Wellington Medical Practice

THIRD PARTY
CONFIDENTIALITY AGREEMENT
Including Data Protection and Information Security

During the course of your association with the Practice, you may have access to, see or hear, confidential information concerning the medical or personal affairs of patients, staff or associated healthcare professionals. Unless acting on the instructions of an authorised officer within the Practice, on no account should such information be divulged or discussed with anyone. Breach of confidence, including the improper passing of confidential data could result in the Practice taking action against you.

Definitions

Data Protection Legislation means (i) the DPA 2018 (ii) the UKGDPR, the LED and any applicable national Laws implementing them as amended from time to time (iii) the DPA 2018 (iv) all applicable Law concerning privacy, confidentiality or the processing of personal data including but not limited to the Human Rights Act 2018, the Health and Social Care (Safety and Quality) Act 2015, the common law duty of confidentiality and the Privacy and Electronic Communications (EC Directive) Regulations

DPA 2018 means Data Protection Act 2018

UKUKGDPR means the General Data Protection Regulation (Regulation (UK) 2016/679)

Law means any law or subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the Supplier is bound to comply

LED means the Law Enforcement Directive (Directive (EU) 2016/680)

***Controller* –** shall take the meaning given in the Data Protection Legislation

***Criminal offence data* –** means Personal Data relating to criminal convictions and offences or related security measures

***Personal Data* –** shall take the meaning given in the Data Protection Legislation

***Processor* –** shall take the meaning given in the Data Protection Legislation

Processing and cognate terms shall have the meaning given in the Data Protection Legislation

Special Categories of Personal Data shall take the meaning given in the Data Protection Legislation;

Without limiting the generality of the above, for the purpose of this clause, "confidential information" means and includes any information relating to the Practice, its business and activity including but not limited to person and patient identifiable information and other sensitive information in whatever form but excluding any matter that has become public knowledge or part of the public domain and all other information provided to you which is either labelled or expressed to be confidential, or given to you in circumstances where one would expect the information to be confidential to the Practice.

The Supplier shall, in relation to any Personal Data processed in connection with its obligations under this Agreement process that Personal Data only in accordance with the instructions set out by the Practice, unless the Supplier is required to do otherwise by Law. If it is so required, the Supplier shall promptly notify the practice before processing the Personal Data unless prohibited by Law.

You should also be aware that regardless of any action taken by the Practice, a breach of confidence could result in a civil action against you for damages

By signing this Agreement you undertake:

- To treat as confidential any information that you may come into contact with during the course of your association with the Practice and thereafter
- To only access areas where confidential information is held if permissions are granted
- To respect the rights of patients who may not wish others (i.e. their friends/relatives) to know that they have visited the Practice

Any breaches of this Agreement will be reported to the Caldicott Guardian of the Practice for investigation

The Supplier shall, in relation to any Personal Data processed in connection with its obligations under this Agreement ensure that it takes all reasonable steps to ensure that Supplier Personnel are subject to appropriate confidentiality undertakings with the Supplier or any Sub-processor that are in writing and are legally enforceable

Extra defined terms used:

Supplier Personnel means any and all persons employed or engaged from time to time in the provision of the Services and/or the processing of Personal Data whether employees, workers, consultants or agents of the Supplier or any subcontractor or agent of the Supplier.

Security Measures

Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Supplier shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including, but not limited to, as appropriate:

1.1 the pseudonymisation and encryption of Personal Data;

1.2 the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

1.3 the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and

1.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing.

Engaging Sub-Processors

Before allowing any Sub-processor to process any Personal Data related to this Agreement, the Supplier must:

1.1 notify THE PRACTICE in writing of the intended Sub-processor and processing;

1.2 obtain the written consent of THE PRACTICE;

1.3 enter into a written agreement with the Sub-processor which gives effect to the terms set out in this Agreement such that they apply to the Sub-processor [and in respect of which THE PRACTICE is given the benefits of third-party rights to enforce the same]; and

1.4 provide THE PRACTICE with such information regarding the Sub-processor as THE PRACTICE may reasonably require.

The Supplier shall remain fully liable for all acts or omissions of any Sub-processor.

Extra-defined terms used:

Sub-processor means any third party appointed to process Personal Data on behalf of the Supplier related to this Agreement;

Subjects' Rights

The Supplier must assist the Practice by taking appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of THE PRACTICE's obligation to respond to requests for exercising rights granted to individuals by the Data Protection Legislation.

UKGDPR Compliance

The Supplier must assist the Practice in ensuring compliance with the obligations set out at Article 32 to 36 of the UKGDPR and equivalent provisions implemented into Law, taking into account the nature of processing and the information available to the Supplier.

Deletion or Return of Data

The Supplier shall, in relation to any Personal Data processed in connection with its obligations under this Agreement at the written direction of the Practice, delete or return the Personal Data (and any copies of it) to The Practice on termination of the Agreement unless the Supplier is required by Law to retain the Personal Data. If the Supplier is asked to delete the Personal Data the Supplier shall provide The Practice with evidence that the Personal Data has been securely deleted in accordance with the Data Protection Legislation within a period agreed within the written direction of The Practice.

Extra defined term

Working Day means a day other than a Saturday, Sunday or bank holiday in England

UKGDPR Record of Processing

The Supplier must create and maintain a record of all categories of data processing activities carried out under this Agreement, containing:

1.5 the categories of processing carried out under this Agreement;

1.6 where applicable, transfers of Personal Data to a third country or an international organisation, including the identification of that third country or international organisation and, where relevant, the documentation of suitable safeguards;

1.7 a general description of the Protective Measures taken to ensure the security and integrity of the Personal Data processed under this Agreement; and

1.8 a log recording the processing of Personal Data in connection with this Agreement comprising, as a minimum, details of the Personal Data concerned, how the Personal Data was processed, where the Personal Data was processed and the identity of any individual carrying out the processing.

The Supplier shall ensure that the record of processing maintained in accordance with clause is provided to the Practice within two Working Days of a written request.

Extra defined terms used

Protective Measures means appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data; ensuring confidentiality, integrity, availability and resilience of systems and services; ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident; and regularly assessing and evaluating the effectiveness of the such measures;

This contract does not relieve the Supplier from any obligations conferred upon them by the Data Protection Legislation

Data Protection Officer

The Supplier shall designate a Data Protection Officer if required by the Data Protection Legislation, and shall communicate to the Practice the name and contact details of any Data Protection Officer.

OR

The Supplier shall designate a Data Protection Officer and shall communicate to THE PRACTICE the name and contact details of the Data Protection Officer.

Extra defined term used

Data Protection Officer shall take the meaning given in the Data Protection Legislation;

I have read, understood and agree to comply with the Practice's Third Party Confidentiality Agreement