****

**Marsh Gardens, Honley, Holmfirth, HD9 6AG**

**CONFIDENTIALITY OF PATIENT DATA**

**Introduction**

This document sets out the arrangements in the practice for the confidentiality of patient data. The Practice complies with the Data Protection Act and General Data Protection Regulations (GDPR) 2018.

**The Practice’s Responsibilities**

The Practice will:

* Ensure that employees fully understand all their responsibilities with regard to confidential data, by ensuring employees undertake Information Governance training and sign a written statement of the responsibilities they are undertaking towards the security of all data within the surgery. Competency will be assessed as an annual process;
* Complete and submit the Data Security and Protection Toolkit self-assessment on an annual basis;
* Ensure that arrangements are in place for the confidential disposal of any paper waste generated at work. When any outside company is used the Practice will ensure that the company used are accredited to destroy sensitive papers (records of the registration of the company and a log of collections will be kept).

The Practice strictly applies the rules of confidentiality and will not release patient information to a third party (other than those involved in the direct care of a patient) without proper valid and informed consent, unless this is within the statutory exempted categories such as in the public interest, or if required by law, in which case the release of information and the reasons for it will be individually and specifically documented and authorised by the responsible clinician.

The Practice follows the Health and Social Care Information Centre document “A Guide to Confidentiality in Health and Social Care, Sept 2013”.

**Patient Information**

All patient information is considered to be confidential and we comply fully with the Data Protection Act and Caldicott Principles. All employees in the practice have access to this information in relation to their role, have confidentiality clauses in their contracts of employment and sign a confidentiality agreement annually. All staff members adhere to the Confidentiality: NHS Code of Practice 2003.

To ensure safe and effective patient care, patients’ information may be shared with other parties within the care team who are involved in their direct care. Where a patient wishes information not to be shared within the care team providing direct care, then they must discuss this with their GP and a note in the record made.

Patient information will not be shared outside of the direct care team without written consent being sought. An individual has the right to refuse to have their information disclosed, although this may have an impact on their care, their wishes will be complied with.

It is imperative that when it is right to release details to a third party that the information only includes what has been asked for and not necessarily the full record.

***There is currently one national data extraction from which patients may wish to “opt out” – this is known as The Summary Care Record (SCR):***

The SCR enables healthcare staff providing care for patients in an emergency from anywhere in England to be made aware of any current medications or allergies the patient may suffer from. This information from every patient record is sent electronically up to the NHS Spine in order for this to happen. If patients wish their information to be withheld from the SCR, they can “opt out”. Please ask at reception for the SCR Opt Out Form or download this from: <https://digital.nhs.uk/services/summary-care-records-scr/summary-care-records-scr-information-for-patients#opting-out>

**Telephone Recording**

It is practice policy to record telephone calls for the purposes of patient and staff care, security, and dispute resolution. Recordings and their use will comply with the Practice’s Data Protection registration.

**Protection against viruses**

Data is vulnerable to loss or corruption caused by viruses. Viruses may be introduced from removable storage media and by direct links via email and web browsing.

Precautions to be taken:

* Virus protection software is installed on ALL computer equipment;
* The supplier of our clinical software (The Health Informatics Service) manages the anti-virus software version control and ensures it is regularly updated;
* New programmes should not be downloaded without the permission of The Health Informatics Service – this reduces the risk of malware being downloaded and affecting the computer.