessments.

11.1 Street Medical Practice shall carry out a Data Protection Impact Assessment for any and all new projects and/or new uses of patients' personal data.

11.2 Data Protection Impact Assessments shall be overseen by the person responsible and shall address the following:

- the type of patients' personal data that will be collected, held, and processed relating to a new project
- the purpose for which patients' personal data is to be used
- how patients' personal data is to be used
- the parties (internal and/or external) who are to be consulted
- any risks posed to patients
- any risks posed both within and to Street Medical Practice as an independent healthcare organisation, and
- proposed measures to minimise and handle identified risks.

12. Keeping patients informed.

12.1 Street Medical Practice shall provide the information set out in Part 12.2 below to every patient.

12.2 Where patients' personal data is collected directly from patients, those patients will be informed of its purpose at the time of collection.

The following information shall be provided:

- details of Street Medical Practice as an independent healthcare organisation including, but not limited to, the identity of person responsible
- the purpose for which the patients' personal data is being collected and will be processed (as detailed in Part 18 of this Policy)
- where applicable, the legitimate interests upon which Street Medical Practice is justifying its collection and processing of the patients' personal data
- where the patients' personal data is to be transferred to one or more third parties, details of those parties and reasons for the transfer
- where the patients' personal data is to be transferred to a third party that is located outside of the European Economic Area (the *'EEA'*), details of that transfer, including but not limited to the safeguards in place (see Part 25 of this policy for further details)
- details of data retention
- details of the patient's rights under the GDPR
- details of the patient's right to withdraw their consent to Street Medical Practice processing of their personal data at any time
- details of the patient's right to complain to the Information Commissioner's Office (the '*supervisory authority*' under the GDPR)
- where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the patients' personal data and details of any consequences of failing to provide it, and
- details of any automated decision-making or profiling that will take place using the patients' personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

13. Patient access.

13.1 Patients may make subject access requests ('*SARs*') at any time to find out more about the personal data which Street Medical Practice holds about them, what it is doing with that personal data, and why.

13.2 Patients wishing to make a SAR should do using a Subject Access Request Form, sending the form to the person responsible.

13.3 Responses to SARs shall normally be made within 1 calendar month of receipt at Street Medical Practice, however this may be extended by up to 2 months if the SAR is complex and/or numerous requests are made. If such additional time is required, the patient shall be informed.

13.4 All SARs received shall be handled by the person responsible.

13.5 Street Medical Practice does not charge a fee for the handling of normal SARs. Street Medical Practice reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a patient, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

14. Rectification of personal data.

14.1 Patients have the right to require Street Medical Practice to rectify any of their personal data that is inaccurate or incomplete.

14.2 Street Medical Practice shall rectify the personal data in question, and inform the patient of that rectification, within 1 calendar month of the patient informing Street Medical Practice of the issue. The period can be extended by up to 2 months in the case of complex requests. If such additional time is required, the patient shall be informed.

14.3 In the event that any affected patients' personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

15. Erasure of personal data.

15.1 Patients have the right to request that Street Medical Practice erases the personal data it holds about them in the following circumstances:

- it is no longer necessary for Street Medical Practice to hold that personal data with respect to the purpose for which it was originally collected or processed
- the patient wishes to withdraw their consent to Street Medical Practice holding and processing their personal data
- the patient objects to Street Medical Practice holding and processing their personal data (and there is no overriding legitimate interest to allow Street Medical Practice to continue doing so) (see Part 17 of this Policy for further details concerning the right to object)
- the patient's personal data has been processed unlawfully, or
- the patient's personal data needs to be erased in order for Street Medical Practice to comply with a particular legal obligation.

15.2 Unless Street Medical Practice has reasonable grounds to refuse to erase patients' personal data, all requests for erasure shall be complied with, and the patient informed of the erasure, within 1 calendar month of receipt of the patient's request.

The period can be extended by up to 2 months in the case of complex requests. If such additional time is required, the patient shall be informed.

15.3 In the event that any patients' personal data that is to be erased in response to a patient's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

16. Restriction of patients' personal data processing.

16.1 Patients may request that Street Medical Practice ceases processing the personal data it holds about them. If a patient makes such a request, Street Medical Practice shall retain only the amount of personal data concerning that patient (if any) that is necessary to ensure that the personal data in question is not processed further.

16.2 In the event that any affected patients' personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

17. Objections to personal data processing.

17.1 Patients have the right to object to Street Medical Practice processing their personal data based on legitimate interests, such as direct marketing.

17.2 Where a patient objects to Street Medical Practice processing their personal data based on its legitimate interests, Street Medical Practice shall cease such processing immediately, unless it can be demonstrated that Street Medical Practice has legitimate grounds for such processing override the patient's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

17.3 Where a patient objects to Street Medical Practice processing their personal data for direct marketing purposes, Street Medical Practice shall cease such processing immediately.

18. Personal data collected, held, and processed.

18.1 The following patients' personal data is collected, held, and processed by Street Medical Practice (for details of data retention, please refer to Street Medical Practice Data Retention Policy):

Data	Type of Data	Purpose of Data
Patient name	Hand written on paper. Entered on computer.	To identify personal healthcare record.
Patient's postal address	Hand written on paper. Entered on computer.	To identify personal healthcare record.

Data	Type of Data	Purpose of Data
Patient's email address	Hand written on paper. Entered on computer.	To identify personal healthcare record.
Patient's date of birth	Hand written on paper. Entered on computer.	To identify personal healthcare record.
Patient's next of kin	Hand written on paper. Entered on computer.	To identify personal healthcare record.
Patient gender	Hand written on paper. Entered on computer.	To identify personal healthcare record.
Patient's height	Hand written on paper. Entered on computer.	For personal medical purposes. To assist in the diagnosis and treatment of personal medical conditions.
Patient's weight	Hand written on paper. Entered on computer.	For personal medical purposes. To assist in the diagnosis and treatment of personal medical conditions.
Patient's personal health information such as past medical history and current health problems.	Hand written on paper. Entered on computer.	For personal medical purposes. To assist in the diagnosis and treatment of personal medical conditions.
Patient's GP Name, address and contact details	Hand written on paper. Entered on computer.	To maintain continuity of health treatment and to share personal health information.

19. Data security - transferring personal data and communications.

19.1 Street Medical Practice shall ensure that the following measures are taken with respect to all communications and other transfers involving patients' personal data:

- all emails containing sensitive personal data (either in the body of the email or as an unencrypted attachment) should be encrypted

- all emails containing patients' personal data must be marked '*Confidential'*

- patients' personal data should be transmitted over secure networks only;

- patients' personal data should not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable

- patients' personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely; the email itself should be deleted; all temporary files associated therewith should also be deleted

- where patients' personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data

- where patients' personal data is to be transferred in hardcopy form it should be passed directly to the recipient, and

- all patients' personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked '*Confidential*'.

20. Data security – storage.

20.1 Street Medical Practice shall ensure that the following measures are taken with respect to the storage of patients' personal data:

- all electronic copies of patients' personal data should be stored securely using passwords

- all hardcopies of patients' personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar

- all patients' personal data stored electronically should be backed securely in encrypted format and the backup copy stored separately and remotely from the live information

- no patients' personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to Street Medical Practice or otherwise, and

- no patients' personal data should be transferred to any device personally belonging to a Street Medical Practice employee and patients' personal data may only be transferred to devices belonging to external contractors, or other parties working on behalf of Street Medical Practice where the party in question has agreed to comply fully with the letter and spirit of this policy and of the GDPR *(which may include demonstrating to Street Medical Practice that all suitable technical and organisational measures have been taken).*

21. Data security – disposal.

21.1 When any patients' personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. *(For further information on the deletion and disposal of personal data, please refer to Street Medical Practice Data Retention Policy.)*

22. Data security - use of personal data.

22.1 Street Medical Practice shall ensure that the following measures are taken with respect to the use of patients' personal data:

- no patients' personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of Street Medical Practice requires access to patients' personal data that they do not already have access to, such access should be formally requested from the person responsible

- no patients' personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of Street Medical Practice or not, without the authorisation of the person responsible

- patients' personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time

- if patients' personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it, and

- where patients' personal data held by Street Medical Practice is used for marketing purposes, it shall be the responsibility of the person responsible to ensure that the appropriate consent is obtained and that no patients have opted out.

23. Data security - IT security.

23.1 Street Medical Practice shall ensure that the following measures are taken with respect to IT and information security:

- all passwords used to protect patients' personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised

- all passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols

- under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of Street Medical Practice, irrespective of seniority or department. (If

a password is forgotten, it must be reset using the recommended method applicable to Street Medical Practice IT system.)

- all software (including, but not limited to, applications and operating systems) shall be kept up-to-date. Street Medical Practice shall be responsible for installing any and all security-related updates after the updates are made available by the publisher or manufacturer, unless there are valid technical reasons not to do so, and

- no software may be installed on any Street Medical Practice owned computer or device without the prior approval of the person responsible.

24. Organisational measures.

24.1 Street Medical Practice shall ensure that the following measures are taken with respect to the collection, holding, and processing of patients' personal data:

- all employees, agents, contractors, or other parties working on behalf of Street Medical Practice shall be made fully aware of both their individual responsibilities and Street Medical Practice responsibilities under the GDPR and under this policy, and shall be provided with access to this policy

- only employees, agents, sub-contractors, or other parties working on behalf of Street Medical Practice that need access to, and use of, patients' personal data in order to carry out their assigned duties correctly shall have access to personal data held by Street Medical Practice

- all employees, agents, contractors, or other parties working on behalf of Street Medical Practice handling patients' personal data will be appropriately trained to do so

- all employees, agents, contractors, or other parties working on behalf of Street Medical Practice handling patients' personal data will be appropriately supervised

- all employees, agents, contractors, or other parties working on behalf of Street Medical Practice handling patients' personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise

- methods of collecting, holding, and processing patients' personal data shall be regularly evaluated and reviewed

- all patients' personal data held by Street Medical Practice shall be reviewed periodically, as set out in Street Medical Practice Data Retention Policy

- the performance of those employees, agents, contractors, or other parties working on behalf of Street Medical Practice handling patients' personal data shall be regularly evaluated and reviewed

- all employees, agents, contractors, or other parties working on behalf of Street Medical Practice handling patients' personal data will be bound to do so in accordance with the principles of the GDPR and this policy by contract

- all agents, contractors, or other parties working on behalf of Street Medical Practice handling patients' personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of Street Medical Practice arising out of this policy and the GDPR, and

- where any agent, contractor or other party working on behalf of Street Medical Practice handling patients' personal data fails in their obligations under this Policy, that party shall indemnify and hold harmless Street Medical Practice against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

25. Transferring patients' personal data to a country outside the EEA.

25.1 Street Medical Practice may from time to time transfer ('*transfer'* includes making available remotely) patients' personal data to a third party in a country outside of the EEA.

(An example of such a transfer would be when a patient has been seen and treated in Street Medical Practice clinic by a medical practitioner and a written healthcare record produced and there is a need to share the information with another medical practitioner in another country.)

25.2 The transfer of patients' personal data to a country outside of the EEA shall take place only if one or more of the following applies:

- the transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for patients' personal data

- the transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority

- the transfer is made with the informed consent of the relevant person i.e. Street Medical Practice patient

- the transfer is necessary for the performance of a contract between the patient and Street Medical Practice (or for pre-contractual steps taken at the request of the patient)

- the transfer is necessary for important public interest reasons
- the transfer is necessary for the conduct of legal claims
- the transfer is necessary to protect the vital interests of the patient or other individuals where the patient is physically or legally unable to give their consent, or
- the transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

26. Data breach notification.

26.1 All patients' personal data breaches must be reported immediately to the person responsible.

26.2 If a patients' personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of patients *(e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage)*, the person responsible must ensure that the Information Commissioner's Office (ICO) is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

26.3 In the event that a patients' personal data breach is likely to result in a high risk *(that is, a higher risk than that described under Part 26.2 above)* to the rights and freedoms of patients, the person responsible must ensure that all affected patients are informed of the breach directly and without undue delay.

26.4 Patient data breach notifications shall include the following information:

- the categories and approximate number of patients concerned
- the categories and approximate number of patients' personal data records concerned
- the name and contact details of person responsible (or other contact point where more information can be obtained)
- the likely consequences of the breach, and
- details of the measures taken, or proposed to be taken, by Street Medical Practice to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

27. Policy review.

27.1 This policy will be reviewed on an annual basis.

27.2 Any changes made to the policy as a result of review, will be communicated to all Street Medical Practice staff without delay.

28. Guidance and further reading.

- General Data Protection Regulation (GDPR) guidance
  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

- Guide to the General Data Protection Regulation (GDPR)
  https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

- How healthcare organisations can prepare for the GDPR
  https://www.itgovernance.eu/blog/en/how-healthcare-organisations-can-prepare-for-the-gdpr

- The EU General Data Protection Regulation
  https://www.eugdpr.org/
