Data Protection Policy

Produced by the Business Support Unit
Regulation and Quality Improvement Authority

Title:	RQIA Data Protection Policy		
Author(s):	Head of Business Support Unit, RQIA DPO, BSO		
Ownership:	Head of Business Support Unit, RQIA		
Approval By:	Executive Management Team	Approval Date:	4 January 2022
Operational Date:	1 March 2022	Next Review:	January 2025
Version No.	3.0	Supersedes:	2.0
Key Words:	Data Protection, Confidentiality, Responsibility		
Director Responsible:	Head of Business Support Unit, RQIA		
Lead Author Position:	Head of Business Support Unit, RQIA		
Additional Author(s):	Data Protection Officer (DPO), Business Services Organisation (BSO)		
Department:	Business Support Unit		
Links to other Policies:	Information Governance Policy		
	Records Management Policy		
	Freedom of Information Policy		

Contents

1. Introduction

1.1 The Regulation and Quality Improvement Authority (RQIA) needs to collect personal data about people with whom it deals with in order to carry out its business and provide its services. Such people include employees (present, past and prospective), patients, service users, providers, suppliers and other business contacts. In addition, we may be required by law to process and share personal information with other organisations (including, but not limited to, police, regulatory and health and social care bodies).

1.2 As a public body, RQIA has a statutory duty to safeguard the information it holds, from whatever source, which is not in the public domain. The lawful and proper treatment of personal information by RQIA is extremely important to the success of our business and in order to maintain the confidence of our service users and employees.

1.3 RQIA, its staff and others who process personal information on its behalf must ensure that they follow the principles set out within Article 5 of the UK General Data Protection Regulation (UK GDPR).

1.4 This policy has been written to support staff in compliance with legal requirements and best practice guidance, which is referenced within the Information Governance Assurance Framework.

2. Purpose

2.1 The purpose of this policy is to lay down the principles that must be observed by anyone who works for, or on behalf of, RQIA and has access to personal information.

2.2 This policy aims to clarify how and when personal information may be shared, and the need to make individuals aware of the ways in which their information might be used.

3. Scope

3.1 The scope of this policy is to support the protection, control and management of personal information. The policy will cover all information within RQIA and is concerned with all information systems, electronic and non-electronic information. It applies to all directorates, services and departments, all permanent and temporary staff, all agency workers, and as appropriate to contractors and third party service providers acting on behalf of RQIA.

4. Objectives

4.1 **Privacy by design:** RQIA will apply 'privacy by design' when developing and managing information systems containing personal information by:

- Using data protection impact assessments (DPIAs)[1] where appropriate to identify and mitigate data protection risks at an early stage;
- Processing only the minimum personal information for the minimum time necessary for the purpose(s) that it is being processed; and
- Anonymising personal information wherever necessary, for instance when using it for statistical purposes.

[1] Under Article 35 of the UK GDPR, data controllers will be legally required to undertake DPIAs prior to data processing which is *"likely to result in a high risk to the rights and freedoms of natural persons*".. A regional template has been developed, which provides more detailed information on when, and how, to complete a DPIA

4.2 Fair and Lawful Processing: RQIA will:

- Only collect and use personal information to the extent that it is needed to fulfil operational or legal requirements, and in accordance with the conditions set down under the UK GDPR;
- Provide transparent information on how personal information will be processed by way of 'fair processing notice', which will detail:
  - What information is needed
  - Why this information is needed
  - The purpose(s) that this information will be used for
  - How long this information will be kept for; and
- Ensure the quality of personal information processed.

4.3 Disclosure of Personal Information: RQIA will not disclose personal data to any third party unless it is lawful to do so.

4.4 Safeguarding Information: RQIA will

- ensure appropriate technical and organisational security measures are in place to safeguard personal information so as to prevent loss, destruction or unauthorised disclosure;
- ensure there are mechanisms in place to report breaches of the processing of personal data[2]; and
- manage and investigate all reported breaches appropriately.

4.5 Retention and Disposal: Personal information will be disposed of by means that protect the rights of those individuals, and as such RQIA will:

- Apply retention policies to all personal information;
- Destroy information no longer required in a secure manner; or
- Transfer the information, by arrangement, to the Public Records Office of Northern Ireland (PRONI) where deemed appropriate.

4.6 Uphold Individual's Rights: RQIA will ensure that the rights of the individual under Chapter 3 of the UK GDPR are upheld, where applicable, namely:

- The right to be informed;
- The right of access[3];
- The right to rectification;
- The right to erasure;
- The right to restrict processing;
- The right to data portability;
- The right to object; and
- The rights in relation to automated decision making and profiling.

5. Responsibilities

5.1 Responsibilities are as set out within RQIA's Information Governance Assurance Framework, which is available on request.

[2] All breaches of personal data must be reported directly to RQIA's Senior Information Risk Owner (SIRO) and the DPO at BSO, where appropriate. A form is available on RQIA's Intranet.

[3] It is RQIA's policy to provide the final version of any letters or other documents which contain personal information. This is because the final version is the correct version of the personal information held. Drafts may contain incorrect information which was subsequently corrected prior to the letter or document being sent. It is therefore RQIA's position not to provide draft documentation unless a final version was not sent.

6. Performance and Monitoring Compliance

6.1 The effectiveness of this policy will be assessed on a number of factors:

- Nomination of an individual or individual with specific responsibility for data protection within RQIA;
- compliance with the requirement of the UK GDPR;
- the management of data breaches, including near misses;
- the retention and disposal of records in accordance with GMGR; and
- completion of a satisfactory Information Management Assurance Checklist to the Department of Health.

7. Non-Compliance

7.1 A failure to adhere to the relevant legislation[4], this policy and any associated procedures, may result in disciplinary action. In relation to the use of ICT equipment, including the use of the internet and email, staff should be aware that they may be personally liable to prosecution and open to claims for damages if their actions are found to be in breach of the law.

7.2 Serious breaches may be reported to the PSNI, ICO or other public authority for further investigation.

8. Review

8.1 This policy and any associated procedures will be reviewed no later than 2 years from approval, to ensure their continued relevance to the effective management of information governance within RQIA.

9. Equality Statement

9.1 This policy has been screened for equality implications as required by Section 75 and Schedule 9 of the Northern Ireland Act 1998. The screening has identified no specific equality impacts for all section 75 groups. The equality screening has been published and can be accessed here https://hscbusiness.hscni.net/services/3231.htm

[4] Additionally, a range of offences are listed within Part 6, Sections 170 – 173 of the Data Protection Act 2018: https://www.legislation.gov.uk/ukpga/2018/12/part/6/crossheading/offences-relating-to-personal-data/enacted