CONFIDENTIALITY – PATIENT DATA

INTRODUCTION

This document sets out the arrangements in the practice for the confidentiality of patient data.

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 the data. Competency will be assessed as an ongoing process and as part of the appraisal process.

The practice will continue to complete and submit the IG 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 or the employees' home.

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.

In addition to the General Data Protection Regulation (GDPR) 2018, the 2004 Gender Recognition Act (GRA) makes it a criminal offence to disclose an individual's transgender history to a third party without their written consent if that individual holds a Gender Recognition Certificate (GRC). Patients do not need to show a GRC or birth certificate in order for the GRA 2004 to be in effect. Therefore, we act as though every trans patient has one. This means we always obtain a trans patient's written consent before sharing details about their social or medical transition, sometimes also called gender reassignment, with other services or individuals. This includes information such as whether a patient is currently taking hormones or whether they have had any genital surgery, as well as information about previous names or the gender they were given at birth. Consent should always be obtained before information relating to the patient being trans is shared in referrals and this information should only be shared where it is clinically relevant.

The practice follows the Health and Social Care Information Centre document "A Guide To Confidentiality in Health and Social Care, Sept 2013".

Leaflet Wording (Patient Information Leaflet or Poster)

All patient information is considered to be confidential and we comply fully with the Data Protection Act 1998 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.

Where appropriate, patient information may be shared with other parties within the care team involved in the direct care of patients, based on implied consent. This will be on a "need to know" basis only and in order to ensure the safe, effective care of patients. 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.

There are currently two national data extractions from which patients may wish to "opt out"

1. 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 they 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 one at: http://www.nhscarerecords.nhs.uk/optout/optout.pdf

2. Care.data programme

In order to improve health services, NHS England has commissioned a modern data service from the Health and Social Care Information Centre (HSCIC) known as the care.data programme. The aim of the service is to create a complete picture of care provided to patients by social care, GP practices and hospitals, and it will make use of patient information extracted from GP medical records.

Once this information has been linked to the data taken from hospitals, a new record will be created. This new record will not contain information that identifies you. The type of information that is then shared, and how it is shared, is controlled by law and strict confidentiality rules.

If you wish to "opt out" and prevent an extraction of information from your record being taken please ask for further information at reception.

At present, the proposed national roll-out of the care.data programme has been postponed and, rather than an immediate national roll-out, the HSCIC will be working with a number of "Pathfinder GP practices" that will test, evaluate and refine all aspects of the data collection process before it is applied nationally.

CCTV

CCTV is installed internally in public areas and externally for security. Recordings are used entirely at the discretion of the partners including provision of images to the police or other official bodies, and will otherwise comply with the Practice's Data Protection registration and the principles of patient confidentiality. Image data is held securely within the practice. The practice adheres to "Surveillance Camera Code of Practice, The Home Office, June 2013" and the Information Commissioner's "CCTV Code of Practice, 2008".

Please note that it is the Practice's policy to record all telephone calls for the purposes of patient and staff care, security, and dispute resolution. Recordings and their use will be at the Partners' discretion and will also 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 floppy discs, CDROM/DVDROM, 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 manage the anti virus software version control and regular updates.