Data Protection and Confidentiality Policy

Version 5.0

Version:	5.0	Date approved:	2023-01-18
Author:	Head of IG and S & DPO	Review date:	2025-01-18
Approved by:	IGSG	Document uncontrolled when printed	

DOCUMENT CONTROL SHEET Key Information:

DOCUMENT CONTROL	
Owner:	Head of Information Governance and Security & DPO
Document Control:	Version 5.0
Date Live From:	26 July 2021
Review/Approval Group:	IGSG
Last Reviewed:	Jan 2023
Review Due/Cycle:	2 Years from approval

DOCUMENT CHANGE LOG			
Version	**Author**	**Date**	**Comment**
V1.0	A. Morton	Jan ‘11	Final approved by IGSG 18.01.11
V2.0	S. Gibson	Feb '16	Re-write to include Confidentiality and Privacy
V2.0	S. Gibson	Apr '16	Approved by EMT
V2.1	A. Craig	Feb ‘19	Document Review
V2.2	S. Gibson	Apr ‘19	Document Review
V3.0	S. Gibson	Apr ‘19	Approved by IGSG
V3.01	IGS	Jun ‘21	Document Review
V3.02	IGS	Jun ’21	Format update
V3.03	IGS	Jul ‘21	Document Review
V4.0	IGSG	Jul ‘21	Approved by IGSG
V4.01	IGS	Dec ‘22	Document Review
V4.02	IGS	Dec ‘22	Document Review
V4.03	S. Gibson	Dec ‘22	DPIA Section Added
V4.04	S. Gibson	Dec ‘22	Amended links
V4.05	S. McConnell	Jan ’23	Minor update
V5.0	S. Gibson	Jan ‘23	Approved by IGSG

Approvals: this document was formally approved by:

Name/Title/Group	Date:	Version:
EMT	2016.04.26	2.0
IGSG	2019.04.24	3.0
IGSG	2021.07.26	4.0
IGSG	2023.01.18	5.0

NB. This document is uncontrolled when printed. The contents of this document are subject to change, any paper copy is only valid on the day of printing. To ensure you have the most up to date version of this document please access the document directly from the NHS 24 Intranet site.

Table of Contents

1. Introduction

1.1 This is the Data Protection and Confidentiality Policy adopted by NHS 24.

1.2 NHS 24 needs to collect and use large volumes of sensitive and personal identifiable information that is confidential information relating to patients, employees, suppliers and others with whom it communicates in the provision of services. In addition, it may be a legal requirement to collect and use certain types of information in compliance with this legislation. All such personal information, no matter how it is collected, recorded or used, must be dealt with properly and securely to ensure Confidentiality, Integrity and Availability.

1.3 NHS 24 can be both a Controller and a Processor as defined by the UK General Data Protection Regulation and as such it seeks to ensure that all personal and sensitive information is not divulged without just cause and that it complies with the requirements of all current data protection legislation in force at any given time.

1.4 All NHS 24 staff have an ethical and legal duty to keep Personal Identifiable Information (PII) and business information confidential. This policy details how all NHS 24 Staff, including contractors, students and volunteers (who may not have a contract with NHS 24) will meet its legal obligations and requirements concerning data protection, confidentiality and privacy.

2. Policy Objectives

2.1 The objectives of this policy are to ensure that:

- The principles that govern all uses of personal identifiable information are clearly understood by all.
- NHS 24 as Controller complies with the Data Protection Act 2018, UK General Data Protection Regulation (GDPR), Human Rights Act 1998, and other relevant legislation at all times.
- Staff members clearly understand through this policy our commitment towards effective data protection, confidentiality and privacy compliance.
- Staff members who manage and/or process personal identifiable information understand their responsibilities in relation to data protection, confidentiality and privacy; that they are contractually responsible for following good data protection practice and are appropriately trained and effectively supervised.
- NHS 24 will ensure that all new systems and processes, when appropriate, will be subject to a Data Protection Impact Assessment.
- That the rights of any individual are observed in line with the relevant Data Protection Legislation and the associated principles (See Appendix 1) and that they know who to approach regarding these rights and that they are promptly and courteously dealt with.

3. Policy Statement

3.1 NHS 24 will take all reasonable measures to comply with its legal responsibilities under the Data Protection Legislation, the Human Rights Act 1998 and the Common Law Duty of Confidentiality.

4. Definition of Terms

4.1 **Personal Data** – as defined by the UK GDPR means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Some common personal data items are:

- Name
- Address
- Date of birth
- Community Health Index (CHI) number.

4.2 **Special Categories of Personal Data** reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Under the legislation the processing of this "special category data" is subject to more stringent conditions.

4.3 **Processing** – means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

4.4 **Controller** – means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. NHS 24 as the public authority is the Controller.

4.5 **Processor** – means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.

4.6 **Caldicott** - The Caldicott report raised concerns regarding the way information flowed, not only within NHS organisations, but also between non-NHS organisations. Both Caldicott and the Data Protection Legislation cover information held on paper as well as electronically. All staff must adhere to these principles. (See Appendix 1).

5. Scope of the Policy

5.1 This policy applies to all employees, volunteers and any contractors ("Staff") supplying services or carrying out work on behalf of NHS 24 from any location regardless of the access method or equipment used who have access to or are responsible for any NHS 24 information.

6. Legal Context

6.1 **Data Protection Legislation** – legislation which establishes a framework of rights and duties which are designed to safeguard personal information. This framework balances the legitimate needs of organisations to collect and use personal data for

business and other purposes against the right of individuals to respect for the privacy of their personal details. The legislation applies to “personal (including sensitive or special category) data” held about identifiable living individuals. The relevant data protection legislation means the UK General Data Protection Regulation (EU) 2016/279, the Data Protection Act 2018, the Privacy and Electronic Communications (EC Directive) Regulations 2003, the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice (Interception of Communications) Regulations 2000 (SI 2000/2699), and any applicable decisions and guidance made under them together with any other law, statute, directive, regulation, other legislation in whatever form, delegated act (under any of the foregoing), rule or other binding restriction, decision or guidance in force from time to time with regards to the processing of personal data.

6.2 NHS 24 has a duty to keep all personal information held on patients and staff confidential and secure. Employees must ensure they do not pass on information to anyone unless authorised to do so and must also ensure that all personal details are processed in accordance with the rights of the data subjects as defined under the Data Protection Legislation.

6.3 The organisation and the staff employed within NHS 24 must abide and adhere to the Principles of the Data Protection Legislation: (See Appendix 1).

6.4 **Human Rights Act 1998** - Article 8.1 of the European Convention on Human Rights, as given effect to by the Human Rights Act 1998, provides that “everyone has the right to respect for his private and family life, his home and his correspondence.”

6.5 **Common Law duty of Confidentiality -** Common law is not based on statute and Acts of Parliament, it is based on the decisions made by the courts on specific cases and is developed over time. This law underpins the duty of confidentiality that states that:

- ‘If information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information provider's consent.’
- Information is confidential when it is not in the public domain, not common knowledge and is worthy of protection due to the damage, harm or distress that disclosure might cause
- This duty extends to all staff who work for NHS 24.

6.6 **Confidentiality Exception -** Where it is known, or believed, that an individual may be at risk of harm then the interests of public protection override the need for confidentiality.

7. Responsibilities

7.1 **Chief Executive**
The Chief Executive has overall responsibility for NHS 24's compliance with the Data Protection Legislation, Common Law Duty of Confidentiality and associated regulations.

7.2 **Senior Information Risk Owner (SIRO)**
The Senior Information Risk Owner has responsibility for the management and mitigation of risks associated with NHS 24's information management processes.

7.3 **Caldicott Guardian**
The Caldicott Guardian is responsible for ensuring that NHS 24 satisfies the highest practical standards for handling patient information standards in compliance with the Caldicott Principles.

7.4 **Head of Information Governance and Security and DPO**
The implementation of, and compliance with, this policy is delegated to the Head of Information Governance and Security and DPO who will act as data protection officer as designated by Article 37 of the UK GDPR and will provide advice and guidance on all areas of Information Governance and Security. The responsibilities of the Head of Information Governance and Security & DPO are as follows:

- Ensuring relevant legislation and guidance are incorporated into NHS 24 practices
- Inform and advise NHS 24 and its employees on how to carry out their obligations pursuant to data protection law
- To monitor compliance with the UK GDPR, as well as other domestic law relating to data protection and with the policies of NHS 24 in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits
- To provide advice where requested as regards to data protection impact assessments and to monitor its performance pursuant to Article 35 of the UK GDPR
- To cooperate with the Information Commissioner
- To act as the point of contact for the Information Commissioner on issues relating to processing, including the prior consultation referred to in Article 36 of the UK GDPR, and to consult where appropriate, with regard to any other matter.

The Information Governance and Security Team, led by the Head of Information Governance and Security & DPO will provide training and training materials for staff in relation to data protection, confidentiality and privacy.

7.5 **Information Asset Owners**
The Executive Management Team are the responsible Information Asset Owners (IAOs) for the activities aligned to them. They are required to ensure that the processing of personal data further to those activities or in respect of any projects or initiatives they lead on behalf of NHS 24 is conducted appropriately and in compliance with the Data Protection Legislation. They are required to seek the involvement of the DPO as per article 38 of the UK GDPR. The IAOs will ensure that any new or substantially changed use of personal data (such as a new or upgraded system or business process) will be subject to a Data Protection Impact Assessment.

7.6 **Line Managers**
Managers at all levels are responsible for ensuring that the staff for which they are responsible are aware of, understand and adhere to this policy. They must ensure their teams undertake all appropriate training and are aware of their responsibilities and the most effective way of ensuring adequate information security and confidentiality.

7.7 **Staff**
All staff, whether permanent, temporary or contracted and contractors must comply with the requirements of their contract in relation to 'duty of confidentiality' and to adhere to this policy and the related documents and procedures which can be found on the NHS 24 Intranet. Staff will undertake mandatory training required in order to achieve a standard of knowledge and understanding in these issues relative to the duties of their post.

7.8 **Information Governance & Security Group**
The Information Governance & Security Group (IGSG) is chaired by the SIRO. It provides oversight and drives progress in relation to Information Governance and security activities. The IGSG meets quarterly and provides assurance to the NHS 24 Board through quarterly reports and an annual report to sub-committees of the Board.

8. Implementation

8.1 All staff contracts will include an employee commitment to confidentiality and to abide by the principles laid down in the Data Protection Legislation. To ensure that knowledge of these guidelines and procedures is kept up to date, staff will be required to sign a confidentiality statement. It is the responsibility of all NHS 24 to ensure compliance with all legislation, related policies, procedures, protocols and supporting guidance contained and referenced in this policy document.

8.2 Any staff transferring between NHS organisations, any appointments of temporary staff, agency staff, students or trainees, must be made aware of this policy and other related documents by the appropriate line manager/team leader.

8.3 The Head of Information Governance and Security and DPO will ensure that NHS 24 will register as a Controller with the Information Commissioner. Information on this registration is available online on the Information Commissioners website at:

https://ico.org.uk/about-the-ico/what-we-do/register-of-fee-payers/ and by entering NHS 24 at the Name.

8.4 All contracts with external suppliers must comply with CEL 25 (Safeguarding the Confidentiality of Personal Data Processed by Third Party Contractors).

8.5 All contracts with external suppliers must include clauses relating to confidentiality and Data Protection or have a separate agreement, such as a data processing agreement.

8.6 NHS 24 are mandated by the Scottish Government (MEL (1999) 19) and (HDL (2006)41) to ensure that there is always a nominated 'Caldicott Guardian' with ultimate responsibility for maintaining the confidentiality of patient identifiable data and as a public authority under the Data Protection Legislation to designate a Data Protection Officer with specific responsibility for advising on and monitoring data protection within the organisation.

8.7 This policy will be reviewed every two years to ensure that it continues to be effective and comply with current legal requirements.

8.8 An annual review and audit will be made of the way in which personal identifiable information is managed in relation to data protection compliance.

8.9 In line with the Data Protection Legislation in the case of a personal data breach the Controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the ICO.

8.10 In line with the Network and Information Systems Regulations 2018 NHS 24 as an Operator of Essential Services (OES) must notify the Scottish Government regulators (Health Competent Authority (CA)) about any incident which has a significant impact on the continuity of the essential service that NHS 24 provides. This must be reported without undue delay and in any event no later than 72 hours after having become aware that a NIS incident has occurred.

8.11 NHS 24 share relevant information with other NHS Scotland Health Boards under the terms of the Intra-NHS Information Sharing Accord.

8.12 NHS 24 utilise the Scottish Government Information Sharing Toolkit. This enables NHS 24 and partner agencies to share personal information in a lawful manner.

8.13 Operational protocols and guidelines which underpin this policy are available on the NHS 24 Intranet.

8.14 Where deemed appropriate by management, breaches of the legislation covered in this policy and any associated policy may result in action being taken through current NHS 24 disciplinary procedures.

9. Access and Rights to Information

9.1 Under the Data Protection Act Legislation, individuals have a right to see or be provided with a copy of personal information the organisation processes concerning them, this is known as a ‘Data Subject Access Request’. Information and guidance for handling Data Subject Access Requests is available on the NHS 24 Intranet.

9.2 Data subjects also have other rights detailed in the Data Protection Legislation such as Rectification, Erasure, Restriction of Processing, Data Portability and the right to Object to automated decision making, including profiling. Information on these rights is available on the NHS 24 Intranet.

10. Data Sharing/Processing Agreements

10.1 A data processing agreement is a contract between two parties containing details of how data is processed, including its scope and purpose. The agreement will define what the roles of the Controller and Processor are. It is a statutory requirement to have a data processing agreement in place prior to the Processing of the personal data starting. The responsibility for ensuring a data processing agreement is in place lies with the Information Asset Owner for the project or initiative.

10.2 A data sharing agreement is a contract between two or more parties where all parties are Controllers. Unlike a data processing agreement, the recipient is not acting under the instruction of the disclosing party. It is best practice to put in place a data sharing agreement prior to sharing personal data. The responsibility for putting a data sharing agreement in place lies with the Information Asset Owner for the project or initiative.

10.3 A data sharing/processing agreement can either be a separate agreement or part of a wider contract, for example, a contract for the provision of services.

10.4 A record of the data processing or sharing agreement should be added to the contract log.

10.5 NHS 24's Data Protection Officer can give advice on whether a data processing or sharing agreement is required.

10.6 Both data sharing and processing agreements should be kept under regular review which is the responsibility of the Information Asset Owner.

11. Data Protection Impact Assessments

11.1 Where personal or special category data is involved then as per the UK GDPR and in line with the principles of privacy by design and Accountability a Data Protection Impact Assessment (DPIA) must be completed for any new or change in service to ensure all risks to the rights and freedoms of natural persons are appropriately considered, controlled and reported. It must be instigated as soon as the new or change in service is identified by the Project/System Manager or Information Asset Owner and for all new systems. The DPIA must be completed prior to the processing of personal data.

11.2 Where similar processing activities are undertaken consideration can be given to using one overarching DPIA.

11.3 Generation and completion of the DPIA is the responsibility of the Information Asset Owner (IAO) for the personal data. The IAO (or where appropriate the relevant delegate and/or project team) should consult with the Data Protection Officer and the Information Governance and Security team who will input to and form part of the assessment of the DPIA.

11.4 DPIAs must be instigated at the start of a project or planned change and reviewed during the project and/or planned change. This allows for any risks which are identified through the DPIA process to be appropriately mitigated prior to the commencement of the processing.

11.5 Where it is considered appropriate, the DPO may recommend a DPIA for approval to the SIRO and the IAOs with conditions. Such conditions will have an agreed time limit for completion of the condition.

11.6 The DPIA must go through an approval process which includes the Senior Information Risk Owner, the Caldicott Guardian (where patient data is involved), the Data Protection Officer and the relevant Information Asset Owner(s) which will include the business process ownership.

11.7 NHS 24 will utilise an electronic system for generation, storage, review and approval of DPIAs.

12. Data Protection by Design and by Default

12.1 NHS 24 are required to, at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures. This is to ensure that only the necessary personal data is processed and that the risks to the processing activity can be minimised.

12.2 This will include measures such as:

- Detailing the purposes of the processing activity
- Ensuring there is an appropriate legal basis
- Measures that ensure data will not be processed for another purpose
- Measures to ensure the accuracy and integrity of the data
- Controls for accessing the data, ensuring it can only be accessed by those who require the access
- Ensuring that any relevant data processing or data sharing agreements are in place
- Ensuring that the relevant data protection notices are in place
- Ensuring that technical controls (such as encryption) are in place as required
- Ensuring that the process to be followed in the event of a security or data breach are detailed.

13. Relevant Legislation Guidance and Code of Practice

13.1 This policy should be read in conjunction with the following:

Local Policies can be found on the NHS 24 Intranet.

Legislation and National Policies and Codes of Practice

- Data Protection Act 2018
- General Data Protection Regulation
- UK GDPR improved formatting (third party link)
- The Network and Information Systems Regulations 2018
- Freedom of Information (Scotland) Act 2002
- Human Rights Act 1998
- Adults with Incapacity (Scotland) Act 2000
- Public Records (Scotland) Act 2011
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- Disposal of Records (Scotland) Regulations 1992
- The Regulation of Investigatory Powers (Scotland) Act 2000
- NHS HDL (2003) 30, Regulation of Investigatory Powers (Scotland) Act
- Patient Rights (Scotland) Act 2011
- Computer Misuse Act 1990
- Access to Medical Reports Act 1988
- Access to Health Records Act 1990
- CEL 13 2008 Information sharing between NHS Scotland and the Police

- CEL 25 (2011) NHS Scotland: Safeguarding the Confidentiality of Personal Data processed by Third Party Contractors.
- CEL 25 (2012) NHS Scotland: Mobile Data Protection Standard
- Scottish Government Records Management: Health and Social Care Code of Practice (Scotland) 2020
- The Nursing and Midwifery Council - The Code
- National Guidance for Child Protection in Scotland (2021)
- Adult Support and Protection (Scotland) Act 2007

Appendix 1 – The Principles

Data Protection Legislation Principles

Personal Data Shall be:

a. Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
b. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with UK GDPR Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
c. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
d. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
e. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed purely solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with UK GDPR Article 89(1) subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of the data subject ('storage limitation');
f. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

The Controller shall be responsible for, and able to demonstrate compliance with, the above principles ('accountability').

Caldicott – The Principles

1. Justify the purpose(s) for using confidential information
2. Only use it when absolutely necessary
3. Use the minimum that is required
4. Access should be on a strict need-to-know basis
5. Everyone must understand his or her responsibilities
6. Understand and comply with the law
7. Duty to share is as important as duty of confidentiality
8. Inform patients and service users about how their confidential information is used