Version	Date Published	Review Status
2.4	Aug 2014	Updated May 2018

CONFIDENTIALITY – 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 GDPR regulations.

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 ongoing process and as part of the appraisal process.

The practice will complete and submit the Data Security and Protection Toolkit self-assessment on an annual basis.

The practice will also ensure that arrangements are in place for the confidential disposal of any paper waste generated at work.

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 the 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".

Key Principles

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 have signed a confidentiality agreement. All staff members adhere to the Confidentiality: NHS Code of Practice 2003.

To ensure safe and effective 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 team providing direct care, then they must discuss this with their GP.

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

It is imperative that when it is right to release details to 3rd parties 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" – the Summary Care Record:

The SCR enables healthcare staff providing care for patients in an emergency and 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 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 from:
systems.hscic.gov.uk/scr/library/optout.pdf

Protection against Viruses

Data is vulnerable to loss or corruption caused by viruses. Viruses may be introduced from data sticks, CD-ROM/DVD-ROM, other storage media and by direct links via e-mail and web browsing.

Precautions to be taken

- Virus protection software is installed on ALL computer equipment.
- The supplier of our clinical software manages the anti-virus software version control and ensures it is regularly updated.
- New programmes should not be downloaded without the permission of the IT or practice manager. This reduces the risk of malware being downloaded and affecting the computer.

Resources

Confidentiality: NHS Code of Practice
Cyber Security Policy {x}
Confidentiality Clause Staff Contracts {x}
Data Protection Policy {x}
Subject Access Request Policy {x}