NHS Confederation

The NHS Confederation

Charity number 1090329

Company number 04358614

Data Protection Policy

Date policy agreed by Board of Trustees	March 2019, updated March 2022
Date of policy review	March 2025
Owner of policy	Director of People and Governance

Contents

Introduction

Purpose of this policy

As a Data Controller the NHS Confederation takes its responsibilities regarding the management of the requirements of data protection legislation, very seriously. 'Data protection legislation' includes the Data Protection Act 2018 and the UK General Data Protection Regulations (GDPR), as modified, or replaced from time to time, and any other related legislation (such as the Privacy & Electronic Communications (EC Directive) Regulation 2003).

This policy sets out how the NHS Confederation manages those responsibilities and aims to place data protection at the heart of the NHS Confederation's operations to protect and promote the rights of individuals and protect the charity from the risk of data breaches.

Scope

This policy applies to everyone working at or with the NHS Confederation[1]. It applies to:

- all staff, including chief executives, directors, senior managers, employees (whether permanent, fixed term or temporary), seconded staff, homeworkers, agency workers and volunteers
- consultants and contractors
- trustees and committee members.

Any employing or contracting manager must ensure that all temporary staff, consultants, or contractors are aware of this policy.

By the NHS Confederation we mean the NHS Confederation charity, any subsidiary companies, and any hosted networked organisation.

This policy applies to all personal data the NHS Confederation collects, stores and processes, regardless of the location of where the data is stored (e.g. on an employee's own device) and regardless of the data subject. The main personal information held is in relation to representatives at member organisations, employees, board and committee members, volunteers, employment applicants and other stakeholders. Personal data refers to any identifiable data relating to an individual. It doesn't need to be data that is considered private and can relate to an individual's 'work details'

[1] Collectively referred to as workers in this policy

The NHS Confederation has designated the **Director of People and Governance** as the individual who is responsible for ensuring that the NHS Confederation implements this policy.

This policy should be read in conjunction with the organisation's IT Security Policy, Privacy Statement and Procedures for Data Breaches and Subject Access Requests. The Policy should also be read in conjunction with the Information Commissioner's Office guidance on data protection legislation.

Policy Statement

The NHS Confederation is committed to being fully compliant with all applicable data protection legislation and to following good practice in respect of all the personal data it holds, both in electronic form and on paper.

Commitments

The NHS Confederation will always comply with the data protection principles and other obligations in the data protection legislation, including:

- Obtaining and using personal information only on a sound lawful basis and for a clearly defined purpose or purposes (first and second principles).
- Informing individuals of how their personal data is or will be used and providing clear and appropriate privacy notices (first principle).
- Ensuring that the right information is held, enough but not too much (third principle).
- Ensuring that as far as possible the information is accurate and up to date (fourth principle).
- Holding personal data no longer than necessary (fifth principle).
- Recognising the rights individuals have over their data, informing them of their rights, and responding appropriately to the exercise of these rights.
- Ensuring that all personal data is held securely, and access is properly authorised (sixth principle).
- Understanding the restrictions on transferring data outside the UK and legal requirements with regards sharing data with other organisations.

Accountability

We demonstrate our accountability for complying with the data protection principles by:

- Designating a data protection lead; and establishing a cross-organisation IT, Data Governance and Security Staff Group

- Designating the Audit and Risk Committee to hold the executive accountable for data protection.
- Adopting a Privacy by Design approach when processing personal data and completing Data Protection Impact Assessments (DPIA) for all new projects or partnerships that require the use of personal data, where an existing is significantly modified or whenever special category data is being processed.
- Conducting and retaining Legitimate Interest Assessments or retaining evidence that consent has been obtained, where either of these are the basis for processing;
- Retaining an Information Asset Register, a register of Data Breaches and Subject Access Requests and details of appropriate responses. In the case of Data Breaches, we will retain a record of whether they reached the threshold for reporting to the Information Commissioner's Office and any subsequent change in practice.
- Ensuring appropriate and robust Data Sharing Agreements or Data Processing Agreements are in place for when we work with other organisations on personal data.
- Integrating data protection into our policies and procedures, such as privacy notices and designs of our databases.
- Training staff on compliance with Data Protection Law and keeping a record accordingly; and
- Regularly testing the privacy and security measures implemented and conducting periodic reviews, including by our internal audit function, to assess compliance and identify areas for improvement.

Guidance notes

Rights of data subjects and Subject Access Requests

Data Protection legislation provides individuals (known as data subjects) with rights in relation to the way we handle their personal data. The NHS Confederation will respond promptly and appropriately to any request from a data subject to exercise their rights under legislation.

All data subjects are entitled to make a Subject Access Request to ask the NHS Confederation whether it holds any personal data relating to them and, if so, to be given a description of and a copy of that personal data. Exemptions may apply in certain circumstances.

Responses to Subject Access Requests are co-ordinated by the organisational data protection lead and in accordance with the Subject Access Request Procedure. Any requests received should be forwarded to dataprotection@nhsconfed.org for processing and should not be responded to directly.

Assessments

NHS Confederation staff will conduct a Data Protection Impact Assessment in the following situations:

- Whenever it is proposed to enter into a data sharing agreement with a new partner, or to make modifications to an existing data sharing agreement.
- Whenever a new project or activity is established that involves the processing of special category and/or criminal record personal data, or where other risks can be identified.
- Whenever an existing process involving the use of personal data is significantly modified (and where it is proposed to start processing special category and/or criminal record data).
- Whenever it is proposed to share special category and/or criminal record data outside an existing data sharing agreement unless the disclosure is an isolated case and made to an appropriate authority.

The NHS Confederation will always work towards processing data with Active Consent being the main legal basis. However, the NHS Confederation may carry out a Legitimate Interests Assessment where it is felt that it is in the interest of the individual to have their data processed in a substantially different way for which consent was secured. In such circumstances, the Legitimate Interest Assessment must be approved by the Head of Governance and Compliance.

In addition, an appropriate assessment may be carried out whenever an incident occurs that suggests that a risk has not previously been sufficiently evaluated.

Data Security

The NHS Confederation will ensure there are sufficient systems and controls in place to maintain the security and integrity of the data held. All users of IT systems and those who handle personal data are required to follow the protocols and guidance set out in in the IT Security Policy.

Relevant IT systems are regularly reviewed to ensure that they incorporate up to date security measures.

Bearing in mind that many security breaches are the result of human error rather than systems failure, all those who handle personal data on the NHS Confederation's behalf receive specific training and reminders on appropriate precautions.

Access to personal data

Employees and data processors contracted by the NHS Confederation will only have access to personal data where it is required as part of their functional remit or to be able to deliver the piece of work contracted. All those who handle personal data are required to:

- acquaint themselves with the purpose(s) for which it was obtained and to use it only for those and compatible purposes.
- ensure that data subjects are provided with appropriate privacy notices and appropriate consents have been secured.

- keep the personal data secure and current, following current NHS Confederation policies and procedures.
- securely destroy the data once its retention period expires.
- consult their manager, and/or the data protection lead if in any doubt about how personal data may be processed.
- keep records, as required, to demonstrate the NHS Confederation's accountability for its data protection obligations.

Data Sharing

The NHS Confederation may share personal data with other organisations only in one of the following circumstances:

- Under the terms of a funding agreement that explicitly requires the sharing of personal data and the arrangements around data sharing have been clearly expressed.
- Under the terms of a joint data controller agreement.
- Under the terms of a data sharing agreement.
- Under the terms of a data processor contract.
- With the explicit consent of the data subject.
- In exceptional circumstances on the authority of the data protection lead, who shall determine the basis on which the sharing may legitimately take place.

Any Agreement or contract for data processing should explicitly outline roles and responsibilities with regards to data and compliance with data protection legislation. Any third party that has entered an agreement with the NHS Confederation shall be expected to read, understand, and comply with this policy.

Transfers abroad

The NHS Confederation avoids transferring personal data outside the UK as far as reasonably possible. Whenever a service is employed that involves processing personal data outside the UK, the data is kept within jurisdictions that have been assessed as 'adequate' where possible.

Any other transfer of personal data outside the UK must be approved in advance by the data protection lead, who will ensure that the transfer is compliant with the UK GDPR and any restrictions imposed by funding or other agreements.

Data Retention Schedules

Personal Data must not be held for longer than necessary and it must be destroyed securely. Personal Data should be reviewed periodically to check it is accurate and up to date and to determine whether retention is still necessary. Appropriate measures must always be taken to ensure that the Personal Data that has been earmarked for destruction cannot be reconstructed and processed by third parties.

The NHS Confederation's **Data Retention Schedule** sets out the periods for which different sets of records held by the Confed will be retained.

Data Breaches

In the event of a data breach, potential data breach or ‘near miss’, the data protection lead will:

- Investigate the nature and extent of the incident.
- Ensure immediate steps are taken to prevent any further harm.
- Report the incident to the Information Commissioner if it reaches the required threshold.
- Alert Group Executive and assess whether the incident reaches the required threshold for a Serious Incident Report to the Charity Commission.
- Inform any individuals who may be seriously adversely affected where necessary.
- Recommend proportionate changes to systems and procedures to minimise the risk of a similar breach recurring.
- Report the data breach and lessons learnt to the Finance and Operations Committee.

All those who handle personal data on the NHS Confederation’s behalf are placed under an obligation to report any data breach, potential data breach or ‘near miss to the data protection lead immediately they become aware of it. Prompt reporting is regarded as a strong mitigating factor if a breach is reported by the organisation responsible for its occurrence.

The **Data Breach Procedure** sets out the steps to be followed to notify that a breach has taken place and the actions that will be taken in response.

Training

The NHS Confederation ensures that all its employees [and volunteers] are aware of policies and procedures and understand their personal responsibility to follow these to protect personal data appropriately.

The NHS Confederation will provide appropriate and relevant training to all its staff [and volunteers]. Data protection will be covered in the induction process and the data protection lead will ensure that general training is provided at least once every two years or when there are significant changes to data protection legislation or the NHS Confederation’s policies or procedures.

Managers are responsible for identifying specific training needs within their teams and should ensure that data protection considerations are included in informal training, such as during team meetings.

The data protection lead will ensure that staff with specific data protection responsibilities have access to information on developments in this area (such as through briefings from the Information Commissioner’s Office and specialists in this area) and individual training if required. The data protection lead will ensure appropriate procedures, guidance and templates are available to staff to ensure compliance with data protection obligations.

The NHS Confederation will keep records of attendance at all data-protection-related training.

Responsibilities

The NHS Confederation is committed to protecting the rights and confidentiality of those whose personal data it holds. Every worker is bound by a legal common law duty of confidentiality and has an obligation to protect the personal data that they may encounter during their work.

Workers who are NHS Confederation employees are also bound by the confidentiality and data protection clauses in their employment contract.

The Board of Trustees: As the Data Controller the charity's board of trustees is responsible for ensuring appropriate policies and procedures are in place to comply with data protection law.

The NHS Confederation **Chief Executive** is responsible for implementing the appropriate policies and procedures and ensuring they are communicated to staff through training and information sharing

The **Group Executive** are responsible for communicating the importance of adhering to the Data Protection Policy and for ensuring that good data protection practices are embedded in the organisation's operational activities

The **Director of People and Governance** is the nominated Senior Information Risk Owner responsible for taking the lead on risk management and information security and assist the Group Executive in the delivery of their responsibilities. They also oversee the data breach reporting and investigation procedures in place.

The Organisational **Data Protection Lead** is the **Head of Governance and Compliance** who is responsible for ensuring day to day compliance with data protection requirements by maintaining policies and procedures, advising staff, delivering training, and ensuring appropriate agreements are in place with data processors alongside contracts.

Employees are responsible for ensuring they comply with the requirements of this policy and all related policies, and to report any data breach incidents to the Data Protection Lead as soon as identified, in line with the Data Breach Procedure.

Any unlawful obtaining or disclosure of personal data (including the transfer of personal data outside the EEA) or any other breach of the Data Protection Legislation will be treated seriously and may lead to disciplinary action under the NHS Confederation's Disciplinary Policy.

Annex 1 Definitions

Data controller	The Organisation who determines the purpose and means of collecting, processing, and storing your data and who you would approach with your Subject Access Request.
Data Protection Impact Assessment	A process to help identify and minimise the data protection risks of a project.
Data Processor	The organisation or individual who is responsible for processing personal data on behalf of a controller.
Data Processing Agreement	A formal agreement if an organising is being contracted to process the information on behalf of anther organisation. It sets out roles and responsibilities as well as obligations to data protection legislation.
Data Sharing Agreement	A formal agreement between more than one organisation (controllers) if data is being shared. It sets out roles and responsibilities as well as obligations to data protection legislation
Data subject	The identified or identifiable living individual to whom personal data relates.
Information Asset Register	An organisation's register or log of all systems and places where personal data might be stored or processed.
Joint controller	Where there is more than one organisation involved in determining the means of collecting, processing, and storing your data.
Lead controller	Where there is more than one organisation involved in the data controlling, normally there would be an agreement on who would take on the Lead role in responding to Subject Access Requests. They are given the name of Lead Controller
Legitimate Interest Assessment	Used by an organisation to assess whether it can process data in a different way to which consent was sought to identify if data subjects would have legitimate interest in their data being processed in a new way.

Personal data	means information relating to identifiable individuals such as employees, contractors, former employees, job applicants, members, contract and other staff, suppliers, and marketing contacts. This includes expression of opinion about the individual and any indication of someone else's intentions towards the individual. Personal data includes ‘sensitive personal data’.
Sensitive personal data	means personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings.
Subject Access Request	A request by which an individual can make to an organisation to see what personal information is retained by them