PRACTICE POLICY – Confidentiality – Patient Data

Owner:	Marie Strachan
Date Created:	June 2018
Date Last Reviewed:	August 2019
Last Reviewed by:	Marie Strachan
Next Review Due:	August 2020
Location:	All Sites
Circulation:	All Staff
Keywords:	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 DSP 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".

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

CCTV

CCTV is installed internally in public areas and externally for security. The uses of recordings are identified in a Data Protection Impact Assessment (DPIA), including the provision of images to the police or other official bodies, and 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, 2015".

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 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, 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.