Data Protection and Information Governance Policy

Document Control	
Document Name	Data Protection and Governance Policy
Publication Date	April 2019
Version Number	1.1 POL10
Target Audience	Practice Staff
Description	Procedure indicating the importance of data protection and governance
Action Required	
Author	Michelle Davenport
Last Reviewed:	14/05/24
Next Review Date	December 2024

Table of Contents

Information Governance

Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in clinical governance, service planning and performance management.

It is therefore of paramount importance to ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability and structures provide a robust governance for information management

The Practice recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The Practice fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff and commercially sensitive information. The Practice also recognises the need to share patient information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and, in some circumstances, the public interest.

The Practice believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of all clinicians and managers to ensure and promote the quality of information and to actively use information in the decision making process.

There are four key interlinked strands to the information governance policy:

- Openness
- Legal Compliance
- Information Security
- Quality Assurance

Openness

Non-confidential information on the Practice and its services should be available to the public through a variety of media, in line with the Practices code of openness and Duty of Candour Policy.

The Practice has established and will maintain policies on an annual basis to ensure compliance with the Freedom of Information Act.

The Practice will undertake annual assessments and audits of its policies and arrangements for openness.

Patients should have ready access to information relating to their own health care, their options for treatment and their rights as patients.

The Practice will have clear procedures and arrangements for liaisons with the press and broadcasting media.

The Practice will have clear procedures and arrangements for handling queries from patients and the public.

Legal Compliance

Purpose and Scope

The purpose of this policy is to describe how the processing of personal data is undertaken at Heaton Mersey Medical Practice. It describes our approach to meeting obligations in respect of the processing of personal data, and ensuring that in carrying out our work we can comply with the Data Protection Act 2018 and the General Data Protection Regulation (GDPR) 2016.

This policy shall apply to Partners and Employees of the Practice and any other person or organisation required to process personal data on our behalf.

Policy Statement

Heaton Mersey Medical Practice is registered as a Data Controller with the Information Commissioners Office (ICO) under the Data Protection Act 2018 and The GDPR 2016 (The Acts). The Act imposes conditions relating to the collection, usage and handling of personal information.

The scope of activities which forms the basis for our registration as a Data Controller is defined as Doctor (GP).

During the course of our activities, staff will gather, store and process personal information and must recognize the need to treat it in an appropriate and lawful manner.

The types of information that we may be required to handle include details of current, past and prospective partners, employees, suppliers, business associates, patients and others with whom we communicate. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Act and other regulations. The Act imposes restrictions on how we may use that information.

This policy sets out our rules on data protection and our approach to meeting the legal conditions that must be satisfied in relation to obtaining, handling, processing, storage, transportation and destruction of personal information.

Legislation places specific responsibilities on us, as a Data Controller, and our staff, recognising that an act of non-compliance may lead to legal prosecution. It may also damage our reputation. Data Protection is a matter of good business and social responsibility. To ensure that an appropriate level of data protection is maintained, this policy must be observed in relation to the collection, holding, use and disclosure of personal information.

Regular monitoring and reviewing of the effectiveness of this policy will take place to ensure that it continues to achieve its stated objectives.

Any breach or suspected breach will be investigated and may lead to disciplinary action where that breach arises as a result of the action of a staff member. In some cases a breach of the terms of this policy may be treated as gross misconduct, leading to the summary dismissal of any employee who is found responsible.

Definitions of data protection and GDPR Terms

"Data" is information that is stored electronically, on a computer, or in certain paper-based filing systems.

"Data subjects", for the purpose of this policy, include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

"Personal data" means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).

"Data controllers" are the people who (or organisations that) determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. We registered with the UK Information Commissioner's Office (ICO) as a data controller for all personal data that we use.

"Data users" include staff whose work involves using personal data. Data users have a duty to protect the information they handle by complying with this data protection policy and its protocols at all times.

"Data processors" include any person who processes personal data on behalf of a data controller. The staff of data controllers are excluded from this definition, but it could include suppliers that handle personal data on our behalf.

"Processing" is any activity that involves the use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data, including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

"Sensitive personal data" includes information about a person's physical or mental-health condition, racial or ethnic origins, political opinions, religious or similar beliefs, trade union membership, or sexual life. It also includes data about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings, or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, and will usually require the express consent of the person concerned.

Protocols for data protection compliance

The Practice Manager is the assigned role within Heaton Mersey Medical Practice with functional responsibility for co-ordination and maintaining our data-protection registration process and who will advise on any issues in relation to compliance with this policy.

The GP Partners and the Practice Manager are responsible for ensuring that employees and suppliers/service providers understand and carry out their responsibilities und the Acts and the relevant policies.

The Practice Manager is responsible for informing all staff of any new processing activity, or amendments to existing processing activities, or personal data.

Hard-copy and electronic media containing personal information must be securely stored to protect them from unauthorised use, or from activity that threatens the availability, confidentiality and/or integrity of personal data.

Personal data must not be disclosed to unauthorised persons other than in accordance with this policy.

Correspondence received from members of the public and/or employees requesting information under the Data Protection Act and GDPR, or making any reference to the Acts in regard to our work, must immediately be forwarded to the Practice Manager.

Every staff member must understand their responsibilities for data protection.

Data Protection Principles

The organisation is committed fully to compliance with the requirements of the Data Protection Act 2018. The 2018 Act applies to all organisations that process data to their employees, as well as to others e.g. customers and clients. It sets out principles which should be followed by those who process data; it gives rights to those whose data is being processed.

To this end, the organisation endorses fully and adheres to the eight principles of data protection, as set out in the DPA.

Any person processing personal data must comply with the eight enforceable principles of good practice and observe any instructions issued to the processing of personal data. The principles provide that personal data must:

- Data must be processed fairly and lawfully.
- Data must only be obtained for specified and lawful purposes.
- Data must be adequate, relevant and not excessive.
- Data must be accurate and up to date.
- Data must not be kept for longer than necessary.
- Data must be processed in accordance with the "data subject's" (the individual's) rights.
- Data must be securely kept.
- Data must not be transferred to any other country without adequate protection in place.

Fair and Lawful Processing

The Data Protection Act in not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller's representative is, the purpose for which the data is to be processed by us, and the identities of anyone to whom the data may be disclosed or transferred.

For personal data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, more than one condition must be met. In most cases the data subject's explicit consent to the processing of such data is required.

Limited Purpose and Appropriateness

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Act. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.

Adequate, relevant and non-excessive processing

Personal data should only be collected to the extent that it is required for the specific purposes specifically permitted by the Act. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.

Accurate Data

Personal data must be accurate and kept up to date. Information that is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of personal data at the point of collection and at regular intervals thereafter. Inaccurate or out-of-date data should be destroyed.

Timely Processing

Personal data should not be kept longer than is necessary for the purpose. This means that data should destroyed or erased from our systems when it is no longer required. Guidance on how long certain data is to be kept before being destroyed will be given the Records Retention Schedule.

Data must be processed in line with the data subjects' rights. Data subjects have a right to:

- Request access to any data held about them by a data controller;
- Prevent the processing of their data for direct-marketing purposes;
- Ask to have inaccurate data amended; or
- Prevent processing that is likely to cause damage or distress to themselves or anyone else.

Information Security

We must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss. Also, our reputation relies on managing data protection effectively to avoid potential adverse publicity and reputation damage from any failure.

The Acts require us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction Personal data may only be transferred to a third party's data processer if they give explicit agreement to comply with those procedures and policies, or if they put in place adequate measures themselves.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

- Confidentiality means that people who are authorised to use the data can access it
- Integrity means that personal data should be accurate and suitable for the purpose for which it is processed
- Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should not normally, therefore, be stored solely on our individual PCs.

Security protocols include:

- Entry controls: Entry and movement around the premises must be strictly controlled through appropriate authorised persons seen in entry-controlled areas should be reported.
- Secure, lockable desks and cupboards: desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
- Methods of disposal: paper documents should be shredded or securely disposed of through approved means. Digital/optical media should be physically destroyed when they are no longer required.
- Equipment: data users should ensure that individual monitors do not show confidential information to passers-by and that they lock screens when not in use.

Security of Paper Records

All members of staff are responsible for any records which they create or use in the performance of their duties. Furthermore, any record that an individual creates is a public record.

The key statutory requirement for compliance with records management principles is the Data Protection Act 2018. It provides a broad framework of general standards that have to be met and considered in conjunction with other legal obligations. The Act regulates the processing of personal data, held both manually and on computer.

It applies to personal information generally, not just to health records, therefore the same principles apply to records of employees held by employers, for example in finance, personnel and occupational health departments.

Personal data is defined as data relating to a living individual that enables him/her to be identified either from that data alone or from that data in conjunction with other information in the data controller's possession. It therefore includes such items of information as an individual's name, address, age, race, religion, gender and physical, mental or sexual health.

Processing includes everything done with that information, ie holding, obtaining, recording, using, disclosing and sharing it. Using includes disposal, ie closure of the record, transfer to an archive or destruction of the record.

Additionally, clinicians are under a duty to meet records management standards set by their professional regulatory bodies.

When a new patient registers, their records should be obtained from their last GP by the Practice Administrator. In the meantime, an electronic record should be started, ideally before the patient is seen for the first time. In the event of emergency requests for newly registered patients, efforts should be made to obtain basic details, faxed if possible, from their previous GP. Paper records obtained should be summarised according to Summarising Policy as soon as is practical, ideally within 8 weeks.

Records should be stored in such a way that the record can be easily retrieved at any time, that any outstanding issues can be dealt with, and that there is an auditable trail of record transactions. Most recent volumes of patient records should be stored in reception and supplementary volumes upstairs in the archive room. Volumes should be marked Vol I, Vol II, Vol III etc. Earlier volumes should be secured together.

Storage accommodation for current records should be clean and tidy, should prevent damage to the records and should provide a safe working environment for staff.

Equipment used to store current records on all types of media should provide storage that is safe and secure from unauthorised access and which meets health and safety and fire regulations, but which also allow maximum accessibility of the information commensurate with its frequency of use.

The last key holder to leave the premises is responsible for making sure the building is left secure at the end of the day and the alarm set. All members of staff should be aware of their personal responsibilities regarding confidentiality, outlined in their contracts and in practice policies.

Security of Electronic Records

Smartcards

Where access to the clinical or other systems is to be controlled via the issue of a Smart Card the following will apply:

- Smart cards are issued to an individual on a named basis and are for the use of that person only. Problems with Smart Cards should be dealt with by Jackie McDowell
- The access level relating to an individual is personal and must not be shared or otherwise made accessible to another member of staff
- The Smart Card is to be kept under the personal control of the individual to whom it has been issued at all times and **must not be left inserted into a smart card reader when the individual is not present**
- On leaving a terminal the Smart Card is to be removed ***on every occasion***
- Staff members must take their Smart Card with them when they leave work, and store it securely.
- Staff members sharing Smart Cards will be considered for disciplinary action in accordance with the Practice's normal procedures. This would normally be after an informal warning
- Staff members must report the loss of a card to The Practice Manager or Jackie McDowell as soon as it is known that the card is missing
- Smart Cards will not normally be handed over between individuals. In the event of a staff member needing to relinquish a card (e.g. over a holiday period) then this will be passed back to The Practice Manager or Jackie McDowell or nominated person who will log the transfer and retain the card securely

PC Access

All staff with authorised access to clinical systems **must have their own** Windows password, EMIS login and Docman login. Where possible, staff are to use their Smart Cards when logged in to EMIS, otherwise barcodes will not be printed on prescriptions.

Passwords for accessing clinical systems must be changed regularly or at the prompt. They should not be stored in any way that may make them accessible to unauthorised users.

Staff **must log out of EMIS and Windows** when changing over or finishing at the end of their shift.

Locum doctors will be issued their own EMIS password by Jackie McDowell or designated member of staff.

Storage and Backup

Storage and Backup of the Electronic Record (EMIS Web) is the primary responsibility of the CCG. Daily backups of Docman are automatic. Any identified backup failure should be reported to the IG Lead and/or CCG. Updates of Docman will be managed by the IG Lead or remotely by the CCG.

Maintenance and backup of servers is the responsibility of the CCG. The following precautions should be taken in relation to Heaton Mersey Medical Practice:

- Servers should not be used as regular workstations for any application
- Use a shared drive on a networked server for all data wherever possible

Recent review of existing backup arrangements using USB now requires any containing confidential business information, such as accounts, to be stored in a locked filing cabinet. Information stored on shared drive (W:) is backed up according to CCG policies, and this is sufficient for day to day backups of all such data.

No patient data will be stored on a PC or other equipment in non-secure areas.

Jackie McDowell will be responsible for any business information which is being stored on removable media.

In the event that data restoration is required, contact the IT support desk on 0161 765 6688 for guidance before proceeding further.

Bulk Data Extractions

No bulk extracts or manipulation of data or coding is permitted other than with the prior permission of Dr G Dent.

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.

Overall responsibility for virus protection rests with the CCG. The following precautions will be taken:

- Staff must not download any attachments from unknown senders etc.
- Ensure that preview panes in email software are not open when sending/receiving mail
- Physical restrictions e.g. drive locks / disable drives will be used where appropriate

- All staff will be made aware of data security issues in all IT related protocols and procedures
- Data security will be mentioned in the organisation's disciplinary policy
- Use of removable drives such as USB memory sticks should not be necessary and is subject to prior authorisation from the Practice Manager.

Installation of Software

Software purchases will be authorised IT Helpdesk who will supervise the loading of the software onto the system or individual PCs in accordance with the software licence.

Staff are prohibited from installing or upgrading personal or purchased software.

Staff are prohibited from downloading software, upgrades, or add-ins from the internet.

Staff are permitted to receive and open files received in the normal course of business providing they have been received and virus scanned through the standard virus software installed by the clinical system supplier.

Hardware

Staff and contractors are not permitted to introduce or otherwise use any hardware or removable storage devices into the Practice other than that which has been provided, or pre-approved, by the Practice.

The Practice Manager is responsible for ensuring that the Practice has adequate supplies of removable storage media of a type approved for use in the Practice. The use of removable storage media is by authorised staff only.

Removable storage media (including CDs and other similar temporary items) which are no longer required must be stored securely or destroyed in a confidential way. Any queries should be discussed with the Practice Manager.

Protection against physical hazards

Common sense applies!

- Check that the PC or server are not at risk of pipes and radiators which, if damaged, could allow water onto the equipment
- Do not place PCs near to taps/sinks
- Do not place PCs close to windows subject to condensation and water collection on windowsills
- Ensure that the PC is not kept in a damp or steamy environment

- Computers generate quite a bit of heat and should be used in a well-ventilated environment. Overheating can cause malfunction, as well as creating a fire hazard
- Try to place the PC away from direct sunlight and as far as possible from radiators or other sources of heat

Normal health and safety protection of the building against fire, such as smoke alarms and CO_2 fire extinguishers should be sufficient for computers. If backup tapes are kept on the premises they must be protected against fire in a fireproof safe

- Report any defective wiring
- Ensure that ventilators on computers are kept clear
- Do not stack paper on or near computers
- Ensure that the environment is generally clean and free from dust.

In the event of the premises becoming unusable, the practice will liaise with IT Helpdesk regarding alternative access and equipment subject to the Business Continuity Plan.

Physical security

- Burglar alarm should be set whenever the building is left unoccupied.
- Locks on all windows and window grills in vulnerable areas have been installed. Windows must not be left open when the building is unoccupied.

- Appropriate locks have been installed on external and internal doors and should be used if a room is left unattended for a significant period of time if there is the potential for access by a member of the public.
- All separate rooms should be locked when the building is unoccupied
- Ensure any keys stored on site are not in an obvious place and any instructions regarding key locations or keypad codes are not easily accessible
- Unauthorised access during opening hours should be reported to one of the Partners.
- Ensure that there is appropriate insurance cover - where applicable – in place.
- Do not store patient identifiable information on PC equipment which is not contained in a secure area
- Maintain a separate record of hardware and software specifications of every PC in the building (CCG owned assets are recorded at the CCG).

Where the building is not fully occupied e.g. during out of hours clinics, only the required rooms and corridors should be accessible to the public e.g. admin areas and consulting rooms not in use to be kept locked. Responsibility for locking the doors and securing the building when unoccupied rests with the last key holder to leave.

Specific precautions relating to IT hardware are:

- Locate PCs as far away from windows as possible
- Clearly 'security mark' all PCs and all parts of PCs i.e. screen, monitor, keypad.
- Have an asset register for all computer equipment, which includes serial numbers (Held by CCG).
- Ensure every PC is password protected

Information Security Incident Reporting Procedure

Introduction

Information security is everyone's responsibility; this policy has been developed to ensure employees identify information security incidents, suspected information security weaknesses or near misses or security threats to services or systems and report these incidents through appropriate management channels for investigation and follow up.

An Information Security Incident

An information security incident is any violation of an Information Governance (IG) /Information Security Policy. The term information security incident and suspected incidents is very broad and includes, but is not limited to, incidents that relate to the loss, disclosure, denial of access to, destruction or modification of the Practice's information, or information systems.

An information security incident can be defined as any event that has resulted or could result in:

- The disclosure of confidential information to an unauthorised individual
- The integrity of a system or data being put at risk
- The availability of the system or information being put at risk

An adverse impact can be defined for example as:

- Threat to personal safety or privacy
- Legal obligation or penalty
- Financial loss
- Disruption of Practice business
- An embarrassment to the Practice

Examples of security incidents:

- Using another user's login /smart card
- Unauthorised disclosure of information

- Leaving confidential / sensitive files out
- Theft or loss of IT equipment
- Theft or loss of computer media, i.e. floppy disc or memory stick
- Accessing a person's record inappropriately e.g. viewing your own health record or family members, neighbours, friends etc.,
- Writing passwords down and not locking them away
- Identifying that a fax has been sent to the wrong recipient
- Sending/receiving a sensitive email to/from "all staff" by mistake
- Giving out or overhearing personally identifiable information over the telephone
- Positioning of pc screens where information could be viewed by the public
- Software malfunction
- Inadequate disposal of confidential material

Diligent employees should question procedures, protocols and events that they consider could cause damage, harm, distress, break of compliance or bring the practice's name into disrepute.

Reporting of Security Incidents

All information security incidents should be reported to The Practice Manager who will ascertain the level of risk and ensure any immediate action is taken appropriate to the level of risk. All incidents will need to be formally recorded on an incident report form. The responsible officer in the Practice will investigate, document and if necessary, provide feedback on the outcome of the incident.

All significant incidents relating to information security should be reported to the CCG's Information Governance Lead and Caldicott Guardian, particularly in instances where these involve bulk data loss or confidentiality breaches.

A log will be kept of all incidents reported, irrespective of whether they lead to a complaint or not. All incidents should be considered as to whether they indicate a need for improvement in arrangements. The log may be incorporated into other incidents logs as appropriate. A regular report on the number, type and location of information security incidents should be made, allowing any trends to be picked up and addressed.

By reporting such incidents or near misses it allows the Practice to relate to similar occurrences and highlights any areas of vulnerability, identifying where greater awareness is needed, or procedures/ protocols that require reviewing. Good reporting generates better statistical data thus, keeping the Practice informed.

When reporting an information security incident, it is important to ensure sufficient information is given to the IG lead to enable them to understand and respond appropriately to the report. Users can report security related incidents in confidence;

no information about a user's involvement in a security incident will be released without explicit permission.

If reporting software malfunctions, symptoms of the problem and any messages appearing on the screen should be noted. The PC should be isolated and the use of it stopped, until reported. Users must not attempt to remove suspected software or attempt to 'repair/mend' equipment unless authorised to do so.

Description of Incident

It is important that the information security incident reports give as much detail as possible. Including a description of activities leading up to the security incident, information about circumstances prevailing at the time, how the incident came about, how the incident was detected.

The information security incident or suspected incident report should include full details of the incident in as much details as possible to enable a full investigation to be carried out if necessary. However, when logging incidents, personal details should, wherever possible, be omitted.

Whenever possible when reporting information security incidents, any protocols or procedures which may have been compromised should be referenced on the report.

All information security incidents will be prioritised in accordance with the severity of the incident by the person logging these on the risk or incident reporting system.

Heaton Mersey Medical Practice requires that information security incidents be reported as soon as possible after they occur or have been identified. Reports sent immediately after the incident are likely to be the most valuable; if there is a delay between an incident occurring and the discovery of said incident, the incident should still be reported.

Follow Up

Incidents should be used in training sessions about security and confidentiality as using 'real life events' relevant to a Practice can always be related to by staff, a lot better than in imaginary events. This will give the attendees an example of what could occur, how to respond to such event and how to avoid them in the future.

Handling and Disclosure of Personal and Sensitive Information

The nature of General Practice requires all staff and those associated with it to handle confidential information in a secure manner. Transfer must be controlled and compliant with any relevant legislation, e.g. the Data Protection Act 1998 (DPA2018 by May 2018), Confidentiality: NHS Code of Practice, Caldicott Principles and newly introduced GDPR (General Data Protection Regulation 2016).

On a daily basis, confidential information moves around the Practice and between organisations in paper, electronic and other media e.g. telephone, memory sticks, images.

Each mode of data handling will be risk assessed to ensure that appropriate measures have been incorporated into how that particular activity must be carried out. Safe haven procedures must be complied with to ensure appropriate protection of confidential/personal information

Procedures and standards to protect information and media have been established to reflect 'best practice'. Failure to comply with instructions given within this document may result in disciplinary action being taken against any individuals

This document has been approved by the Practice's IG Lead and Caldicott Guardian and will be subject to review and monitored for compliance

Telephone

Wherever possible, ensure that the call is being taken out of earshot of patients/visitors. Where a glass panel screens the reception area, keep it closed when talking on the telephone.

Receiving Telephone Calls

When receiving incoming calls where you need to confirm something personal or book an appointment that requires the caller to establish their identity you need to ask

- Who is calling
- Confirmation of their address/other personal identifiers (date of birth, telephone number)
- The nature of their call

Under no circumstances repeat what they have said back to them if you are not in a secure location.

If the caller is asking for specific personal information, be absolutely sure that they are entitled to receive it. If in doubt, you should take advice from your Line Manager

Making Telephone Calls

Always make telephone calls that involve personal information in an area that is secure and away from people who should not overhear your conversation

- Verify the identity of the person you wish to speak to
- Keep the level of detail to a minimum – the individual will usually know the reason for the communication
- Never take direct dial number if you need to call the individual back at work – always go through the main switchboard
- Do not leave any messages on answer phones that contain personal information – you should only leave a message asking the person to call you back leaving a telephone number, not the name of the surgery

Telephone Answering Machines

Be careful when taking messages off answering machines. Always ensure that audio messages cannot be overheard by other people whilst playing them back

Record information obtained from this type of media by following the Written Messages Protocol contained within this document.

Electronic Transfers of Patient Data

There is a statutory and contractual obligation on Practices under the GMS contract to have in place a written procedure for the transfer electronically of patient data. The purpose of this protocol is to define circumstances in which this takes place within the practice and the administrative and security procedures which will apply.

For the purposes of this, electronic transmission is defined as:

- Email
- Fax
- Pathology Test Results
- Out of Hours Transmissions (OOH)
- Electronic Prescription Requesting (EPMS)

The overriding standard applicable to each of these is the General Data Protection Regulation 2016 and Act 1998 as summarised on the DoH website.

Email

Sending/receiving information by email does not offer 100% security, therefore Practice email accounts should only be used for business purposes in order to reduce the possibility of virus attacks, data hacking, etc.

Email attachments are one of the most common methods for transmitting viruses. Whilst the Practice has anti-virus software installed on its computers, users should not open attachments received if they were not expecting them

Staff must not send any patient identifiable or other sensitive information by email

If person identifiable information needs to be sent by email, please contact the Practice Manager

- Patient identifiable information will not generally be sent by e mail.
- It is acceptable for patient identifiable information to be sent by e mail providing it is wholly within the NHS NET system.
- Where, in the interests of expedience, an e mail with or without attachments must be used to provide information, texts, images or other identifiable sections must be removed prior to dispatch. In these circumstances the recipient will be contacted by telephone to advise them that the e mail will be sent and they will be informed verbally of the identity of the patient along with any relevant personal detail. The de-personalised items may then be e mailed.
- Care will be taken to ensure that minor errors in the e mail address used do not result in an inappropriately or incorrectly addressed e mail.

If person identifiable information needs to be sent by email, please contact the Practice Manager

Wi-Fi

The SSID provides Internet only access for 3rd parties and members of the public by means of web authentication portal.

Wifi Handover
Document_2.docx

Pathology/Test Results

- Most results are transmitted to the practice via the clinical system pathology link.
- The following results will NOT be received electronically – MRI Scans.
- GP Partners *will* be responsible for viewing the results daily. In his/ her absence the results will be divided between the doctors that are in that day and they will view the results. The reviewing clinician will identify any patient related action required.
- Nominated administrative staff will be responsible for the re-allocation of results to alternative GPs in the event of named GP absences.
- The nominated administrative staff will check for any unmatched patients or unmatched doctors daily. If the result cannot be matched manually, they will print off the result and return it to the pathology department advising that the practice is unable to trace the patient.
- The pathology department will be contacted regarding any missing results or interchanges.

- All administrative staff will check that the Admin results action queue created by the GPs is actioned daily and that all appropriate actions have been taken. Results will not be removed from this queue until all actions are complete.
- All patient related reports will be dealt with on the day of receipt.
- Individual clinicians will append comments to the results and file as a consultation into the clinical patient record.
- The clinicians will notify reception by means of the "Electronic Practice Notes" system of any additional action required.
- Receptionists/administrative staff will check the "Electronic Practice Notes" at regular intervals throughout the day and prior to leaving, to ensure that action has been taken.

Out of Hours Transmissions (OOH)

- Information relating to OOH consultations are transmitted directly into the clinical system each morning.
- Medical secretaries are responsible for viewing the transmissions prior to 11:00 hours. In the event of absence, the nominated person will arrange for the role to be deputised.
- The transmissions will be passed to the appropriate GP for viewing prior to 12:00 hours.
- The GP will action the information and arrange any follow up action.
- The nominated person will create a consultation record and file the electronic transmission within the patient record on the clinical system. Where the details suggest a particularly urgent situation the GP may be interrupted in surgery to view the details.

Electronic Prescription Requesting (EPMS)

The Electronic Prescription Management Service provides electronic requesting transmissions directly into the clinical system, electronic authorisation of prescription requests and re-transmission of the authorised prescription back to the pharmacy for issue.

- The patient must complete a consent and application form prior to registration to the system.
- The patient will have the choice to opt in and out of the system and will be able to select either of the methods (electronic or normal/manual) at any time.
- The administration and clinical staff accessing the system will ensure at each authorisation that there is no duplication, or potential duplication, of prescriptions being obtained either electronically or concurrently, manually.
- The nominated administrative staff are responsible for accessing the inbox twice daily to view new electronic prescription requests.

- The nominated persons are responsible for initial review of the request, investigation of pharmacy queries relating to that prescription and either accepting or rejecting the request back to the pharmacy.
- The nominated persons will be responsible for the manual matching of patients to GPs where necessary.
- The nominated persons are responsible for the initiation of any requests received direct from patients attending the surgery for a prescription to be processed and delivered electronically.
- The nominated persons are responsible for the monitoring of each prescription request received electronically until each has been authorised back to the pharmacy by the patient's "Usual GP" or the GP responsible for the authorisation.
- All repeat prescription requests received electronically will be accepted and authorised, or rejected, within 24 working hours of receipt within the clinical system.

All other Transfers of Patient Data Electronically

Will be managed in accordance with the Latest NHS digital Guidance -. i.e., GP2GP guidance and GDPR NHSD Best practice.

Disaster Recovery

- The Practice data is backed up daily, automatically and stored on the cloud.
- Backups are verified regularly by the software and system supplier
- Firewalls and virus checkers are kept up to date and running, and users are trained in virus avoidance and detection.
- Computers are protected from physical harm, theft or damage, and from electrical surges using protective plugs.
- The Practice plans for how to deal with loss of electricity, external data links, server failure, and network problems.

Quality Assurance

The Practice has established and will maintain policies and procedures for information quality assurance and the effective management of records

The Practice undertakes annual assessments and audits of it information quality and records management arrangements

Staff are expected to take ownership of, and seek to improve, the quality of information within their services. Wherever possible, information quality should be assured at the point of collection.

The practice will promote information quality and effective records management through policies, procedures/user manuals and training:

Lead Staff

Lead Staff for Information Governance

The Practice has assigned responsibility roles to the following people:

Senior Information Risk Officer (SIRO) – Dr. Graeme Dent

Caldicott Guardian and Data Protection Officer – Dr Graeme Dent and the Practice Manager

Role and Responsibility of SIRO

The SIRO role is primarily around information governance compliance and risk.

The SIROs role is to ensure information assets and risks within the Practice are managed as a business process rather than as a technical issue.

The SIRO is responsible for ensure the staff recognises the importance of information assets in delivering Practice objectives. Where appropriate, the SIRO should seek input from others (internally and externally) to further highlight the contemporary information risks and threats which may prevent Practice objectives from being achieved.

The SIRO, as a champion of governance, must ensure there are consistent and repeatable approached to managing risk at all levels of the Practice.

Role of the Caldicott Guardian

A Caldicott Guardian is a senior person within a health or social care organisation that makes sure that the personal information about those who use its services is used legally, ethically and appropriately, and that confidentiality is maintained.

Caldicott Guardians should be able to provide leadership and informed guidance on complex matters involving confidentiality and information sharing.

The Caldicott Guardian should play a key role in ensuring the Practice satisfies the highest practical standards for handling personal information. Their main concern is information relating to patients, service users and their care, but the need for confidentiality extends to other individuals, including their relatives, staff and others.

Role and Responsibility of the Data Protection Officer

To inform and advise the Practice and its employees about their obligations to comply with the GDPR and other data protection laws

To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits

To be the first point of contact for staff and for patients whose data is processed.

Designated Data Controllers

The designated Data Controllers, Dr G Dent and the the Practice Manager will deal with day-to-day matters. Any member of staff, or other individual who considers that the policy had not been followed in respect of personal data about himself or herself should raise the matter with one of the designated Data Controllers.

Staff Responsibilities

All staff are responsible for:

- Checking that any information that they provide to the organisation in connection with their employment is accurate and up to date.
- Informing the organisation of any changes to information that they have provided, e.g., changes of address, either at the time of appointment or subsequently. The organisation cannot be held responsible for any errors unless the employee had informed it of such changes.

Confidentiality: NHS Code of Practice

The Confidentiality Code of Practice is a result of a major public consultation that included patients, carers and citizens, the NHS, other healthcare providers, professional bodies and regulators.

The Code offers detailed guidance on:

- Protecting confidential information.
- Informing patients about uses of their personal information.
- Offering patients appropriate choices about the uses of their information; and
- The circumstances in which confidential information may be used or disclosed.

Caldicott Principles

The Caldicott Principles were developed in 1997 following a review of how patient information was handled across the NHS. The Review Panel was chaired by Dame

Fiona Caldicott and it set out six Principles that organisations should follow to ensure that information that can identify a patient is protected and only used when it is appropriate to do so. Since then, when deciding whether they needed to use information that would identify an individual, an organization should use the Principles as a test. The Caldicott Principles are:

Principle 1 – Justify the purpose(s) for using confidential information

Every proposed use or transfer of personal confidential data within or from an organization should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

Principle 2 – Don't use personal confidential data unless it is absolutely necessary

Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

Principle 3 – Use the minimum necessary personal confidential data

Where us of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

Principle 4 – Access to personal confidential data should be on a strict need-to-know-basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that the need to see. This may mean introducing access controls or splitting data flows where on data flow is used for several purposes.

Principle 5 – Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personal confidential data – both clinical and non-clinical staff are made fully aware of their responsibilities and obligations to respect patient confidentiality.

Principle 6 – Comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

In April 2013, Dame Fiona Caldicott reported on her second review of information governance and introduced a new 7th Caldicott Principle:

Principle 7 – the duty to share information can be as important as the duty to protect patient confidentiality

Health and Social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of the employers, regulators and professional bodies.

Subject Access Requests

Please see the Practice policy

Subject Consent

In most cases, the Practice can only process personal data with the consent of the individual. In some cases, if the data is sensitive, as defined in the DPA (and to which special rules apply), express consent must be obtained.

Status of this Policy

The Policy does not form part of the formal contract of employment for staff but it is a condition of employment that staff will abide by the rules and policies made by Heaton Mersey Medical Practice from time to time. Any failure to follow the Data Protection Policy may lead, therefore, to disciplinary proceedings.

Conclusion

This policy sets out this Practices commitment to protecting personal data and how that commitment is implemented in respect of the collection and use of personal data.