Marple Cottage Surgery

Information Governance Policy (summary)

Named Leads:
DPO & SIRO: Johan Taylor
The Caldicott Guardian: Dr Maher Al-Ausi

1. **Monitoring**
This policy will be reviewed on an annual basis

2. Legislation and related documents
This policy and a set of procedural document manuals are available on the practice intranet
Staff will be made aware of procedural document updates as they occur via email, meetings and training
Acts Covered Under Policy:

- Data Protection Act 1998, revised May 2018 (GDPR regulations)
- Health and Social Care Act 2012
- Human Rights Act 1998
- Computer Misuse 1998
- Electronic Communications Act 2000

3. IG Introduction:
IG is an overarching term used for information security, confidentiality and the accuracy, reliability and relevance of information used

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 that information is efficiently managed, and that appropriate policies, procedures, management accountability and structures provide a robust governance framework for information management.

4. **Commitments to IG**
Marple Cottage Surgery is committed to implementing information governance effectively and will ensure the following:

- Information will be protected against unauthorised access;
- Confidentiality of information will be assured;
- Integrity of information will be maintained;
- Information will be supported by the highest quality data;
- Regulatory and legislative requirements will be met;
- Business continuity plans will be produced, maintained and tested;
- Information governance training will be available to all staff as necessary to their role;

- All breaches of confidentiality and information security, actual or suspected, will be reported and investigated.

5. *Responsible Leads*

The IG Lead, Caldicott Guardian, Data Protection Officer and SIRO are senior persons responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing.
They play a key role in ensuring that the practice responsibilities satisfy the highest practicable standards for handling patient identifiable information.

The IG Lead – Mr J Taylor
- Is responsible for the implementation and monitoring of IG related policy and adherence, supported by the SIRO and Caldicott Guardian
- Fosters a culture for protecting and using data

The Caldicott Guardian – Dr M Al-Ausi
- Is advisory
- Is the conscience of the organisation
- Provides a focal point for patient confidentiality & information sharing issues
- Is concerned with the management of patient information

The Data Protection Officer – Mr J Taylor
- is to assist with monitoring internal compliance
- inform and advise on your data protection obligations
- provide advice regarding Data Protection Impact Assessments (DPIAs)
- act as a contact point for data subjects and the supervisory authority.

The SIRO – Mr J Taylor
- Is accountable
- Fosters a culture for protecting and using data
- Provides a focal point for managing information risks and incidents
- Is concerned with the management of all information assets

6. Caldicott guidelines

Personal and / or sensitive data must be kept confidential in accordance with the Data Protection Act 1998 and the Caldicott Principles. Marple Cottage Surgery will ensure that anyone processing personal data in relation to the organisation will comply with the Caldicott Principles on Use of Patient Identifiable Information:

1. Justify the purpose(s)
   Every proposed use or transfer of patient-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by an appropriate guardian.
2. Don't use patient-identifiable information unless it is absolutely necessary. *Patient-identifiable data items should not be used unless there is no alternative.*
3. Use the minimum necessary patient-identifiable information
   Where use of patient-identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identifiably.
4. Access to patient-identifiable information should be on a strict need to know basis
   Only those individuals who need access to patient-identifiable information should have access to it, and they should only have access to the information items that they need to see.
5. Everyone should be aware of their responsibilities

Action should be taken to ensure that those handling patient-identifiable information, (both clinical and non-clinical staff) are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6. Understand and comply with the law
   Every use of patient-identifiable information must be lawful. Someone in each organisation should be responsible for ensuring that the organisation complies with legal requirements.
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 their employers, regulators and professional bodies.

(The Caldicott Committee (December 1997), Dept of Health; *7th Caldicott Principle was added in the March 2013 Information Governance Review conducted by Dame Fiona Caldicott – also known as Caldicott2.

7. ***Data Controller***

'Data Controller' refers to the use or management of data but not the ownership of it. Marple Cottage Surgery is the Data Controller for all patient records that it holds and is aware of the differentiation between Data Owner and Data Controller

The Data Protection Act 1998 / 2018 requires every organisation that processes personal information to be registered with the Information Commissioner's Office (ICO), unless they are exempt. Failure to do so is a criminal offence. All data breaches should be reported to the ICO

8. Confidentiality

Marple Cottage Surgery is committed to safeguarding the confidentiality of personal information by ensuring it follows its legal obligations for data protection, information sharing, disclosures of personal confidential data and subject access rights. Information sharing must be consistent with the interests of the patient and / or staff.

8.1 Confidentiality policies and agreements

We have internal policies and external guidance to help adhere to the strict NHS Code of conduct.

8.2 Staff

We need to ensure that all staff members and partners of the practice follow procedures of security and confidentiality of information used and held in the practice.

Reference to: use of passwords, patient confidentiality, security of rooms and building, recording information and content of communications (staff confidentiality; IM&T security policy, staff policy/employees handbook/staff contracts, induction policies/schedules, meeting agendas, home working policy)

8.3 Contractors and third parties:

We also need to ensure that all Contractors and third parties e.g. visitors, students, etc that are granted access to staff only areas of the practice follow the same procedures of security and confidentiality of information used and held in the practice **(Contractor Confidentiality Agreement).**

9. Data sharing

We have strict internal processes regarding how we use and share data, which we publicise via posters at the practice, new patient welcome packs, practice website, etc.

9.1 Fair processing notice

We provide a Fair processing notice to inform patients how we use their personal information, which is available on the Practice website, and we promote confidentiality and protection of data via this policy, staff training.

9.2 Privacy notices
We provide a range of Privacy notices detailing how we use specific patient information

9.3 Informing Patients How we Use Data
Patient information regarding how we use their medical records is explained in leaflets listed below

Stockport Health Record (SHR) leaflet

Summary Care Record (SCR) patient leaflet

SCR letter to patients

SCR opt out form

Patient data sharing opt out form (Care.data, SCR, SHR)

9.4 General Principles of data sharing

- Verbal Permission must be obtained from patient and / or carer before divulging information. In certain cases, written consent should be obtained.
- Clarify to patient/carer, the persons to whom information will be given, and why.
- Get positive permission to share information.
- Verbal permission must be documented in the patient's medical record.
- Written permission must be filed or scanned into the patient's notes
- Medical information is accessed on a "need to know" basis in order to perform duties and no other.

9.5 Gaining consent
As a general rule, clients/service users should be asked for consent before their information is shared with colleagues or another organisation.
It is neither practicable nor necessary to seek an individual's specific consent each time information needs to be passed on in order to deliver care and treatment to clients/service users.

9.5.1 Express consent is given orally or in writing by a person who is fully informed about the purpose and nature of the data that is to be disclosed, and is needed for disclosure of identifiable data that is not for direct patient care – see A in diagram below (typically called "secondary uses").
Common secondary uses for data extracted by queries run against the practice patient database are; health care planning, commissioning of health services, research, education and training.
Express consent or dissent should normally be recorded in the patient's record. If consent is provided in the form of a signed consent form or letter, it should be stored in the patient's record, where possible, as a scanned document attached to the electronic record.

9.5.2 Implied consent is considered to be acceptable when identifiable information is shared with the health care team or others providing care, including administrative staff, for the purpose of provision of care to the identified patient(s) or it is used for clinical audit by the team providing health care – see B in diagram below.

Consent is inferred if the patient can be expected to understand that information will be disclosed for these purposes, the extent of the disclosure and their right to opt out, but they have not objected to the disclosure. If the data are to be processed fairly the information should be made available in a number of ways including poster, leaflets, discussion in a consultation, etc – SCR is an example

9.5.3 Inability to give consent
There are two types of circumstances where individuals cannot give consent. The first relates to clients/service users in a coma or suffering from some types of severe mental health

problems. In these cases the decision to share personal-identifiable information should be made on the individual's behalf by those responsible for providing care, taking into account the known views of clients/service users and carers. The client's/service user's best interests are paramount in these decisions. Where practicable, advice should be sought from the senior healthcare professional.

The reasons for the final decision should be clearly recorded.

The second circumstance is where individuals are listed on a database or other list and they cannot easily be asked for permission to use their information. By law it is difficult to transfer this type of information. You should have a full discussion with your data protection manager before any transfer.

9.6 Clinical decision
Where a decision is to be made whether to release information to a third party in circumstances other than those laid down below, **administrative and reception staff should refer the matter to a GP for an assessment of the situation before information is divulged.** Reception and administration staff should not ordinarily make confidentiality decisions where the authority is in doubt.

9.7 Sharing and disclosure policy
Practice guidance and who and what we share is included within the practice **Sharing and disclosure of patient identifiable information** policy.

9.8 Sharing information by phone
When sharing information over the telephone if established that the information requested can be shared always confirm that the requestor is genuine by asking for a switchboard line (never a mobile or direct line) and ringing back. If any doubt that the person is who they say they are speak to a manager.

10. Transfer of records

10.1 Method of transfer
Patient identifiable information can be transferred by the following means:
- Post - either internal NHS or Royal Mail or other reputable 3rd party carrier;
- N3 email - to and from .nhs.net email addresses;
- EMIS Web (which operates via secure N3 connections).
- CD media (only for transferring patient record data via the approved NHS commissioned medical transfer process)

Breach of these policies is a serious matter and could give rise to disciplinary action being taken.

10.2 Justification for Transfer
Information may be passed on where the patient has consented or if some such as
- Investigating complaints and legal claims.
- Teaching.
- Statistical analysis or research (specific consent should be sought to any activity relating to teaching or research that will involve people personally).
- Whistle blowing.
- Statute or court order requires the information.
- Other reasons eg protection of the public.

10.3 Responsibility for Passing on Information
GPs are responsible for their decision to pass on information. If unsure whether to pass on information ask the health professional responsible for the patient's care or a nominated senior manager.

The unauthorised passing on of patient information by any member of staff is a serious matter and may result in disciplinary action and possible legal action.

10.3.1 Non-identifiable Information (Anonymised)
Where anonymised information would be sufficient, identifiable information should be omitted where possible. Patient identifiable information should not be used unless it is essential for the purpose.

10.3.2 Identifiable Information
Includes data from which the patient can be identified by using any one of the following data items:

- Forename
- Surname
- Address
- Postcode
- Date of Birth
- Other dates (i.e. death, diagnosis)
- NHS Number
- Sex
- Ethnic Group

10.3.3 Non-Compliance
Non-compliance with this code of conduct by any person employed by the Marple Cottage Surgery may result in disciplinary action being taken.

11. Data quality: Electronic patient record
Each patient's medical record is integral to the health care of the patient, to the services we provide and to our business. Obviously it is essential that records are kept as accurately as possible and are up-to-date. The information in the patient records is needed to ensure our processes (eg appointment maintenance, call/recall, prescription reviews, clinical audit) run efficiently and effectively.

At the same time we are legally bound by the Data Protection Act and the Freedom of Information Act.

Also in 2008/9 we signed up to be compliant (GPSoC) with using the national NHS digital network (N3). This means that we maintain a secure environment for the information we hold and making sure that sharing information and/or data is appropriate.

All reference documents relating to Information Governance, including GPSoC, are on the NHS Digital website.

12. ***Information / Data Protection / Security***

12.1 Data Protection Registration
Marple Cottage Surgery is registered with the Information Commissioners Office; reference number Z5575348

Marple Cottage Surgery is aware that it handles and stores information about identifiable, living people – for example, about patients – and as such is legally obliged to protect that information.

In accordance with the Data Protection Act, we will:

- Only collect information that you need for a specific purpose
- Keep it secure
- Ensure it is relevant and up to date
- Only hold as much as you need, and only for as long as you need it
- Allow the subject of the information to see it on request

In committing to these,

12.2 IG Staff training
All staff who are employed for or on behalf of the GP Practice including full time, permanent, or temporary, must be aware of Information Governance and keep up to date with information governance training. The GP Practice will maintain a log of training and ensure staff are kept up to date.

12.3 Disaster recovery
A business impact assessment and business continuity plans are undertaken/reviewed whenever there is a structural change in the IT infrastructure, including replacement of servers.

12.4 Relevant legislation
This policy has been written to meet legal requirements and best practice guidance including:

- Data Protection Act 1998/ 2018 and GDPR
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- The Protection and Use of Patient Information (HSG 96 18)
- Caldicott Report on the Use of Patient Identifiable Information (1997) and subsequent Caldicott2 (2013)
- Freedom of Information Act 2000
- The Department of Health's guidance 'Confidentiality – NHS Code of Practice, Nov 2003
- Privacy and Electronic Communications Regulations
- Environmental Information Regulations
    - • Health and Social Care Act 2012
    - • Human Rights Act 1998
    - • Computer Misuse 1998
    - • Electronic Communications Act 2000

13. IT / Data Management

13.1 IT Equipment
Marple Cottage Surgery It equipment is owned and managed by Greater Manchester CSU

13.2 *IT Communications*
Marple Cottage Surgery has an N3 communications link which is subject to a maintenance and support agreement with BT.

13.3 Access Control Policies
System security comprises the following:

13.3.1 Risk Assessments
Prior to implementation of strategic systems changes, a risk assessment will be undertaken to determine the security requirements given the data concerned. For example, the level and type of access controls, location of hardware associated with the system, type of data held, etc.

13.3.2 Network Security
GM CSU ensures that its local network is protected by authentication, encryption and network connection controls which prevent unauthorised access including via wireless technology.

13.3.3 Cyber security
GM CSU ensure accreditation of cyber security

13.3.4 Account Management
User accounts should be amended immediately upon there being a change in the staff team to ensure that all user accounts are appropriate. This could be the existence of an account of the

level of information to which the member of staff has access and includes creation and removal of access rights.

The Managing Partner, or deputy, will be responsible for ensuring that access rights are appropriate when setting up User Accounts

13.3.5 Secure Logon Procedures

All computer systems should have a logon procedure that includes at least a unique user ID and password. The following features should be put in place for all Marple Cottage Surgery systems:

- System/application identifiers are not to be displayed until the logon procedure has been successfully completed.
- Where login errors are made there should be no indication as to which part of logon information is incorrect. This prevents unauthorised users identifying patterns when attempting to gain access to systems.
- The number of unsuccessful consecutive logon attempts is limited to 3.
- There is no limit as to the maximum time allowed for any one logon. However, password protected screen savers are used prevent unauthorised use.
- The password being entered is not displayed in clear text. The systems show a number of asterisk characters.
- Passwords should not be transmitted in clear text over the network under any circumstances.

13.3.6 Identifying users

In order to facilitate access control and audit functions all users have unique identifiers in the form of a unique username and password combination. Group IDs are not to be used.

13.3.7 Password management system

A password management system should operate as follows:

- No group passwords on the system; all users will be identified as individuals (including system administrators) when they log on.
- Users should change their initial password (issued by the system administrator) following their first logon.
- The system should log user passwords and prevent re-use.
- Users should change their own passwords at least quarterly but can do so more often where they feel their current one has been compromised.
- There are to be no restrictions on the use of alphas and/or numerics in order that users can set memorable passwords and are therefore encouraged to change them frequently.
- All passwords should be stored or transmitted using encryption or hashed.

13.3.8 User names and passwords

When staff are logged into a computer under their own username, they must either log out, ‘lock’ the computer or activate a password protected screensaver if they leave it.

Should staff wish to use an unattended computer where a previous user has left their access open, they must log out from that session before they commence their own session.

Staff must not disclose a personal password to anyone. A username and personal password is for one person’s use only. If a member of staff thinks someone else knows their password they must change it immediately and inform their Line Manager.

13.3.9 Session time-out

Timed and password protected screen savers should be used to prevent unauthorised access to data for timed-out sessions. The screen saver should be set to come on at 15 minutes or less.

13.3.10 Information access restrictions

File storage systems should be constructed in order to ensure all and only appropriate personnel have access to a folder which can then be viewed, altered, copied or deleted.

Data file owners are required to password protect all files which contain identifiable patient or staff data.

Sensitive system isolation: All Marple Cottage Surgery systems are considered to hold sensitive data and therefore there controls apply to all systems and isolation strategies are not considered appropriate/beneficial.

14. **Safe Havens / Secure Transfers of Information**

All transfers of personal confidential data must be undertaken as per the Data Protection Act 1998 (specifically principle 7). Please refer to the Secure Transfers of Information Procedure which details how the GP practice complies. Marple Cottage Surgery will ensure that:

a) Information should only be transferred for a justifiable purpose
b) The transfer should only take place when absolutely necessary
c) Only the minimum information necessary should be transferred
d) The information should be transferred on a need to know

15. Acceptable use of IT equipment

15.1 Prohibited Activities

Practice staff should not create, store, transfer (from any media or via email) or deliberately receive material that could be judged to be offensive. Offensive/inappropriate material or activities can include:

- Material that is abusive, threatening, serves to harass or bully, discriminates, encourages discrimination on racial/ethnic grounds, or on grounds of gender, sexual orientation, marital status, disability, political or religious beliefs.
- Material that may be obscene, indecent or tasteless.
- Material that may cause distress, inconvenience or anxiety.
- Material about illegal activities, including pornography, drugs, computer hacking, militant/extremist behaviour, violence or weapons – unless it is clearly related to your professional role.

If staff receive inappropriate email or become unintentionally connected to a website, which contains offensive or inappropriate material, the member of staff should disconnect from the site immediately and inform their Line Manager.

Deliberate activities with any of the following consequences are prohibited:

- Corruption or inappropriate destruction of data
- Using equipment in a way that makes systems unavailable to others
- Wasting staff effort or computing resources
- Introducing any weakness to, or compromising IT security.

Staff should not download and/or install any software unless authorised by Management Team.

15.2 Monitoring of activity

Where monitoring of systems takes place to identify system failure/capacity problems and misuse there will not be any monitoring of individual users unless there is justification to do so from general monitoring or concerns raised.

16. Personal data breaches / Information Security Incidents

16.1 Personal data breaches

Must be reported to the DPO immediately, who will inform the ICO within 72 hours
All breaches will be investigated as part of the practice SEA process and logged in the Data Breach Register
For further information please refer to Data Breach Notification Policy

16.2 Serious information Incidents

From June 2013 organisations must report IG SIRIs to the DH via the IGT incident reporting tool (as specified in the guidance).
Records should include appropriate, accurate and up to date information.
https://www.igt.hscic.gov.uk/resources/SIRI%20Reporting%20Tool%20Publication%20Statement.pdf

17. Access to Records (Subject Access Requests)

The GP practice complies with the Data Protection Act 1998 regarding the right for individuals to request access to their personal confidential data processed by GP Practice. Subject Access Requests policy

17.1 Summary:

- Any request by an individual for access to information that we hold about them must be made in writing.
- Requests can be made by individuals acting on behalf of the patient, but they must declare on the 'Subject Access' form why they have this entitlement and provide proof if required. This is generally where they have parental responsibility for a child (It may also be where an individual has been legally appointed by a Court of Protection or Guardianship order – in such circumstances seek further advice about the purpose and the details of what should be released.)
- The written request must contain sufficient information to enable the Practice to undertake the search required (e.g. Name, Address and Date of Birth).
- Marple Cottage Surgery is not obliged to comply with individuals' request until the requester has given you adequate information and one may wish to verify a person's identity by asking them to confirm their NHS number (if known).
- Marple Cottage Surgery does not have to release the information until the request has been received in writing.
- A from 25th May 2018 requests must be free from charge
- Under GDPR regulations, requests for access to records used to have to be met within 30 calendar days

17.2 Withholding Information

Information can be withheld, if it may cause the subject undue harm or distress if it is disclosed to them. For example where a patient is unaware of a suspected diagnosis, then they should not learn of this by reading their notes. It is advised that if information that may cause harm/distress is identified, then discussion with the patient should take place about this prior to, or as part of disclosure.

Information that identifies another individual can also be withheld. If the individual is a third party, then their identity should be protected unless they have consented to its release, or there is an overriding justification to release it without their consent. In such cases names could be blanked or substituted. Note however identity can be implied from comments or situations

If in any doubt about withholding information, please seek further support fro the Informatics Manager

17.3 Request Form

Patients requesting information should be supplied with the Subject Access Requests Form

18. Information Asset Register
Marple Cottage Surgery maintains and Information Asset Register that identifies all types of patient and staff data this is retained and identifies how it is kept secure.

19. **Records Management / Data Storage**
All records whether health or corporate records and held in either paper or electronic format will be stored securely within the practice.

For all types of records health professionals must:

- never inappropriately access records
- shut/lock doors, offices and filing cabinets
- query the status of visitors/strangers
- advise senior personnel if anything suspicious or worrying is noted
- confirm the identity of telephone callers

Manual records held within the GP Practice will be:

- held in secure room
- records tracked if moved, with a note of their current location
- returned to the filing system as soon as possible after use
- stored closed when not in use so that the contents are not seen by others
- inaccessible to members of the public
- kept on site unless removal is essential.

In the case of electronic records health professionals must:

- Always log out of any computer system or application when work is finished
- Always save documents on the network folders – never on the local hard drive. If the computer crashes or breaks, you will not be able to retrieve your files as they will be destroyed too
- never leave a terminal unattended and logged in. Always lock your screen.
- never share Smartcards or passwords with others
- change passwords at regular intervals to prevent others using them
- always clear the screen of a previous patient's information before seeing another

Staff Information
Staff information is retained for HR purposes in both paper and electronic form

20. Data Retention and Destruction of Records
There is detailed advice about the minimum retention periods applicable to NHS records and about records management in the Records Management
https://www.gov.uk/government/publications/records-management-nhs-code-of-practice

The recommendations apply to both electronic and manual records, and the BMA advises private practitioners to follow the same rules. When health professionals are responsible for destroying health records, they must ensure that the method of destruction is effective and does not compromise confidentiality. Incineration, pulping and shredding are appropriate methods of destroying manual records. Electronic data should be destroyed using appropriate data destruction software – further information can be sought from the IT provider.

For example the current recommendations from the Department of Health are contained in (HSC 1998/217: Preservation, Retention and Destruction of GP General Medical Services records relating to patients) recommends that medical records should be retained for the following periods:

- Records relating to children and young people (including paediatric, vaccination and community child health records) – until the patient's 25th birthday or 26th if an entry was made when the young person was 17; or 10 years after death of a patient if sooner.

- Records relating to persons receiving treatment for a mental disorder within the meaning of the Mental Health Act 1983 – 20 years after no further treatment considered necessary; or 10 years after patient's death if sooner.
- Maternity records – 25 years
- Records relating to those serving HM Armed Forces – not to be destroyed.
- Records relating to those serving a prison sentence – not to be destroyed.
- All other personal health records – 10 years after conclusion of treatment, the patient's death or after the patient has permanently left the country.

Where records are to be destroyed it should be done using a safe and reputable source and written confirmation of the destruction should be obtained and retained.

21. Freedom of Information Act 2000 (FOI)/Data Protection Act 1998
Marple Cottage Surgery supports the Freedom of Information Act 2000 in making public information available to those who request it.

We will do this by:
- Making information available to patients and for staff as appropriate upon request;
- Making sensible charges within legally acceptable parameters that are reflective of the actual cost of providing the information.

Where a patient requests access to their records or requests a copy of their records Marple Cottage Surgery will respond in accordance with the Data Protection Act 1998 requirements.

22. Non- Compliance
It is an offence to obtain, disclose, sell or advertise for sale, or bring about the disclosure of personal data, without the consent of the data controller. It is also an offence to access personal data or to disclose it without proper authorisation.

All staff working for or on behalf of the Marple Cottage Surgery agree to uphold information governance standards on signing their contract of employment. This agreement continues after employment, where relevant, has ceased. Non-compliance with this code may result in disciplinary action being taken in accordance with Disciplinary Procedures and in line with the NHS Care Record Guarantee.

23. Planning for when it may go wrong:
We need to ensure that we have protected ourselves against potential loss of continuity due to data, information or hardware loss [Reference Disaster recovery policy],

24. Monitoring and improvements:
Incidences regarding information security are used for training, improving policy and processes and are discussed and recorded appropriately, eg meetings, SEA reports, protocol amendments.

25. Data Security and Protection Annual Assessment
The practice complete an annual Data Security and Protection Assessment and develop and annual improvement plan