Information Governance Policy  
Includes data security, data and correspondence sharing, smart card, data retention, data disposal, and Caldicott principles

Millbrook Surgery

2022

Information Governance Policy  
Includes data security, data and correspondence sharing, smart card, data retention, data disposal, and Caldicott principles

Contents

[Information Governance Policy 3](#_Toc64285543)

[Purpose and definitions 4](#_Toc64285544)

[Scope 4](#_Toc64285545)

[Roles, rights, and responsibilities 5](#_Toc64285546)

[Principles of this policy 6](#_Toc64285547)

[Data breach policy 7](#_Toc64285548)

[Smartcards 8](#_Toc64285549)

[Copying correspondence – the principles of copying letters to patients 10](#_Toc64285550)

[Data retention 14](#_Toc64285551)

[Data disposal 16](#_Toc64285552)

[Training 18](#_Toc64285553)

[Monitoring and reporting 18](#_Toc64285554)

[Summary of NHS legal and mandatory documentation 19](#_Toc64285555)

[Versions 19](#_Toc64285556)

[Bibliography 20](#_Toc64285557)

# Purpose and definitions

The purpose of this policy is to provide guidance for staff and assurance to patients that Millbrook Surgery is committed to continually providing high quality healthcare for all patients and supporting the staff who provide this care. The aim of the policy is to provide staff with the foundation and principles to understand when information should be held privately and when and how to share information at the practice.

All patients regardless of age, gender, ethnic background, culture, cognitive function, or sexual orientation have the right to have their privacy and dignity respected.

Information governance is a concept that describes the processes and systems used by organisations to manage information. It refers to processes and systems to guarantee that:

* Records are held securely.
* Information is recorded clearly and accurately.
* Information can be read and relied upon by people providing care.
* Patient confidentiality is respected.

Clear and appropriate information governance is a firm foundation for good medical practice at Millbrook Surgery.

## Scope

This policy applies to all employees of Millbrook Surgery, contractors, seconded staff, placements, and agency staff.

## Roles, rights, and responsibilities

**Caldicott Guardian**

The Caldicott Guardian acts as the conscience of the organisation and works within the remit of the national information governance framework.

He or she has a responsibility to have a detailed understanding of this framework and undertake regularly training to maintain this understanding.

They have a responsibility to guide staff in when information sharing is required or requested.

Caldicott Guardians should facilitate appropriate information sharing and to guarantee that this sharing is proportionate and handled securely.

**All staff**

All staff have a responsibility to understand the principles of information governance to undertake regular training and to adhere to this policy.

All staff have a responsibility to access only the information they need when they need it and to ensure that they take reasonable steps to prevent access to information by others as appropriate. For example, locking doors, computers when not in use and not sharing access or passwords to systems.

All staff have a responsibility to uphold the processes of data privacy for all patients. To understand their responsibility to ensure that all data they enter is accurate, timely, and appropriately detailed for the purposes of patient safety.

All staff should be aware of how to ensure that patient information is kept securely and not shared with anyone unless this is clinically appropriate, with consent (where appropriate) and with the knowledge of the Caldicott Guardian.

**Practice manager**

To update the policy, ensure that it is aligned with national guidelines, distribute appropriately, and ensure that staff are trained at induction and at regular intervals so that they are aware of the principles of information governance and the content of the practice policy.

## Principles of this policy

This policy adheres to local and national guidance and policy including the GMC guidelines on sharing information, NHS Information Governance toolkit, NHS Digital Security Standards, GDPR, and the Data Protection Act 2018.

When sharing information, we are mindful of GMC guidelines that are to:

* Use the minimum necessary personal information.
* Use anonymised information if it is practicable to do so and if it will serve the purpose.
* Manage and protect information.
* Make sure any personal information we hold, or control is effectively protected at all times against improper access, disclosure, or loss.
* Be aware of our responsibilities.
* Develop and maintain an understanding of information governance that is appropriate to our roles.
* Comply with the law.
* Be satisfied that we are handling personal information lawfully.
* Share relevant information for direct care in line with the principles in this guidance unless the patient has objected.
* Ask for explicit consent to disclose identifiable information about patients for purposes other than their care or local clinical audit unless the disclosure is required by law or can be justified in the public interest.
* Tell patients about disclosures of personal information we make that they would not reasonably expect, or check they have received information about such disclosures, unless that is not practicable or would undermine the purpose of the disclosure.
* We will keep a record of decisions to disclose, or not to disclose, information.
* Support patients to access their information.
* Respect, and help patients exercise, their legal rights to be informed about how their information will be used and to have access to, or copies of, their health records.

## Data breach policy

We have a clear process so that we can report, escalate, and investigate any possible data breach.

The most senior member available should be informed about the possible breach to firstly investigate the circumstances, contain it, and assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen and ultimately decide whether a personal data breach has occurred and whether to report this to the Information Commissioner’s Office (ICO).

The ICO advise that an organisation needs to establish the ‘likelihood and severity of the resulting risk to people’s rights and freedoms. If we establish that is likely that there will be a risk, then we must notify the ICO. If the decision is made not report the breach on the balance of risk, we need to be able to justify this decision and how we arrived at the decision, and this will be fully documented. We will also set out how we will contact those individuals involved in the breach (if this deemed appropriate) in order to explain the breach and offer an apology.

Further plans will be made to reduce any future risks and mitigation will also be put in place to avoid future data breaches of this type.

## Smartcards

Smartcard access is based on role-based access control (RBAC). RBAC refers to the national policy that provides the framework and architecture to link the user, the system, and the national Spine that stores patient information. As a framework RBAC aims to help deliver a specific commitment contained in the NHS Care Record Guarantee, which is to show only those parts of a patient record needed to deliver care.

**Smartcard user responsibilities**

When a smartcard is issued, a personal identification number (PIN) must be chosen by the individual to whom the card is registered. This PIN must not be written down or shared with anybody else, as stipulated in the organisation’s information security requirements and the smartcard terms and conditions. Smartcards must be kept securely at all times.

It is clear that the security of this card is the responsibility of the user.

Access gained with a Smartcard will be viewed as access by the registered cardholder, and any inappropriate use will be their responsibility.

Smart cards must not be left in unattended keyboards, and when staff are away from their desk the smartcard must be taken with them.

**Lost or stolen smartcards**

If a smartcard is lost or stolen, this must be reported immediately.

An incident form must also be completed, and local incident reporting procedures followed. The lost or stolen smartcard will be cancelled, and a replacement smartcard issued. A replacement card must be obtained immediately and only collected in person from the agent printing the card to ensure ID checks are adhered to.

Colleagues must not be asked to share their smartcard and/or PIN, as this type of misuse may be subject to disciplinary procedures in line with the practice disciplinary policy.

**Forgotten smartcards**

If the user does not have their smartcard when arriving for work, the user must report to their line manager who may be able to issue a local username and password for the system required, alternatively, the user might be sent home in order to collect the card. Any delays that would be experienced through collecting the card should be discussed with his or her line manager. Repeated episodes of this type may be dealt with under practice disciplinary procedures.

**PIN code unlocking/changing**

If the smartcard has been locked or the user has forgotten their PIN, they must contact the local smartcard administrator for the organisation in order for the change and unlock process to be performed.

**Sharing of smartcards**

Under NO circumstances should smartcards and PINs be shared. Monitoring and review of the use of smartcards and PINs will be conducted by the practice. Inappropriate access with a smartcard will be investigated by the practice and both the registered smartcard holder and the person using the card maybe subject to disciplinary procedures.

**Change of job role/leaving the organisation**

If a member of staff leaves the organisation to work within another organisation of the NHS or if they move to another department within the current organisation they will retain their smartcard, but the current roles/positions will need to be deactivated requesting the removal within the smartcard administering system. If a member of staff leaves the NHS, the access will be deactivated by the organisation and the smartcard must then be retained by his or her line manager on their last day of employment. The line manager will need to dispose of the card in line with information governance standards and smartcard policy.

**Issue of smartcards**

If it is determined that the role of a member of staff requires access to an application, they must be registered as an authorised user. Appropriate access must be organised through the line manager. The access allocated to staff must be based on the role they perform and must be agreed by their line manager before any smartcard is issued.

All new smartcard user applications must be supported by adequate identification documentation.

# Data retention

A health record is anything which contains information in direct relation to the clinical history, diagnosis, treatment, or review of a service user which has been created or gathered as a result of the work of NHS employees. This can include:

* + Service user Health Records (electronic or paper based).
  + Microfiche, scanned, or digitalised health records.
  + Audio and videotapes, cassettes, photographs, emails, scanned records, SMS text messages, twitter or skype, or websites and intranet data.
  + Data processed for secondary use purposes. Secondary use is any use of person level or aggregate level data that is not for direct care purposes. This can include data for service management, research or for supporting commissioning decisions.

Personal medical records in the NHS, including imaging are held to be the property of the Secretary of State. NHS medical records are stored in premises designated by the appropriate authority.

Access to a patient's medical records is governed in the patient's interest by the ethics of the medical and allied professions. Under the Public Records Act 1958 employees are responsible for any records that they create or use in the course of their duties.

Therefore, any records created or received by an employee of the NHS are public records are subject to both legal and professional obligations.

The records management function is a specific responsibility within our organisation. It provides a managerial focus for records of all types in all formats, including electronic records, throughout their lifecycle from creation through to disposal.

The records management function has clear responsibilities and objectives and are resourced to achieve these. A designated member of staff (the Practice Manager) has the lead responsibility for records management within Millbrook Surgery organisation.

This policy:

* Outlines the role of records management within the organisation and its relationship to the organisation’s overall strategy.
* Defines roles and responsibilities within the organisation, including the responsibility of individuals to document their actions and decisions in the organisation’s records and to dispose of records appropriately when they are no longer required.
* Provides a framework for supporting standards, procedures and guidelines, and regulatory requirements.
* Indicates the way in which compliance with the policy and its supporting standards, procedures, and guidelines will be monitored and maintained.
* Provides the mandate for final disposition of all information by the partners overseeing the processes and procedures.
* Meets the records management requirements of the FOIA, the DPA and the Environmental Information Regulations, Data Processing Impact Assessments, subject access requests and GDPR.

This policy statement will be reviewed at regular intervals (at least once every 2 years) and if appropriate should be amended to maintain its relevance.

**Staff records**

Staff record summary will contain as a minimum:

* + Summary of the employment history with dates.
  + Pension information including eligibility.
  + Any work-related injury.
  + Any exposure to asbestos, radiation, and other chemicals which may cause illness in later life.
  + Professional training history and professional qualifications related to the delivery of care.
  + List of buildings where the member of staff worked, and the dates worked in each location.
  + Disciplinary case files can be held in a separate file so they can be expired at the appropriate time and do not clutter up the main file. That does not mean that there should be no record that the disciplinary process has been engaged in the main record.

**Record retention guidelines**

Different records should be retained for varying lengths of time according to guidance provided by the Information Governance Alliance.

Appendix 3 of the document can be downloaded as a spreadsheet from NHS Digital. <https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care>

Our retention guidelines include:

**GP records** – retain for 10 years after the death of a patient.

**Pharmacy, controlled drugs** – retain for 20 years and review.

**Telephony systems** (including out of hours services) – retain for 3 years.

**Cause of death counterfoil** – retain for 2 years.

**Staff duty rota** – retain for 6 years.

**Staff and Occupational health record** – retain until 75th birthday or for 6 years after staff member leaves employment.

**Visitor data** – retain for 2 years

# Data disposal

The data disposal policy is to ensure that information stored on equipment and media is safely destroyed or erased. This document is applied to all the information and communication technology at Millbrook Surgery practice.

**Reference documents**

* Regulation of Investigatory Powers Act 2000.
* The Privacy and Electronic Communications Regulations 2003.

**Disposal and destruction of equipment and media**

All data and licensed software stored on mobile storage media (e.g., on CD, DVD, USB flash drive, memory card, etc.; but also, on paper) and on all equipment containing storage media (e.g., computers, mobile phones, etc.) will be disposed of securely using an approved data destruction company. The company used must be ISO 27001 certified and carry out data destruction to NHS data sanitisation standards.

**Hardware storage devices**

We take the approach that it is easier to dispose of all hardware securely, rather than attempting to separate out the sensitive items.

Devices are physically destroyed, or the information is destroyed, deleted or overwritten using techniques to make the original information non-retrievable rather than using the standard delete or format function. Destruction and disposal of records are logged and held by the practice manager.

We dispose of all electrical equipment using WEEE compliant companies who only dispose within the UK. Equipment that is broken or non-reusable is permanently destroyed to make reading data from the device impossible. Equipment that is of no use but is useable is cleared of any data and software that may be on them before disposal.

**Any other sensitive information**

Erasure and destruction records, commission for the destruction of information. Formal procedures for the secure disposal of media are in place to minimise the risk of confidential information leakage to unauthorised persons. The procedures for secure disposal of media containing confidential information are proportional to the sensitivity of that information.

All medical records containing confidential information are stored in locked areas.

**Distribution**

Employees will be made aware of this policy via TeamNet.

Patients will be made aware of this policy using patient leaflets and on the practice website.

## Training

All staff will be given training on information governance and data security at induction and at regular intervals thereafter.

Any training requirements will be identified within an individual's Personal Development Reviews. Training is available in the Training module within TeamNet.

**Equality and diversity impact assessment**

In developing this policy, an equalities impact assessment has been undertaken. An adverse impact is unlikely, and on the contrary the policy has the clear potential to have a positive impact by reducing and removing barriers and inequalities that currently exist.

If, at any time, this policy is considered to be discriminatory in any way, the author of the policy should be contacted immediately to discuss these concerns.

Monitoring and reporting

Monitoring and reporting in relation to this policy are the responsibility of the practice manager.

The following sources will be used to provide evidence of any issues raised:

* PALS.
* Complaints.
* Significant and learning events.

Any incidents relating to information governance and security will be monitored via incident reporting.

## Summary of NHS legal and mandatory documentation

Department of Health. The common law duty of confidentiality <https://webarchive.nationalarchives.gov.uk/+/http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/Browsable/DH_5803173>

National health Services Act 2006 <http://www.legislation.gov.uk/ukpga/2006/41/contents>

Health and Social Care Act 2012 <http://www.legislation.gov.uk/ukpga/2012/7/contents>

Freedom of Information Act 2000 <http://www.legislation.gov.uk/ukpga/2000/36/contents>

Data Protection Act 2018 (includes GDPR) <http://www.legislation.gov.uk/ukpga/2018/12/contents>

Human Rights Act 1998 <http://www.legislation.gov.uk/ukpga/1998/42/contents>

NHS Digital Destruction and Disposal of Sensitive Data [destruction-and-disposal-of-sensitive-data-version-32.pdf (sfh-tr.nhs.uk)](https://www.sfh-tr.nhs.uk/media/4864/destruction-and-disposal-of-sensitive-data-version-32.pdf)

## Versions

Document review history

|  |  |  |  |
| --- | --- | --- | --- |
| **Version number** | **Author/reviewer** | **Summary of amendments** | **Issue date** |
| 1.0 | Clarity Informatics | Policy written | 30.4.2020 |
| 2.0 | Clarity Informatics | Added smartcard and copying correspondence | 21.5.2020 |
| 3.0 | Clarity Informatics | Added data retention periods and data destruction/sanitation information | 15.2.2021 |
| 4.0 | Clarity informatics | Reviewed and updated | 11.2.2022 |
| 5.0 |  |  |  |
| 6.0 |  |  |  |
| 7.0 |  |  |  |

# Bibliography

Department of Health. Report on the review of patient-identifiable information <https://webarchive.nationalarchives.gov.uk/20130124064947/http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_4068404.pdf>

UK Government. Caldicott Review: information governance in the health and care system 2013 <https://www.gov.uk/government/publications/the-information-governance-review>

Information Commissioner’s Office <https://ico.org.uk/>

Information Commissioner’s Office. Guide to the General Data Protection Regulation (GDPR) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/>

General Medical Council <https://www.gmc-uk.org/>

Primary Care Support NHS England. How to move medical records with labels <https://pcse.england.nhs.uk/services/medical-records/how-to-move-medical-records/>

Information Commissioners Office. What is the Freedom of Information Act? <https://ico.org.uk/for-organisations/guide-to-freedom-of-information/what-is-the-foi-act/>

NHS England. Information Governance Toolkit <https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/data-security-and-protection-toolkit>

NHS England. About information governance <https://www.england.nhs.uk/ig/about/>

NHS Digital. Data security standards <https://digital.nhs.uk/about-nhs-digital/our-work/nhs-digital-data-and-technology-standards/framework/beta---data-security-standards>

Care Quality Commission. Data security and protection – expectations for general practice <https://www.cqc.org.uk/guidance-providers/gps/nigels-surgery-85-data-security-protection-expectations-general-practice>

NHS X. Securing excellence in primary care (GP) digital services: the primary care (GP) digital services operating model 2019-2021 <https://www.england.nhs.uk/wp-content/uploads/2019/10/gp-it-operating-model-v4-sept-2019.pdf>

NHS Digital. Records management code of practice for health and social care 2016. <https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care>

Mathioudakis, A., Rousalova, I., Gagnat, A.A. et al. How to keep good clinical records. *Breathe (Sheff)*. 2016;12(4): 369-373 <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5297955/>

UK Government. Confidentiality: NHS Code of Practice <https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice>

UK Government. Information Security Management: NHS Code of Practice <https://www.gov.uk/government/publications/information-security-management-nhs-code-of-practice>

UK Government. NHS information governance: legal and professional obligations <https://www.gov.uk/government/publications/nhs-information-governance-legal-and-professional-obligations>