York Medical Group

Data Security & Protection Policy

Document Control

A. Confidentiality Notice

This document and the information contained therein is the property of York Medical Group.

This document contains information that is privileged, confidential or otherwise protected from disclosure. It must not be used by, or its contents reproduced or otherwise copied or disclosed without the prior consent in writing from York Medical Group.

B. Document Details

Classification:	
Author and Role:	
Organisation:	York Medical Group
Document Reference:	
Current Version Number:	
Current Document Approved By:	Dr David Geddes
Date Approved:	10/2/18

C. Document Revision and Approval History

Version	Date	Version Created By:	Version Approved By:	Comments
1.0	27/10/2015	iQ Medical	iQ Medical	Reviewed & Unchanged
1.1	7/12/18			Updated to include reference to GDPR
1.1	18/2/20			Reviewed and unchanged

Introduction

The Data Protection Act 1998 (DPA) requires a clear direction on Policy for security of information within the Practice.

The policy provides direction on security against unauthorised access, unlawful processing, and loss or destruction of personal information.

The following is a Statement of Policy which will apply:

The GDPR (General Data Protection Regulation).

- The GDPR and Data Protection Act 2018 replace the Data Protection Act 1998 with an updated and strengthened data protection framework, however, the key principles of the original Act remain unchanged. The most relevant changes for GPs in their role as data controllers are highlighted in the box below.
- The remainder of the guidance explains GP data controllers' responsibilities under the GDPR, and sets out the main themes of the legislation and what needs to be done to ensure compliance.
- The principles in the guidance apply to doctors working in private practice or other NHS healthcare settings.

The Policy

- The practice is committed to security of patient and staff records.

- The practice will display a poster in the waiting room, explaining the practice policy to patients.

- The practice will make available a brochure on Access to Medical Records and Data Protection for the information of patients.

- The practice will take steps to ensure that individual patient information is not deliberately or accidentally released or (by default) made available or accessible to a third party without the patient's consent, unless otherwise legally compliant.

- This will include training on confidentiality issues, DPA principles, working security procedures, and the application of best practice in the workplace.

- The practice will ensure that arrangements are in place for the confidential disposal of any paper waste

- The practice will undertake prudence in the use of, and testing of, arrangements for the backup and recovery of data in the event of an adverse event.

- The practice will maintain a system of "Significant Event Reporting" through a no-blame culture to capture and address incidents that threaten compliance.

- DPA issues will form part of the practice general procedures for the management of risk.

- Specific instructions will be documented within confidentiality and security instructions and will be promoted to all staff.

Key changes under GDPR

- Compliance must be actively demonstrated, for example it will be necessary to:
- keep and maintain up-to-date records of the data flows from the practice and the legal basis for these flows; and
- have data protection policies and procedures in place.
- More information is required in 'privacy notices' for patients.
- A legal requirement to report certain data breaches.
- Significantly increased financial penalties for breaches as well as non-compliance.
- Practices will not be able to charge patients for access to medical records (save in exceptional circumstances).
- Designation of Data Protection Officers

Key themes

- The guidance sets out the main themes of the legislation and what you need to do to ensure compliance, including:
- What is a data controller?
- Consent and other lawful bases for processing
- Right to object
- Data controller responsibilities for processing: privacy notices
- Accountability: demonstrating compliance
- Dealing with requests for confidential health data
- Breach reporting
- Subject access requests
- Breach reporting
- Additional concepts under GDPR

The practice Data Protection Officer is Dr David Geddes

More Guidance is available from the information at **ICO**

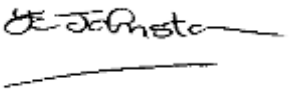
Protection against Viruses

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

Signed:



…… ……

Caldicott Guardian Operations Manager

Date: ……10/2/18…… Date: ……1/3/2018……..

Patient Poster

Data Protection Act – Patient Information

We need to hold personal information about you on our computer system and in paper records to help us to look after your health needs.

Please help to keep your record up to date by informing us of any changes to your circumstances.

Doctors and staff in the practice have access to your medical records to enable them to do their jobs. Your doctor is responsible for their accuracy and safe-keeping.

From time to time, it may be necessary to share information with others involved in your care. Anyone with access to your record is properly trained in confidentiality issues and is governed by both a legal and contractual duty to keep your details private.

All information about you is held securely and appropriate safeguards are in place to prevent accidental loss.

In some circumstances we may be required by law to release your details to statutory or other official bodies, for example if a court order is presented, or in the case of public health issues. In other circumstances you may be required to give written consent before information is released – such as for medical reports for insurance, solicitors etc.

To ensure your privacy, we will not disclose information over the telephone or fax unless we are sure that we are talking to you.

Information will not be disclosed to family, friends, or spouses unless we have prior written consent, and we do not leave messages with others.

You have a right to see your records if you wish. Please ask at reception if you would like further details and our patient information leaflet. An appointment will be required. In some circumstances a fee may be payable.

Post

- Ensure envelopes are marked “private and confidential”.
- Double check the full postal address of the recipient.
- Choose a secure method for sending confidential information through the external post e.g. recorded delivery.
- When necessary ask the recipient to confirm receipt.
- Ensure that incoming internal post is handled

Printer

- Avoid printing confidential/personal information to central printers.
- Keep the number of copies to a minimum.

Photocopying

- Do not make excessive copies of confidential information.
- Regularly check/update your distribution list to ensure copies are not sent to staff that have left or moved to another service.

Bin

- Be sure that you dispose of confidential information appropriately.
- All personal information is confidential and should be shredded.
- Confidential waste paper must not be used as scrap paper

Filing cabinet

- Ensure that filing cabinets containing confidential information are always kept locked when not in immediate use.
- Ensure filing cabinets are not sited in areas which are accessible to members of the public/visitors.
- Ensure regular housekeeping of your files.
- When destroying information ensure you comply with NHS retention guidelines.

Office

- Remember to lock and secure the office when it is unattended and at the end of the day.
- Whenever possible escort visitors at all times on site.
- Remember to wear your identity badge.

Desk

- Operate a clear desk policy, especially when hot desking or working in an open plan office.
- Do not leave confidential information unattended or our overnight – particularly important when hot desking or working in an open plan office.

Conversation

- Ensure you hold confidential conversations in an appropriate place. Inappropriate places include corridors, open plan offices and at the photocopier!
- Gain the patient’s consent before sharing their personal information with relatives.

Laptop

- Confidential information should not be taken off site.
- Laptops should be locked away in the building when not in use.
- Where it is necessary to take confidential information off site, remember;
  - Do not leave the laptop unattended
  - Remove confidential information as soon as possible
  - Password protect files containing confidential information
  - Ensure regular housekeeping of laptop files

Computer

- Be careful where you site your computer screen; ensure any confidential or personal information cannot be accidentally or deliberately seen by visitors or staff who do not have authorised access.
- Always keep your password confidential and do not write it down.
- Do not share passwords; this may be a disciplinary offence.
- Change your password regularly; most systems will force a regular change of password and designate the format of it.
- Remember to log off your computer when leaving the office, or use password protected screen savers for short absences.
- Any user who suspects they may have a computer virus must report it immediately to their IT helpdesk/Practice/System Manager.
- Any disk or CD coming into the organisation – no matter where it has come from – must be checked before use.

Database

- Ensure that any database that is created is in line with the organisation's Data Protection Notification details.
- Inform the Data Protection Officer when new databases are created or introduced to your department/service.

Telephone

- Be careful about leaving messages on answer phones.
- Be careful when taking messages off answer phones and ensure that messages cannot be overheard whilst being played back.
- When receiving calls requesting personal information:
  - Verify the identity of the caller
  - Ask for a reason for the request
  - If in doubt as to whether information should be disclosed tell the caller you will call them back. Take advice from your manager.
  - Call back to main switch board or known and trusted numbers only – not direct lines you do not recognise or mobile telephones.

Faxing

- Do not fax personal or confidential information unless it is absolutely necessary.
- If it is necessary, ensure that you fax the information to a Safe Haven/secure fax.
- If faxing personal or confidential information:
  - Double check the fax number
  - Ask recipient to confirm receipt of the fax
  - Ensure you mark the fax header "private and confidential"
  - Personal details (e.g. name & address) should be faxed separately from clinical details, which must be accompanied by the NHS number.

Email

- Patient identifiable information should not be sent via email unless the message is encrypted.