



Royal Cornwall Hospitals
NHS Trust

Data Breach Policy

V1.0

December 2023

Accessibility

We have made this policy accessible to ensure those with the following are able to clearly understand the contents of this policy:

- Impaired vision.
- Motor difficulties.
- Cognitive impairments or learning disabilities.
- Deafness or impaired hearing.
- English as a second language.

We are always looking to improve the accessibility of our documents. If you find any problems or think we are not meeting accessibility requirements, please contact our Equality Diversity and Inclusion Team richt.inclusion@nhs.net.

Summary

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity, or availability of personal data. In short, there will be a personal data breach whenever any personal data is accidentally lost, destroyed, corrupted, or disclosed; if someone accesses the data or passes it on without a legal basis; or if the data is made unavailable and this unavailability has a significant negative impact on the data subject.

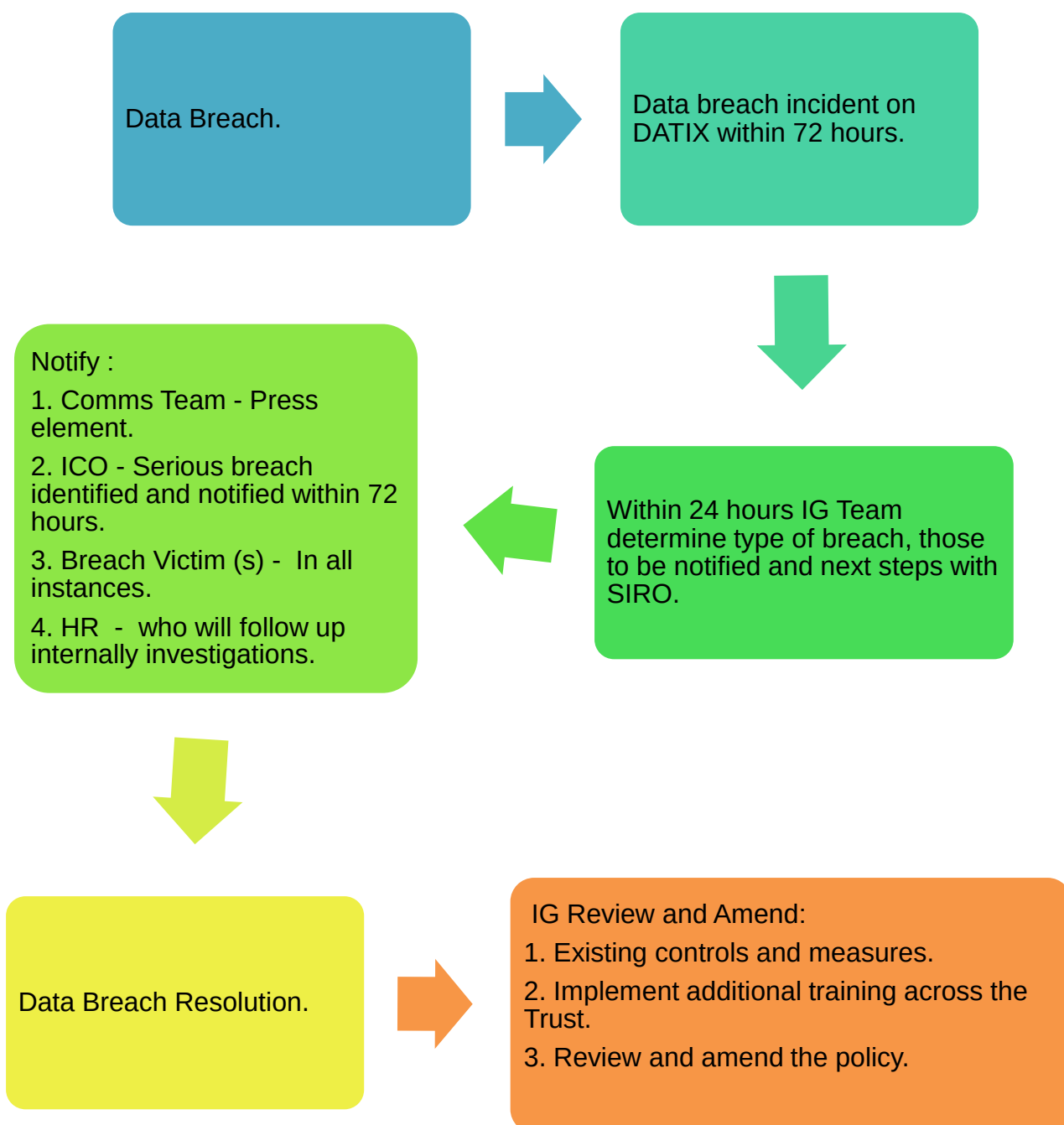


Table of Contents

Accessibility	2
Summary	3
1. Introduction.....	5
2. Purpose of this Policy/Procedure	5
3. Scope.....	5
4. Definitions / Glossary	5
5. Ownership, Responsibilities and HR	7
5.5. Role of the Managers	7
5.6. Role of the Information Governance Group and SIRO	7
5.7. Role of Individual Staff.....	7
6. Standards and Practice	8
6.1. Reporting an Incident:.....	8
6.2. Containment and Recovery:	8
6.2. Investigation and Risk Assessment:	8
6.3. Notification:.....	9
6.4. Evaluation and Response:	10
7. Dissemination and Implementation	10
8. Monitoring compliance and effectiveness	11
9. Updating and Review	11
10. Equality and Diversity	11
Appendix 1. Governance Information	12
Appendix 2. Equality Impact Assessment	14

1. Introduction

- 1.1. The Royal Cornwall Hospital Trust (RCHT) collects, holds, processes, and shares personal data, an asset that needs to be protected.
- 1.2. Every care is taken to protect personal data from incidents (either accidentally or deliberately) to avoid a data protect breach that could compromise security.
- 1.3. Compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative non-compliance, and/or financial costs.
- 1.4. This version supersedes any previous versions of this document.

2. Purpose of this Policy/Procedure

- 2.1. The RCHT is obliged under Data Protection and General Data Protection legislation to have in place an institutional framework designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility.
- 2.2. This policy sets out the procedure to be followed to ensure a consistent and effective approach in managing data breaches and information security incidents across the RCHT.
- 2.3. This policy relates to all personal and special categories (sensitive) data held by the RCHT regardless of format.
- 2.4. The objective of this policy is to contain and manage data breaches, to minimise the risk associated and consider what action is necessary to secure personal data and prevent further breaches.

3. Scope

This policy applies to all staff including temporary, casual or agency staff and contractors, consultants, suppliers, and data processors working for, or on behalf of the RCHT.

4. Definitions / Glossary

- 4.1. For the policy purpose, data security breaches include both confirmed and suspected incidents.
- 4.2. An incident in the context of this policy is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to the RCHT information assets and / or reputation.
- 4.3. An incident includes but is not restricted to, the following:
 - Loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g., loss of laptop, USB stick, iPad / tablet device, or paper record).

- Equipment theft or failure.
- System failure.
- Unauthorised use of access to or modification of data or information systems.
- Attempts (failed or successful) to gain unauthorised access to information or IT system(s).
- Unauthorised disclosure of sensitive / confidential data.
- Website defacement.
- Hacking attack.
- Unforeseen circumstances such as a fire or flood.
- Human error.
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it.
- Staff (all) are knowingly browsing, searching for, or looking at any personal or confidential information about themselves, family members, friends, or other known persons without legitimate purpose.

4.4. Abuse of Privilege

- It is strictly forbidden for staff to look at any personal or confidential information of individuals they know without legitimate purpose. These actions may be an offence under the Data Protection Act.
- Internal investigations will be undertaken by HR and the Information Governance Team in line with disciplinary procedures.

4.5. Acronyms

- RCHT - Royal Cornwall Hospitals Trust.
- UK GDPR - General Data Protection Regulations 2018.
- DPA - Data Protection Act 2018.
- AHRA - Access to Health Records Act 1990.
- SIRO - Senior Information Risk Officer.
- DPO - Data Protection Officer.
- IG - Information Governance.
- HR – Human Resources.

5. Ownership, Responsibilities and HR

- 5.1. Board level are responsible for all matters relating to data breaches. How staff conduct themselves comes under the Caldicott Guardian and Medical Director.
- 5.2. Responsibility for the management of identified breach incidents come under the Trust's Senior Information Risk Officer (SIRO).
- 5.3. The day-to-day management of data breaches relating to data which is attributed to both patients and staff comes under the Head of Information Governance (Data Protection Officer).
- 5.4. All data breaches by staff will be internally investigated and undertaken by Human Resources.

5.5. Role of the Managers

Line managers are responsible for:

- Ensuring all their staff have read and understood the policy outlined.
- Monitoring their staff to ensure they are acting in ways that support the policies outlined earlier in this document.
- Ensure all their staff undertake their mandatory annual Data Security and Awareness training in line with Trust Policy.
- Report data breaches as outlined in this policy.

5.6. Role of the Information Governance Group and SIRO

The IG Group and SIRO Committee are responsible for:

- Monitoring compliance with legislation and Trust Policies through incident reporting.
- Taking any actions that maybe required to mitigate against breaches of data.
- Members of the IG Team and SIRO can act as a Team investigator where data breaches have occurred.

5.7. Role of Individual Staff

All staff members are responsible for:

- Ensuring they comply with Trust policies, procedure, and this policy to safely process data.
- To take responsibility for their actions with all patient and staff data.
- To report any risks or incidents on the Trust's Incident reporting system Datix.

- To ensure they are fully compliant with their annual data awareness mandatory training.

6. Standards and Practice

6.1. Reporting an Incident:

- 6.1.1. Any individual who accesses, uses, or manages the RCHT's information is responsible for reporting any data breach and information security incidents immediately following the Information Use Framework Policy.
- 6.1.2. If the breach occurs or is discovered outside normal working hours, the breach must be reported as soon as practicable.
- 6.1.3. The report must include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information and how many individuals are involved. An incident report form should be completed on DATIX as part of the reporting process.
- 6.1.4. All staff should be aware that any breach of Data Protection legislation may result in the RCHT's Disciplinary procedures being instigated.

6.2. Containment and Recovery:

- 6.1.1. The IG Team will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.
- 6.1.2. An initial assessment will be made by the IG Team to establish the severity of the breach.
- 6.1.3. The IG Team will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.
- 6.1.4. The IG Team and SIRO will establish who may need to be notified as part of the initial containment and will inform the police and ICO, where appropriate.
- 6.1.5. Advice from other professionals may be sought in resolving the incident promptly such as the Communications Team.
- 6.1.6. HR will be notified and will investigate any staff members involved in the data. Breach to ensure a collaborative resolution.

6.2. Investigation and Risk Assessment:

- 6.2.1. An investigation will be undertaken by the IG Team and SIRO immediately and where possible, within 24 hours of the breach being reported.

- 6.2.2. The IG Team will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for the individuals, how serious or substantial those are and how likely they are to occur.
- 6.2.3. The investigation will need to consider the following:
- The type of data involved.
 - Its sensitivity.
 - The protections in place (e.g., encryptions).
 - What has happened to the data (e.g., has it been lost or stolen).
 - Whether the data could be put to any illegal or inappropriate use.
 - Data subject(s) affected by the breach, number of individuals involved and the potential effects on those data subject(s).
 - Whether there are wider consequences to the breach.

6.3. Notification:

- 6.3.1. The IG Team, in consultation with Chief Medical Officer (SIRO) will establish whether the Information Commissioners Office will need to be notified of the breach, and if so, notify them within 72 hours of becoming aware of the breach, where feasible.
- 6.3.2. Every incident will be assessed on a case-by-case basis; however, the following will need to be considered:
- Whether the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms under Data Protection Legislation.
 - Whether notification would assist the individual(s) affected (e.g., could they act on the information it mitigates risks?).
 - Whether notification would help prevent the unauthorised or unlawful use of personal data.
 - Whether there are any legal/contractual notification requirements.
- 6.3.3. Individuals whose personal data has been affected by the incident, and where it has been considered like to result in high risk of adversely affecting that the individual's right and freedoms, will be informed without undue delay as per the Duty of Candour Policy.
- 6.3.4. The IG Team must consider notifying third parties such as the police, insurers, bank or credit card companies, and trade unions. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

- 6.3.5. The IG Team will consider whether the Communications Team should be informed regarding a press release and to be ready to handle any incoming press inquiries.
- 6.3.6. IG Team will notify HR for them to investigate any staff member involved.
- 6.3.7. A record will be kept of any personal data breach, regardless of whether notification was required.

6.4. Evaluation and Response:

- 6.4.1. Once the initial incident is contained, the IG Team will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.
- 6.4.2. Existing controls will be reviewed to determine their adequacy, and whether any corrective action/learning should be taken to minimise the risk of similar incidents occurring.
- 6.4.3. The review will consider:
 - Where and how the personal data is held and where /how it is stored.
 - Existing security measures and potential risks.
 - Whether methods of transmission are secure.
 - Staff awareness.
 - Review the data breach policy.
 - Additional staff training.

7. Dissemination and Implementation

This document will be submitted to the Information Governance Group for approval and following approval will be disseminated to staff via the management structure. New and existing staff will be notified via an email bulletin when the policy is made available on the Documents Library: They will be made aware of its contents during relevant Information Governance training in line with the Training Needs Analysis as outlined in the RCHT Mandatory and Statutory Training Policy.

8. Monitoring compliance and effectiveness

Information Category	Detail of process and methodology for monitoring compliance
Element to be monitored	This Policy will be monitored in its entirety.
Lead	Although the Head of Information Governance will Team this, it the responsibility of all line managers to monitor their own areas of influence.
Tool	Datix will be used to monitor the incidents and risks that are relevant to the data breach content.
Frequency	The management of risks and incidents is an ongoing process resulting in real time continuous monitoring.
Reporting arrangements	The Information Governance Committee will receive reports at each meeting. These will be tabled by the Head of Information Governance. The IGG meets bi-monthly.
Acting on recommendations and Team(s)	Any recommendations or actions will be delegated to the relevant departmental Team as required. A report on progress will be required as directed by the agreed timescale for completion.
Change in practice and lessons to be shared	Significant changes to working practices will be disseminated via the All-Users Bulletins A Team member of the team will be identified to take each change forward where.

9. Updating and Review

- 9.1. The Data Breach policy is updated and reviewed annually.
- 9.2. The review will be conducted by the Head of Information Governance and ratified by the Information Governance Group.
- 9.3. Any revision of activity will be recorded in the Version Control Table as part of the document control process.

10. Equality and Diversity

- 10.1. This document complies with the Royal Cornwall Hospitals NHS Trust service Equality and Diversity statement which can be found in the [Equality Diversity And Inclusion Policy](#) or the [Equality and Diversity website](#).
- 10.2. Equality Impact Assessment

The Initial Equality Impact Assessment Screening Form is at Appendix 2.

Appendix 1. Governance Information

Information Category	Detailed Information
Document Title:	Data Breach Policy V1.0
This document replaces (exact title of previous version):	New Document
Date Issued / Approved:	29 August 2023
Date Valid From:	December 2023
Date Valid To:	December 2026
Author / Owner:	Michele Reed, Information Governance Officer.
Contact details:	rch-tr.infogov@nhs.net
Brief summary of contents:	This policy sets out the procedure to be followed to ensure a consistent and effective approach in managing data breaches and information security incidents across the RCHT.
Suggested Keywords:	Code, Conduct, Confidentiality, Data Protection, Information sharing, Information Governance.
Target Audience:	RCHT: Yes CFT: No CIOS ICB: No
Executive Director responsible for Policy:	Chief Medical Officer
Approval route for consultation and ratification:	Information Governance Group
Manager confirming approval processes:	Director of Integrated Governance
Name of Governance Team confirming consultation and ratification:	Mark Scallan, Head of Information Governance
Links to key external standards:	Data Security and Protection Toolkit Data Protection Act 2018 UK General Data Protection Regulation.

Information Category	Detailed Information
Related Documents:	Information Use Framework Policy. Disciplinary Policy. Employees Confidential Code of Conduct Policy V4.) Page 8 of 23. Duty of Candour Policy. The Gender Recognition Act 2004.
Training Need Identified:	No
Publication Location (refer to Policy on Policies – Approvals and Ratification):	Internet and Intranet
Document Library Folder/Sub Folder:	Health Informatics / Information Governance

Version Control Table

Date	Version Number	Summary of Changes	Changes Made by
23.08.2023	V1.0	Initial issue	Michele Reed Information Governance Officer.

All or part of this document can be released under the Freedom of Information Act 2000.

All Policies, Strategies and Operating Procedures, including Business Plans, are to be kept for the lifetime of the organisation plus 6 years.

This document is only valid on the day of printing.

Controlled Document.

This document has been created following the Royal Cornwall Hospitals NHS Trust [The Policy on Policies \(Development and Management of Knowledge Procedural and Web Documents Policy\)](#). It should not be altered in any way without the express permission of the author or their Line Manager.

Appendix 2. Equality Impact Assessment

Section 1: Equality Impact Assessment (EIA) Form

The EIA process allows the Trust to identify where a policy or service may have a negative impact on an individual or particular group of people.

For guidance please refer to the Equality Impact Assessment Policy (available from the document library) or contact the Equality, Diversity, and Inclusion Team
rcht.inclusion@nhs.net

Information Category	Detailed Information
Name of the strategy / policy / proposal / service function to be assessed:	Data Breach Policy V1.0
Department and Service Area:	Information Governance
Is this a new or existing document?	New
Name of individual completing EIA (Should be completed by an individual with a good understanding of the Service/Policy):	Michele Reed, Information Governance Officer
Contact details:	rcht-tr.infogov@nhs.net

Information Category	Detailed Information
1. Policy Aim - Who is the Policy aimed at? (The Policy is the Strategy, Policy, Proposal or Service Change to be assessed)	To inform staff of their responsibilities with regards to keeping information safe and secure. Providing them with specific guidance to achieve the required standards of the Trust and to meet legislative expectations. It informs staff of what will happen should they be involved in a data breach.
2. Policy Objectives	To ensure person identifiable data is handled securely through staff awareness
3. Policy Intended Outcomes	To minimise incidents and risks associated with the handling of data. To ensure data and subjects are maintained in accordance with legislation.
4. How will you measure each outcome?	Through Datix reports and spot checks.
5. Who is intended to benefit from the policy?	All staff who handle data.

Information Category	Detailed Information
6a. Who did you consult with? (Please select Yes or No for each category)	- Workforce: Yes - Patients/ visitors: No - Local groups/ system partners: No - External organisations: No - Other: No
6b. Please list the individuals/groups who have been consulted about this policy.	Please record specific names of individuals/ groups: Information Governance Group (IGG).
6c. What was the outcome of the consultation?	Agreed.
6d. Have you used any of the following to assist your assessment?	National or local statistics, audits, activity reports, process maps, complaints, staff, or patient surveys: Complaints and reporting methods.

7. The Impact

Following consultation with key groups, has a negative impact been identified for any protected characteristic? Please note that a rationale is required for each one.

Where a negative impact is identified without rationale, the key groups will need to be consulted again.

Protected Characteristic	(Yes or No)	Rationale
Age	No	There are no Age-related concerns
Sex (male or female)	No	There are no Sex related concerns
Gender reassignment (Transgender, non-binary, gender fluid etc.)	No	There are no Gender Reassignment related concerns
Race	No	There are no Race/Ethnic communities related concerns
Disability (e.g. physical or cognitive impairment, mental health, long term conditions etc.)	No	There are no Disability related concerns
Religion or belief	No	There are no Religion related concerns

Protected Characteristic	(Yes or No)	Rationale
Marriage and civil partnership	No	There are no Marriage or Civil Partnership related concerns
Pregnancy and maternity	No	There are no Pregnancy or Maternity related concerns
Sexual orientation (e.g. gay, straight, bisexual, lesbian etc.)	No	There are no Sexual Orientation related concerns

A robust rationale must be in place for all protected characteristics. If a negative impact has been identified, please complete section 2. If no negative impact has been identified and if this is not a major service change, you can end the assessment here.

I am confident that section 2 of this EIA does not need completing as there are no highlighted risks of negative impact occurring because of this policy.

Name of person confirming result of initial impact assessment: Michele Reed, Information Governance Officer.

If a negative impact has been identified above OR this is a major service change, you will need to complete section 2 of the EIA form available here:
[Section 2. Full Equality Analysis](#)