journey to change

NHS
Tees, Esk and Wear Valleys
NHS Foundation Trust

Public – To be published on the Trust external website

Title: Information incidents procedure (confidentiality and privacy breaches)

Ref: CORP-0010-004-v1

Status: Approved
Document type: Procedure
Overarching Policy: Sharing Information and Confidentiality policy

Contents

1 Introduction 3
2 Purpose 3
3 Who this procedure applies to 3
4 Related documents 3
5 What is a breach? 4
5.1 Confidentiality 4
5.2 Integrity 5
5.3 Availability 5
5.4 Events 5
6 Reporting a breach 6
6.1 Near misses 7
6.2 Third party breaches 7
7 Notifying the data subject 7
7.1 When do we need to tell individuals about a breach? 8
7.2 What information must we provide to individuals when telling them about a breach? 8
8 Investigating a breach 9
9 Concluding an investigation 9
10 Liaising with the ICO 9
11 Incidents raised via the complaints or claims process 10
12 Definitions 10
13 How this procedure will be implemented 10
13.1 Implementation action plan 10
13.2 Training needs analysis 11
14 How the implementation of this procedure will be monitored 11
15 References 11
16 Document control (external) 11
Appendix 1 - Equality Impact Assessment Screening Form 13
Appendix 2 – Approval checklist 17
Appendix 3 – Data Security and Protection Incident Report Form 19

1 Introduction

Under UK General Data Protection Regulation (UK GDPR) and the UK Data Protection Act 2018 (DPA 2018), the Trust has a legal obligation to ensure 'privacy by design'.

However, sometimes mistakes can happen that result in a breach of confidentiality or privacy.

UK GDPR and DPA 2018 also introduce a duty on Data Controllers (the Trust) to report certain types of personal data breach to the relevant supervisory authority. In the UK, a Controller must report a notifiable breach of personal data to the Information Commissioners Office within 72 hours of becoming aware of it.

Incident reporting needs an open and fair culture so that staff feel able to report problems without fear of reprisal and know how to resolve and learn from incidents.

This procedure supports Our Journey To Change (OJTC) as set out in the Confidentiality and Sharing Information Policy CORP-0010.

2 Purpose

Following this procedure will help the Trust to:

- Be open and transparent when information incidents occur.
- Report information incidents to the relevant people and regulators in a timely manner.
- Ensure the Data Subject is supported following the breach.
- Investigate incidents and identify root causes.
- Identify information incident trends and problem processes across the Trust.
- Make sure that lessons are learned, areas of concern are acted upon and process improvements made.
- Develop appropriate and relevant communication strategies to increase awareness of and responsiveness to information incidents.

3 Who this procedure applies to

- Anyone working for the Trust who handles person identifiable information in any format.

4 Related documents

This procedure describes what you need to do to implement the 'Breaching Confidentiality' section of the Confidentiality and Sharing Information Policy.

The Confidentiality and Sharing Information Policy defines best practice principles for sharing information which you must read, understand and be trained in before carrying out the procedures described in this document.

- Incident Reporting and Response Policy
- Criminal Incident Reporting Procedure
- Information Governance Policy
- Information Security and Risk Policy
- Requests for information procedure
- Collection of Evidence IG Incidents
- Minimum Standards for Clinical Record Keeping (particularly record keeping for Trans patients)
- Security Procedure (Ridgeway)

5 What is a breach?

GDPR Article 4 (12) defines a 'Personal Data Breach' as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. Such incidents are sometimes referred to as a privacy breach.

Data Security and Protection Breaches can be categorised as:

- Confidentiality – unauthorised access or accidental disclosure of personal data.
- Integrity of systems - unauthorised or accidental alteration of personal data.
- Availability – accidental loss of access to, or destruction of personal data.

5.1 Confidentiality

Unauthorised or accidental disclosure of or access to personal data. For example:

- Letters, emails or telephone message, sent or disclosed to the wrong patient, member of public or staff member, organisation.
- Failure to redact information contained in a subject access request.
- Unauthorised access to records, either by hacking or design, i.e. staff member accessing their own medical record, or the record of a family member, without a lawful basis to do so.
- Discussing information about a patient with a person who does not have a legitimate need to know.

5.2 Integrity

'Integrity' means that records are complete and authentic. Examples of integrity incidents include:

- Records edited or deleted in error.
- Misfiling results or documentation into the wrong record.
- Duplicate records, meaning the patient's record is sitting in more than one place.

5.3 Availability

Unauthorised or accidental loss or access to, or destruction of, personal data, where personal data is unavailable when it should be. For example:

- Insecure disposal of paperwork or hardware. i.e. documents or diaries containing patient details being thrown in the main dustbin, or laptops or computers being taken to the local waste transfer site.
- Staff confidential HR paperwork left in public area, including financial information and personal details, now missing.
- Failure to securely address or send letters to patients or organisations and letter not received.

5.4 Events

The types of event that can lead to an incident can be classed as criminal, technical, people or physical/environmental events. Examples of common events are listed below (note this list is not exhaustive):

- Criminal events:
    - Theft of equipment, data or information, fraud or fraudulent activities.
    - Deception (phishing) e.g., unknown people asking for information, such as a password or details of a third party, that could gain them access to Trust data or receiving unsolicited mail that requires you to enter password data.
    - Attempts to gain unauthorised access to data e.g., hacking Trust systems or tailgating staff into secured areas.
- Technical events:
    - Changes to information or data or system hardware, firmware, or software characteristics without the Trust's knowledge, instruction, or consent.
    - Unwanted disruption or denial of service to a system.
    - Hardware/software failures.

- People Events:
    - Accidental loss of equipment, data or information.
    - Failing to lock a PC screen when left unattended.
    - Human error e.g., emailing personal and/or sensitive personal information to the wrong person.
    - Sharing/transfer of data or information with someone who is not entitled to receive that information; without the consent of the data subject; or sharing more than the necessary amount of personal/sensitive information to complete required tasks.
    - Accessing computer systems/applications using someone else's authorisation e.g., user id and password; sharing logins.
    - Disclosure of passwords/writing it down and leaving it on display where it would be easy to find and used by unauthorised users.
    - Printing or copying confidential information and not storing it correctly or confidentially e.g., leaving documents on photocopiers/printers.
- Physical and Environmental events:
    - Unforeseen circumstances e.g., fire or flood.
    - Unsecure premises.
    - Unlocked/unsecured workstations.

6 Reporting a breach

Any incident involving the loss or unauthorised disclosure of personal identifiable data must be reported on the Trust's incident reporting system as soon as you become aware of it. Also, raise it with your line manager for them to be aware.

Selecting the right category and subcategory for the incident will ensure that the Information Governance Team are notified.

This is so that it can be investigated and mitigated/minimised at the earliest opportunity. The Trust is also required to log these incidents on NHSE's Data Security and Protection Toolkit (DSPT) which is also the escalation route for reporting to the Information Commissioner's Office (ICO).

A notifiable breach of personal data that meets the threshold of reporting to the ICO must be done so within 72 hours of becoming aware of it. Guidance is available via the DSPT that describes how the threshold is determined : Help (dsptoolkit.nhs.uk)

⚠ It is important to remember that a breach is not just about confidential information being disclosed, or the amount of people affected. It is also about the level of harm that can be incurred by the individual whose data has been breached.

'Harm' is determined by the individual as breaches can affect people in different ways depending on their personal circumstances and the nature of the breach.

6.1 Near misses

A near miss is a potential breach that has been prevented, or where the data does not leave the Trust.

For example, a 'no find' paper patient record is traced to a different Trust location to where it is recorded as being held and is therefore not missing.

We should record all breaches, including near misses. This allows us to consider what happened and understand if it could have been prevented. Processes may need to change to prevent further instances happening in the future.

6.2 Third party breaches

If the Trust receives data from an external organisation that does not relate to one of our patients, staff members, etc, notify the organisation as soon as possible. It is their responsibility to report the breach and carry out their own process for Duty of Candour and investigation.

For example, more than one person with the same name in the NHSmail address book and the wrong person has been selected.

If an organisation that is contracted to work on our behalf has a breach, the Trust, as data controller, is responsible for reporting this on the DSPT. We also report the incident on the Trust's incident reporting system to ensure we have an audit trail in case of recurrence, and we raise the incident with the other organisation.

7 Notifying the data subject

As with any incident, we have a duty of candour to an individual affected by a confidentiality or privacy breach.

Recital 85 of the UK GDPR explains that:

"A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches can significantly affect individuals whose personal data has been compromised.

7.1 When do we need to tell individuals about a breach?

If a breach is likely to result in a high risk to the rights and freedoms of individuals, we must inform those concerned as soon as possible.

One of the main reasons for informing individuals is to help them take steps to protect themselves from the effect of a breach.

This would need to be assessed case by case, looking at all relevant factors. If the data subject is a patient, the decision whether to notify them of a breach would also need clinical input to understand the potential impact upon them, and whether the harm caused by notifying them of the breach would outweigh the harm caused by the breach itself.

If the decision is to not notify individuals, we would still need to notify the ICO unless we can demonstrate that the breach is unlikely to result in a risk to rights and freedoms.

7.2 What information must we provide to individuals when telling them about a breach?

You need to describe, in clear and plain language, the nature of the personal data breach and, at least:

- the name and contact details of the Trust's Data Protection Officer you have. This is:

  Andrea Shotton
  Head of Information Governance and Data Protection
  Tarncroft
  Lanchester Road Hospital
  Lanchester Road
  Durham
  DH1 5RD
  Email: tewv.dpo@nhs.net
  Telephone: 0191 333 6574

- a description of the measures taken or proposed to deal with the personal data breach and, where appropriate, a description of the measures taken to mitigate any possible adverse effects.

8 Investigating a breach

If it is necessary to gather further information, a member of the Information Governance team will contact you or your manager to determine what has happened. The impact of the incident will determine if it is necessary to carry out an investigation or whether it can be logged and closed.

An investigation can take different forms depending on the nature of the incident and whether the root cause is immediately apparent. The investigation must collect relevant evidence, recording facts and that follow up action is taken. Examples of evidence includes a written statement, interview, extract of a staff or patient record, audit trail from an electronic system, etc.

If root cause analysis is conducted, the investigator will document their findings using the template in Appendix 3 which is retained within the incident folder along with the evidence and other related documents. Incident documentation is retained in accordance with the NHSX Records Management Code of Practice.

9 Concluding an investigation

The investigation conclusion can take several forms depending on the nature of the incident, whether it has happened before or is likely to recur. This may include:

- Recommendation that advice is sought from People and Culture regarding whether disciplinary action should be taken.
- Presentation of the incident findings to a Decision Making Meeting where the incident involves a Trust clinician.
- Issuing communications to a team, department or the Trust.
- Recommendation to undertake additional training and development.
- Recommendation for changes to process where this has found to be the root cause of the incident.

10 Liaising with the ICO

Failing to report an information incident to the ICO when required to do so can result in a monetary penalty. This may also be combined with other corrective powers, and all actions taken by the ICO are in the public domain.

It is important for the data subject(s) and the Trust that we proactively engage with the ICO as needed. This engagement is coordinated by Information Governance with the oversight and

guidance of the Head of Information Governance/Data Protection Officer (see 7.2). Records of communication with the ICO are retained within the incident investigation folder.

11 Incidents raised via the complaints or claims process

Sometimes information incidents are brought to the Trust's attention via the complaints or claims process.

In these cases, the reporting and investigating process will be as outlined above, but findings are reported to the complaints or claims team for inclusion in their response. Incidents identified in this way will be managed by liaising with the complaints or claims team and agreeing the process, responsibilities and timescales.

12 Definitions

Term	Definition
DPO	• Data Protection Officer (for details, see 7.2)
DSPT	• Data Security and Protection Toolkit
ICO	• Information Commissioner's Office

13 How this procedure will be implemented

- This procedure will be published on both the staff intranet and Trust website and disseminated to all Trust employees via all-staff briefing.

13.1 Implementation action plan

Activity	Expected outcome	Timescale	Responsibility	Means of verification/ measurement
N/A				

13.2 Training needs analysis

Staff/Professional Group	Type of Training	Duration	Frequency of Training
All staff	Mandatory Data Security and Awareness Training	2hrs	Annually

14 How the implementation of this procedure will be monitored

Number	Auditable Standard/Key Performance Indicators	Frequency/Method/Person Responsible	Where results and any Associate Action Plan will be reported to, implemented and monitored; (this will usually be via the relevant Governance Group).
1	Incident statistics	Frequency = Monthly Method = Paper Responsible = Information Compliance Manager	Information incident stats are provided monthly to Digital Performance and Assurance Group (DPAG) with prior oversight of Information Governance Group and Digital and Data Management Meeting. Agreed actions are monitored via DPAG.

15 References

Information Commissioners Office website UK GDPR data breach reporting (DPA 2018) | ICO

NHSE Data Security and Protection Toolkit Data Security and Protection Toolkit (dsptoolkit.nhs.uk)

16 Document control (external)

To be recorded on the policy register by Policy Coordinator

Required information type	Information
Date of approval	19 June 2024
Next review date	19 June 2027

This document replaces	N/A
This document was approved by	Information Governance Group
This document was approved	19 June 2024
This document was ratified by	Digital and Data Management Meeting
This document was ratified	18 June 2024
An equality analysis was completed on this policy on	03 May 2024
Document type	Public
FOI Clause (Private documents only)	n/a

Change record

Version	Date	Amendment details	Status
1	19 June 2024	New procedure	Published

Appendix 1 - Equality Impact Assessment Screening Form

Please note: The Equality Impact Assessment Policy and Equality Impact Assessment Guidance can be found on the policy pages of the intranet

Section 1	Scope
Name of service area/directorate/department	Digital and Data Services
Title	Information Incidents Procedure (Confidentiality and Privacy Breaches)
Type	Procedure/guidance
Geographical area covered	Trust-wide
Aims and objectives	Following this procedure will help the Trust to: • Be open and transparent when information incidents occur. • Report information incidents to the relevant people and regulators in a timely manner. • Ensure the Data Subject is supported following the breach. • Investigate incidents and identify root causes. • Identify information incident trends and problem processes across the Trust. • Make sure that lessons are learned, areas of concern are acted upon and process improvements made. • Develop appropriate and relevant communication strategies to increase awareness of and responsiveness to information incidents.
Start date of Equality Analysis Screening	04 January 2024
End date of Equality Analysis Screening	03 May 2024

Section 2	Impacts
Who does the Policy, Procedure, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan benefit?	All staff, patients and their families and carers
Will the Policy, Procedure, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan impact negatively on any of the protected characteristic groups? Are there any Human Rights implications?	• **Race** (including Gypsy and Traveller) **NO** • **Disability** (includes physical, learning, mental health, sensory and medical disabilities) **NO** • **Sex** (Men and women) **NO** • **Gender reassignment** (Transgender and gender identity) **NO** • **Sexual Orientation** (Lesbian, Gay, Bisexual, Heterosexual, Pansexual and Asexual etc.) **NO** • **Age** (includes, young people, older people – people of all ages) **NO** • **Religion or Belief** (includes faith groups, atheism and philosophical beliefs) **NO** • **Pregnancy and Maternity** (includes pregnancy, women / people who are breastfeeding, women / people accessing perinatal services, women / people on maternity leave) **NO** • **Marriage and Civil Partnership** (includes opposite and same sex couples who are married or civil partners) **NO** • **Armed Forces** (includes serving armed forces personnel, reservists, veterans and their families) **NO** • **Human Rights Implications NO** (Human Rights - easy read)
Describe any negative impacts / Human Rights Implications	None
Describe any positive impacts / Human Rights Implications	A breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches can significantly affect individuals whose personal data has been compromised. This procedure provides assurance to any data subject that their very sensitive information will be properly looked after, but that any breach is taken seriously and is reported and acted upon

	appropriately. Also that we will be open and transparent so that the data subject can be supported appropriately based on their individual circumstances.

Section 3	Research and involvement
What sources of information have you considered? (e.g. legislation, codes of practice, best practice, nice guidelines, CQC reports or feedback etc.)	UK Data Protection Legislation: Data Protection Act 2018 and UK GDPR Data Security and Protection Toolkit Information Commissioner's Office (ICO) Guidance Gender Recognition Act 2004
Have you engaged or consulted with service users, carers, staff and other stakeholders including people from the protected groups?	Although not engaged with directly in developing this document, the working group have had direct contact with people whose information has been breached. Their understanding of the negative impacts and feedback received from data subjects, including people from the protected groups, has been included in this document.
If you answered Yes above, describe the engagement and involvement that has taken place	
If you answered No above, describe future plans that you may have to engage and involve people from different groups	

Section 4	Training needs
As part of this equality impact assessment have any training needs/service needs been identified?	No
Describe any training needs for Trust staff	n/a
Describe any training needs for patients	n/a
Describe any training needs for contractors or other outside agencies	n/a

Check the information you have provided and ensure additional evidence can be provided if asked.

Appendix 2 – Approval checklist

Title of document being reviewed:	Yes / No / Not applicable	Comments
1. Title		
Is the title clear and unambiguous?	Yes	
Is it clear whether the document is a guideline, policy, protocol or standard?	Yes	
2. Rationale		
Are reasons for development of the document stated?	Yes	
3. Development Process		
Are people involved in the development identified?	Yes	
Has relevant expertise has been sought/used?	Yes	
Is there evidence of consultation with stakeholders and users?	Yes	
Have any related documents or documents that are impacted by this change been identified and updated?	Yes	
4. Content		
Is the objective of the document clear?	Yes	
Is the target population clear and unambiguous?	Yes	
Are the intended outcomes described?	Yes	
Are the statements clear and unambiguous?	Yes	
5. Evidence Base		
Is the type of evidence to support the document identified explicitly?	Yes	
Are key references cited?	Yes	
Are supporting documents referenced?	Yes	

6. Training		
Have training needs been considered?	Yes	
Are training needs included in the document?	Yes	
7. Implementation and monitoring		
Does the document identify how it will be implemented and monitored?	Yes	
8. Equality analysis		
Has an equality analysis been completed for the document?	Yes	
Have Equality and Diversity reviewed and approved the equality analysis?	Yes	
9. Approval		
Does the document identify which committee/group will approve it?	Yes	
10. Publication		
Has the policy been reviewed for harm?	Yes	
Does the document identify whether it is private or public?	Yes	
If private, does the document identify which clause of the Freedom of Information Act 2000 applies?	Yes	
11. Accessibility (See intranet accessibility page for more information)		
Have you run the Microsoft Word Accessibility Checker? (Under the review tab, 'check accessibility'. You must remove all errors)	Yes	
Do all pictures and tables have meaningful alternative text?	Yes	
Do all hyperlinks have a meaningful description? (do not use something generic like 'click here')	Yes	

Appendix 3 – Data Security and Protection Incident Report Form

DATA SECURITY & PROTECTION INCIDENT REPORT FORM

Reporting Details	
ID:	Web Ref:
Reporter:	Date Reported:
Contact Number:	Date of Incident:
Location:	Staff / Patient Incident:
Preliminary Type:	Preliminary Level:
What has happened	
How did you find out?	
Was the incident caused by a problem with a network or an information system?	
No.	
Does this incident impact across a national border?	
No.	
Have you informed the Police?	
No.	
Have you informed any other regulatory bodies?	
No.	
Has there been any media coverage of the incident (that you're aware of)?	
No.	
How many citizens have been affected?	
#.	
Who is affected?	
Any further information	
What is potential significance / impact of the adverse effect on individuals?	
1. No adverse effect (There is absolute certainty that there can be no adverse effect) 2. Potentially some minor adverse effect or involves vulnerable groups even if not adverse effect occurs (minor adverse effect must be selected when there is no absolute certainty) 3. Potentially some severe adverse effect (An adverse effect may be release of	

confidential information into the public domain leading to embarrassment or it prevents someone from doing their job such as a cancelled procedure that has the potential of prolonging suffering but does not lead to a decline in health)

4. Potentially pain and suffering or financial loss (Reported suffering, decline in mental health, or financial loss including loss of employment)
5. Death / catastrophic event (A person dies or suffers a catastrophic occurrence)

What is the likelihood that citizens' rights have been affected?

1. Not occurred (There is absolute certainty that citizen's rights have not been affected)
2. Not likely or incident involved vulnerable groups where no adverse effect occurred
3. Likely (There is a chance that there will be an occurrence of an adverse effect arising from the incident)
4. Highly likely (It is almost certain that an adverse effect will occur in the future)
5. **Occurred (An adverse effect has been reported as a result of the incident)**

Conclusions & recommendations

•

Culture of Candour (Patient) – have the data subjects been informed?

Has the incident been documented on the patient's Paris records?
Yes No

If no, please provide a reason?

Has the relevant clinician determined whether it would be appropriate to inform the patient / carer of the incident?
Yes No

If no, please provide a reason?
If yes, what was the outcome?

Has the patient been informed of the incident and an apology provided? (Please supply the date this took place)
Yes No

If no, please provide a reason?

Has the verbal apology been followed up in writing? (Please supply the date this took place)
Yes No

If no, please provide a reason?

Culture of Candour (Staff) – have the data subjects been informed?

Has the staff member been informed of the incident and an apology provided? (Please supply the date this took place)
Yes **No**

If no, please provide a reason? –

Has the verbal apology been followed up in writing? (Please supply the date this took place)
Yes No

If no, please provide a reason?

Has the staff member been offered any support by management?
Yes No

ICO Details	
Toolkit Ref:	ICO Ref:
Date of confirmation email received from ICO:	
ICO's consideration of the case:	
Formal report required: Yes No	
Further action required according to ICO: Yes No N/A	
Confirmed Type:	Confirmed Level:
Date of Upload to Toolkit:	Date of Closure: DD/MM/YYYY hh:mm