Data Protection policy
CG14

Beware when using a printed version of this document. It may have been subsequently amended. Please check online for the latest version.

Applies to:	All NHS Resolution employees, Non-Executive Directors, secondees and consultants, and/or any other parties who will carry out duties on behalf of NHS Resolution. Contractors and panel firms are required to adhere to the terms of their contractual agreements.
Version:	Version 3.0 CG14 - Data Protection Policy
Review date:	September 2023
ORG review	August 2020
IG Group review	August 2020
SMT review	September 2020
Board review	September 2020
Author:	Tinku Mitra
Owner:	Joanne Evans

NHS Resolution

Contents

1. Introduction

The business of NHS Resolution involves the processing of information about individuals ("**personal data**"). Often, due to the nature of the work of the organisation, this information will include details many people would consider to be sensitive and/or private (for example, details about physical or mental health, performance at work, and financial affairs). In order to protect the rights and freedoms of individuals, to retain the trust of those with whom we are dealing and that of the wider public and to minimise the risk of there being a successful legal challenge or regulatory action in relation to the way(s) in which the organisation processes personal data it is essential we act in accordance with the law in this area. We also aim to follow 'best practice' recommendations where this is feasible.

2. Purpose

The purpose of this policy is to set out, in broad terms, the requirements with which we need to comply in processing personal data, and how we go about complying with them. Further information about how we implement this policy is within our guidance note appended.

3. Equality impact assessment

As part of its development, this policy has had an equality impact assessment. No detriment was identified.

4. Duties

- **Chief Executive and Accounting Officer:** Accountable for all information governance matters including compliance with the requirements of data protection law.

- **Audit and Risk Committee:** Has responsibility for the strategic processes for risk identification, control and governance.

- **Senior Information Risk Owner (SIRO):** The SIRO has overall responsibility for leading and fostering a culture that values, protects and uses information for the success of the organisation and benefit of its customers. They own the organisation's overall information risk policy and risk assessment processes, information incident management framework, and ensure they are implemented consistently by Information Asset Owners. It is their job to advise the Chief Executive on the information risk aspects of their statement on internal controls. The Director of Finance and Corporate Planning fulfils this role for NHS Resolution.

- **Caldicott Guardian:** The Caldicott Guardian is an advisory role held by a senior health professional who is responsible for ensuring patient data is kept secure, oversight of all procedures affecting access to person-identifiable health data and to advising on appropriate sharing of patient data. The Director of Safety and Learning fulfils this role for NHS Resolution.

- **Data Protection Officer:** The Data Protection Officer's (DPO) task is to inform, advise and train NHS Resolution and its staff on its obligations in relation to the processing of personal data; monitor NHS Resolution's compliance with these obligations; promote good data protection practice; advise on data protection impact assessments; and be the principal point of contact on behalf of NHS Resolution for the regulator, the Information Commissioner. The Deputy Director of Corporate and Information Governance fulfils this role for NHS Resolution.

- **Information Governance Group:** Has operational oversight of all data protection and confidentiality issues delegated to it by the Accounting Officer.

- **Head of IT & Facilities:** As the Information Security Officer, the Head of IT & Facilities has overall responsibility for the provision of systems and facilities to support accurate, legally compliant, secure and efficient information governance.

- **Information Security and Governance Manager:** The Information Governance Manager is responsible for the day-to-day oversight of data protection issues and for ensuring that data are handled in accordance with NHS Resolution policy and legal requirements.

- **Information Access Manager and Information Access Officer:** Has responsibility for dealing with Subject Access Requests under the General Data Protection Regulation (GDPR) and for ensuring sufficient fair processing information is available to users of NHS Resolution services.

- **Line managers:** All line managers are responsible for the promotion of the principles of the GDPR outlined within this policy and associated policies, within their teams.

- **Employees:** All employees and secondees who are carrying out duties on behalf of NHS Resolution are responsible for adherence to the principles of the GDPR outlined within this policy and implemented in associated guidance and for reporting any related adverse incidents in line with CG11 – Incident Reporting Policy and Procedure.

5. The General Data Protection Regulation (GDPR)

Definitions – for the purposes of the GDPR:

- **Personal data:** Data relating to a living individual who can be identified from the data, directly or indirectly.

  The data may 'relate to' the identifiable living individual, whether in personal or family life, business or profession.

- **Special categories of personal data:** Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union memberships, and genetic data, biometric data when used to identify a person, data concerning health or a data subject's sex life or sexual orientation.

- **Processing:** Processing, in relation to information or data, means operations 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.

- **Data subject:** Data subject means "an individual who is the subject of personal data". A data subject must be a living individual. A data subject need not be a United Kingdom national or resident. Generally, in the exercise of its functions, individuals we interact with (for instance, our employees, clinicians working with the Practitioner Performance Advice service, or those bringing claims against the NHS) are 'data subjects'.

  Please note that whilst the GDPR does not apply to information relating to the deceased, confidentiality obligations continue to apply to such data. This is supported within the DHSC Confidentiality Code of Practice and should be followed by all NHS Resolution staff.

- **Data controller:** Data controller means a person or organisation (including a public authority "which, alone or jointly with others, determines the purposes and means of the processing of personal data"

  A data controller decides how and for what purpose personal data is to be used. Generally, in the exercise of its functions, NHS Resolution acts as a 'data controller'.

- **Data processor:** Data processor, in relation to personal data, means any person or organisation which processes the data on behalf of the data controller.

  A data processor will undertake tasks in accordance with a data controller's instructions. They must not use the data for any other purpose.

6. Principles relating to the processing of personal data

The GDPR requires that personal data shall be:

A. Processed lawfully, fairly and in a transparent manner:

NHS Resolution has set out why we process personal data in our Privacy Notice which is set out on NHS Resolution's website at https://resolution.nhs.uk/how-we-use-your-data/ . For the purposes of notification to the Information Commissioner, the Data Controller remains NHS Litigation Authority as the legal entity.

Collected for specified, explicit and legitimate purposes and not further processed in any manner incompatible with those purposes:

To comply with this principle, NHS Resolution must maintain a record of how it uses personal data and ensure this is reflected in its Privacy Notice. If a new use of personal data is proposed that is not already covered by this, steps must be taken to ensure appropriate notice is given.

B. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation):

We put in place a number of measures to achieve this, including:

1) We limit access within our systems to stop data being used for irrelevant purposes;

2) We have data retention policies which help us to ensure that unnecessary data is not kept;

3) We design our processes, forms, and systems so as not to capture extraneous data;

4) We are subject to Court rules and other legal requirements that help to ensure that our data is adequate for our tasks.

It is the responsibility of all NHS Resolution employees to ensure that personal data processing is adequate and limited to what is proportionate to achieve NHS Resolution's public task.

C. Accurate and, where necessary, up to date; and inaccurate personal data are erased and rectified without delay:

Where NHS Resolution employees obtain information either directly from the data subject or via a third party, they must ensure the accuracy of the data held. We ordinarily test new systems before rolling them out more widely in order to establish that they maintain data accuracy. If the data subject informs NHS Resolution of a (factual) inaccuracy, the data must be amended to reflect this. If, as will often be the case in litigation cases there is a dispute as to accounts, this means that NHS Resolution should ensure all competing versions are recorded accurately.

D. Not kept for longer than is necessary for the purposes for which the personal data are processed

NHS Resolution should not retain information for longer than is required to fulfil the purposes for which it is collected, as per **CG16 - Records Management Policy.**

E. Secure:

NHS Resolution will maintain technical and organisational measures to prevent or manage foreseeable incidents and identified risks which may affect the secure processing of personal data. All employees will be kept aware of security issues associated with the processing of data, through training and other measures.

Data protection and confidentiality clauses must be formally defined and included within third party contracts, and appropriate due diligence as to their security arrangements is performed.

When considering appropriate security, NHS Resolution must consider whether the following steps are appropriate:

- Pseudonymisation ' a technique that replaces or removes information in a data set that identifies an individual and encryption
- The ability to secure the confidentiality of data and the stability of the storage platforms ensuring business continuity access to data in the evident of physical or technical incidents.
- Regular testing and evaluating the effectiveness of security measures

If there is a data security breach, data controllers are ordinarily required to report the breach to the Information Commissioner within 72 hours, unless the breach is unlikely to result in risk to the rights and freedoms of the data subject. Any incidents which might meet the threshold for reporting must be reported to the DPO

It is therefore important any suspected data security breach is reported to the DPO as soon as possible. NHS Resolution will then assess whether the breach is reportable under the NHS Digital Guide to the Notification of Data Security and Protection Incidents utilizing the NHS Data Security and Protection Toolkit.

If a data breach is likely to create a high risk to the risks and freedoms of the data subject there is an obligation to notify the affected data subjects directly. Again, the assessment of whether this is required will be undertaken by the DPO.

7. Conditions for processing personal data

When NHS Resolution is processing personal data, it is obliged to ensure that the processing meets at least one of the permitted conditions under Article 6. The precise condition to be met will depend upon the particular activity being undertaken by NHS Resolution. The Article 6 conditions are:

a. The data subject has given their consent to the processing for one or more specific purposes.

b. The processing is necessary for the performance of a contract to which the data subject is party, or for the taking of steps at the request of the data subject with a view to entering a contract.

c. The processing is necessary to comply with legal obligation.

d. The processing is necessary to protect the vital interests of the data subject or another.

e. The processing is necessary for the performance of a public task or in the exercise of official authority

f. The processing is necessary for the legitimate interests of the data controller (except where unwarranted because of prejudice or legitimate interests of data subject). (As a public authority, NHS Resolution cannot rely on this condition for processing in connection with its public task.)

In most circumstances, NHS Resolution's processing of personal data will be in reliance on conditions (c) and (e).

When NHS Resolution is processing special category personal data, it must also ensure that one of the conditions in Article 9 GDPR are met. Those most relevant to NHS Resolution's activities are:

- The data subject has provided explicit consent
- Processing is necessary for legal obligations in relation to employment of social security law
- Processing is necessary for the establishment, exercise or defence of legal claims or wherever courts are acting in their judicial capacity
- Processing is for reasons of substantial public interest as provided for in Schedule 1 to the Data Protection Act 2018
- Processing is necessary for the provision of health or social care or treatment or the management of health or social care systems, and the information is subject to a binding obligation of confidentiality
- Processing is necessary for ensuring high standards of quality and safety of health care, and the information is subject to a binding obligation of confidentiality.

Where personal data relates to alleged or actual criminal activity on the part of the data subject, it is necessary to meet one of the conditions in Schedule 1 to the Data Protection Act 2018, such as processing necessary for the prevention or detection of crime, where the processing must necessarily take place without the consent of the data subject and is necessary for reasons of substantial public interest.

8. Data Protection Impact Assessments

Where NHS Resolution is considering a new project or service change initiative which will include the processing of personal data consideration must be given by the project leadership team throughout the project development process to whether a Data Protection Impact Assessment (DPIA) needs to be completed. DPIAs are a legal requirement for processing that is likely to be high risk and we will conduct screening exercises for projects to establish the degree of likely risk associated with the project. A DPIA is a systematic process which will help

identify and minimise data protection risks. Our DPIAs will take account of compliance risks, and also broader risks to individuals' rights and freedoms including the potential for any significant social or economic disadvantage and the prospects of physical, material or non-material harms. Advice on DPIAs may be obtained from the DPO but it is the responsibility of the project team to complete the DPIA. Records of DPIAs shall be kept by the Information and Security Governance Manager

9. Individuals' rights

NHS Resolution must ensure personal data is also processed in accordance with the rights of data subjects. As well as the entitlement to be informed about NHS Resolution's use of personal data via its Privacy Notices, individual data subjects have rights including the following:

9.1. right to access their own personal data;

9.2. right to rectification of inaccurate data;

9.3. right to erasure in certain circumstances (the right to be forgotten)

9.4. right to restrict processing in certain circumstances

9.5. right to have data transferred to another data controller in certain circumstances (data portability)

9.6. right to object to processing;

9.7. right to prevent processing for the purposes of direct marketing;

9.8. rights in relation to automated decision taking;

9.9. right to complain to the Information Commissioner; and

9.10. right to take action for compensation if the individual suffers damage by any contravention of the Act by the data controller.

10. Subject access and other information rights requests.

Individuals have a right under the GDPR to make a request in writing for a copy of the information held about them. This is called a subject access request. Subjects are also entitled to be given a description of the information, what it is used for, who it might be passed on to, and any other information held. Individuals have other rights under data protection law (for instance to ask for inaccurate data to be corrected or to object to our use of their data).

Any such request for information should be construed a subject access request unless part of the normal course of business. Such requests should be passed to the Information Access Manager. Requests should ordinarily be dealt with within the legal timescale of one calendar month.

We will take reasonable care to ensure information can be requested or is made available in an appropriate format for individuals with disabilities.

For further detail please see Guidance Note on handling Subject Access Request or contact the Information Access Manager.

Many of these rights are modified or restricted in certain circumstances in accordance with the Data Protection Act 2018, in particular, none of the GDPR obligations undermine the protection of data subject to legal professional privilege. Any request to exercise a data subject right should be passed promptly to Information Access Manager or the Data Protection Officer as appropriate.

11. Data exports

Data exports outside the European Economic Area are prohibited, unless there are appropriate recognised protections for the rights and freedoms of data subjects, or there is a permitted exemption to this prohibition.

A transfer can take place if any of the following conditions are met:

- The recipient country is approved by the European Commission as providing appropriate safeguards to data subjects;
- The transfer is to the United States and is under the EU/US Privacy Shield Scheme;
- The data transfer is governed by a binding contract, incorporating model contract clauses approved by the European Commission;
- The transfer is subject to binding corporate rules, approved by the European Commission.

There are other situations where transfers are permitted despite the absence of these recognised safeguards, including:

- The data subject grants explicit, informed permission;
- The transfer is necessary for the establishment, exercise or defence of legal claims.

In the event of data falling into this category, the DPO should be contacted before any data is sent.

12. The Data Protection Act 2018

This compliments the GDPR, by addressing those matters left to national governments under the GDPR and provides additional lawful bases for processing data, and also details the various exemptions to the principles of the GDPR (these largely mirror the exemptions previously available under the DPA 1998).

It also provides the framework for data processing by law enforcement organisations, whose activities fall outside the scope of the GDPR.

It also provides the mechanism by which the GDPR will become UK law on the UK's exit from the EU.

13. The Duty of Confidentiality

NHS Resolution will receive a significant amount of highly sensitive and confidential information as part of its public task. This information given to NHS Resolution in confidence must not be disclosed without consent unless there is a lawful basis for doing so e.g. disclosure to a legal advisor or in connection with litigation, a requirement of law or there is an overriding public interest to do so. Such confidential information is subject to a duty of confidence and, if it is disclosed unlawfully, legal action can be taken against NHS Resolution for breach of confidence. Confidential information will include but is not limited to medical information, personnel information, and commercially sensitive information relating to the business of the organisation.

NHS Resolution has a duty both under the common law and under the Human Rights Act 1998 to ensure that the confidential information it holds is not inappropriately disclosed.

See Confidentiality: NHS Code of Practice for further information.

14. The Regulatory Environment

The Information Commissioner's office (ICO) is the UK's independent public authority set up to uphold information rights. They do this by promoting good practice, ruling on complaints, providing information to individuals and organisations and taking appropriate action when the law is broken.

The ICO enforces and oversees the following legislation:

- GDPR
- Data Protection Act 2018
- Freedom of Information Act 2000
- Privacy and Electronic Communications Regulations 2003
- Environmental Information Regulations 2004

The Information Commissioner's Office (ICO) has extensive statutory powers to investigate an organisation's compliance with the data protection legislation, including compulsory audit powers, and also issues extensive guidance on how the obligations under the GDPR should be met.

Should an individual feel their rights under the data protection legislation have been infringed, they can complain to the ICO, who will investigate and determine whether there has been a breach of the data subject's rights. If there has, the ICO may require further action.

The ICO can also issue monetary penalties in the event of a serious breach of the GDPR - with the upper level of monetary penalty being €20,000,000 or 4% of global annual turnover, whichever is the higher.

The ICO also prosecutes data protection offences, such as the unlawful obtaining or disclosing of personal data, or the unlawful re-identification of de-identified data

There are a number of tools available to the ICO for taking action to change the behaviour of organisations and individuals that collect, use and keep personal data. They include criminal prosecution, non-criminal enforcement and audit.

15. Training and support

NHS Resolution will provide appropriate training to all staff on information governance including data protection.

Managers and other staff may request advice from the Corporate Governance Team should they require support with the implementation of this policy.

This policy should also be read in conjunction with the following policies

16. Monitoring effective implementation

The effective implementation of this policy will be monitored by NHS Resolution's Information Governance Group including review of related incidents reported and associated actions taken and by NHS Resolution Board through review of incidents and risks arising.

17. Other relevant documents

This policy should also be read in conjunction with the following policies

CG02 Information Governance Strategy
CG12 Complaints Policy and Procedure
CG11 Incident Reporting Policy and Procedure
CG15 Freedom of Information Policy and guidance document
CG16 Records Management Policy
ITFA02 Guidance for Working with Confidential or Sensitive Information
ITFA05 Information Security Policy
ITFA21Guidance for using Encrypted USB devices and Email Attachments

Document control

Date	Author	Version	Reason for change
10/10/14	Joel Henderson	V1_0 draft	Initial draft
23/11/14	Joel Henderson	V2_0 draft	Input from ISO Expert
24/01/14	Joel Henderson	V3_0 draft	Comments from IG Group
	Joel Henderson	V4_0 draft	Additional comments from IG Group
13/02/14	Joel Henderson	V5_0 draft	Amendments made to ensure consistency with other policies.
20/02/15	Joel Henderson	V6_0 draft	Amended in line with information handling guidelines.
24/02/15	Joel Henderson	V7_0 draft	Subject access amendments
26/02/15	Joel Henderson	V8_0 draft	Minor format amendments
25/03/15	SMT approved	V9 final	SMT approved
06/03/17	Joel Henderson	V10 draft	Review date
14/03/17	Joel Henderson	V11 draft	SIRO and CG roles updated, approved
05/04/17	Joel Henderson	V12 final	Formatting to reflect name change
04/04/18	Evelyn Lucien	V13 Final	Change to reflect policy number changes
08/08/18	Julian Marku	V14 Final	Changes confined to reflect new legislation and amendment to include date.
1/10/18	Julian Marku	V15	Substantive review by legal advisers
31/10/18	Julian Marku	V15	SMT review
2020			
13/08/20	Tinku Mitra	V1.0	2020 Review
20/08/20	Tinku Mitra	V2.0	ORG review
26/08/20	Tinku Mitra	V3.0	IG group review
02/09/20	SMT	V3.0	SMT review