Northern Ireland Blood Transfusion Service	POLICY DOCUMENT

Document Details

Document Number: POL:20:IGP:006:01:NIBT **No. of Appendices:** 0

Supersedes Number: N/A New Policy

Document Title: DATA BREACH POLICY

ISSUE DATE: 28 SEPTEMBER 2020 EFFECTIVE DATE: 26 OCTOBER 2020

Document Authorisation

Written By : Paula Johnston, Information Governance Manager

Signature: Paula Johnston, Information Governance Manager **Date :** 28.09.2020

Authorised By : Karin Jackson, Chief Executive

Signature: Karin Jackson, Chief Executive **Date :** 28.09.2020

CROSS REFERENCES

This Policy refers to the following documents:

Doc Type	Doc. No.	Title
SOP	QA:070	Procedure for Reporting and Management of Quality Incidents
SOP	GL:017	Procedure for Reporting and Management of Serious Adverse Incidents
SOP	GL:021	Early Alert Procedure

Key Change from Previous Revision:

N/A New Policy.

1. STATEMENT

The Northern Ireland Blood Transfusion Service takes the security and confidentiality of all records very seriously. We have a range of measures, policies and procedures in place to help ensure the confidentiality and security of all records, in all formats, throughout their lifecycle. However it is recognised that despite all the measures in place data breaches may still occur. This policy sets out how the NI Blood Transfusion Service will respond to such breaches if they do occur.

The Northern Ireland Blood Transfusion Service will:

- Take all possible measures to ensure the security and confidentiality of patient, donor and staff information as well as sensitive corporate information.
- Ensure NIBTS complies with the relevant legislation and good practice guidelines in relation to Information Governance and Data Security as required by the General Data Protection Regulation (GDPR), the Data Protection Act 2018 and the Blood Safety and Quality Regulations (BSQR) 2005.
- Ensure all staff and contractors are reminded of their obligations regarding the security and confidentiality of NIBTS records.
- Ensure all staff are made aware of the requirement to report an actual or suspected data breach immediately.
- Ensure all staff complete Information Governance Training as required.
- Ensure data breaches are assessed promptly to ascertain if the breach reaches the threshold for reporting to the Information Commissioner's Office and / or the Department of Health.
- Ensure all data breaches are recorded and investigated without delay in keeping with GDPR requirements.
- Following a data breach, ensure measures are put in place to mitigate the likelihood of the breach occurring again.

2. OVERVIEW

The NI Blood Transfusion Service (NIBTS) is required to demonstrate legal compliance and high standards of corporate governance in relation to the management of information.

NIBTS is subject to the Blood Safety and Quality Regulations (BSQR) 2005 and must comply with the requirements of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

NIBTS recognises its legal and statutory obligations in relation to the management of information assets within its control, and the need for a balance to be struck between openness and confidentiality in the management and use of those information assets. To this end, NIBTS fully supports the principles of corporate governance and recognises its public accountability, but equally places significant importance on ensuring the confidentiality of patient, donor and staff information. NIBTS recognises the need to ensure robust security measures are adopted to protect such information from accidental loss or unauthorised disclosure.

The purpose of this document is to outline how NIBTS will deal with data breaches and the responsibilities for staff in relation to data breaches.

3. RESPONSIBILITY

Chief Executive
The Chief Executive has overall responsibility for ensuring that NIBTS complies with its statutory obligations and Department of Health (DoH) requirements.

Head of HR & Corporate Services
The Head of HR & Corporate Services has overall responsibility for Information Governance within NIBTS and reports on Information Governance to the Board, SMT and the Governance and Risk Committee. The post holder is the Senior Information Risk Owner (SIRO) for the organisation. They manage and oversee the work of the Information Governance Manager.

Senior Managers – Information Asset Owners
Individual Senior Managers (SMT members) fulfil the role of Information Asset Owners for each of their areas. This includes responsibility for ensuring their staff are aware of their responsibilities in relation to Information Governance. They should ensure that all staff receive the appropriate training at induction and throughout their employment.

Information Governance Manager
Reporting to the Head of HR & Corporate Services, the Information Governance Manager is responsible for developing and rolling out the information governance agenda in the organisation. They will have overall responsibility for developing and implementing IG policies and procedures within NIBTS and will provide guidance and assistance to staff in relation to IG matters.

Senior Information Risk Owner (SIRO)
The SIRO is the focus for the management of information risk reporting at Board level. The SIRO will advise the Accounting Officer on the Information Risk aspect of the Governance Statement and will be responsible for the overall information risk and risk assessment process.

Data Protection Officer (DPO)
The Data Protection Officer is a role legally required by the General Data Protection Regulation (GDPR). The DPO role is fulfilled by the IG Manager. The DPO provides advice to the organisation on compliance obligations and completion of privacy impact assessments. They monitor compliance with the GDPR and organisational policies. They co-operate and liaise with the Information Commissioners Office and if necessary have the ability to report directly to the highest level of management within the organisation.

Personal Data Guardian (PDG)
The Personal Data Guardian is a senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing. The PDG plays a key role in ensuring that responsibilities with partner organisations satisfy the highest practicable standards for handling personally identifiable information.

Information Asset Owners (IAOs)
The IAO's primary role will be to manage and address risks associated with the information assets within their function and to provide assurance on the management of those assets. Each NIBTS SMT member will act as the Information Asset Owner for their area.

Information Asset Administrators (IAAs)
IAAs will assist the IAO for their area. In addition they will support and assist with IG related tasks within their departments as required.

4. POLICY

4.1 All suspected breaches should be reported to the Information Governance Manager as soon as they are identified. In the absence of the IG Manager, breaches should be reported to the Information Asset Owner (SMT member) for the department in which the breach occurred. In the absence of the IAO breaches should be reported to the IAA for the area.

4.2 In the first instance NIBTS should take all possible steps to contain the data breach and take all steps possible to recover the data.

4.3 An internal incident should be raised as soon as possible as per SOP:QA:070 'The Procedure for Reporting and Management of Quality Incidents'. An investigation should commence immediately to establish the root cause and potential consequences of the data breach.

4.4 Article 33 of the GDPR requires data controllers to notify the ICO when a breach "is likely to result in a risk to the freedoms and rights of natural persons". This notification must be made "without undue delay" and within 72 hours (including weekends and bank holidays) of the organisation becoming aware of it.

4.5 The incident also needs to be assessed to establish if it should be reported as a Serious Adverse Incident to the DoH as per SOP:GL:017 'Procedure for Reporting and Management of Serious Adverse Incidents' and/or as an early alert as per the SOP:GL:021 'Early Alert Procedure'.

4.6 The IG Manager in conjunction with the relevant Information Asset Owner(s) / Administrator(s), should risk assess the data breach to establish the extent of the breach and the risk to the data subject(s).

4.7 Following the risk assessment the IG Manager should make a determination as to whether the data breach meets the threshold for onward reporting to the Information Commissioner's Office.

4.8 As Data Protection Officer for the organisation, the IG Manager has the final say in whether or not a breach should be reported to the ICO. The Data Protection Officer cannot be dismissed or penalised for carrying out this duty appropriately.

4.9 If the incident is assessed as being reportable to the ICO, this should be done within 72 hours of the incident occurring or the organisation becoming aware of it.

4.10 Consideration should also be given to notifying any affected individuals. The risk to the rights and freedoms of the individual should be assessed along with the likely impact of the breach. The reasoning for any decision made in this regard should be documented.

4.11 NIBTS must fully cooperate with the ICO investigation.

4.12 Following a full investigation, the incident should be evaluated and any steps taken to help ensure it does not happen again.

4.13 A record of all personal data incidents / breaches must be kept regardless of whether or not there is a requirement to report to the ICO.

5. EQUALITY SCREENING OUTCOME

This policy has been drawn up and reviewed in light of the statutory obligations contained within Section 75 of the Northern Ireland Act (1998). In line with this statutory duty of equality this policy has been screened against particular criteria. If at any stage of the life of the policy there are any issues within the policy which are perceived by any party as creating adverse impacts on any of the groups under Section 75 that party should bring these to the attention of the Head of HR & Corporate Services.

The Northern Ireland Blood Transfusion Service is committed to the promotion of equality of opportunity for staff, donors and service users. We strive to ensure that everyone is treated fairly and that their rights are respected at all times. We believe that it is important that our policy is understood by all those whose literacy is limited, those who do not speak English as a first language or those who face communication barriers because of a disability. On request it may be possible to make this policy available in alternative formats such as large print, Braille, disk, audio file, audio cassette, Easy Read or in minority languages to meet the needs of those not fluent in English.'

6. TRAINING REQUIREMENTS

All staff should read this policy and sign to indicate they have read and understood.