Northern Ireland Blood Transfusion Service	POLICY DOCUMENT

Document Details

Document Number: POL:14:IGP:003:02:NIBT **No. of Appendices:** None

Supersedes Number: POL:14:IGP:003:01:NIBT

Document Title: NIBTS INFORMATION GOVERNANCE POLICY

ISSUE DATE: 27 FEBRUARY 2019 EFFECTIVE DATE: 13 MARCH 2019

Document Authorisation

Written By : P Johnston, Information Governance Manager

Signature: _____ **Date :** _____

Authorised By : Ivan Ritchie, Head of HR & Corporate Services

Signature: _____ **Date :** _____

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
		Department of Health Good Management Good Records
POL	HP:014	NIBTS Security Policy
POL	IGP:001	Confidentiality and Data Protection Policy
POL	IGP:002	Records Management Policy
POL	IP:005	NIBTS Computer Security Policy
POL	QP:003	NIBTS Incident Management Policy
APP 1	APPENDIX	Information Governance Management Framework

Key Change From Previous Revision:
Removal of section relating to Information Risk Policy. This will be covered in a stand-alone policy.

1. STATEMENT

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.

The NI Blood Transfusion Service will:

- Ensure the security and confidentiality of patient, donor and staff information as well as corporately sensitive information.
- Make records accessible where possible and in keeping with legislation.
- Ensure NIBTS complies with the relevant legislation and good practice guidelines in relation to Information Governance.
- Train and develop staff to enable them to carry out their responsibilities in relation to Information Governance.
- Manage and review information risk within the organisation to ensure risks are identified and dealt with appropriately.

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 recognises its legal and statutory obligations in relation to the management of information assets within its care, 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, the 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, as well as corporately sensitive information, and the need to ensure robust security measures are adopted to protect that information from accidental loss or deliberate unauthorised disclosure.

The purpose of this document is to outline responsibilities and provide a set of principles covering all aspects of information governance.

3 RESPONSIBILITY

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

Head of HR & Corporate Services
The Head of HR & Corporate Services is the senior manager with 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
Individual Senior Managers (SMT members) fulfil the role of Information Asset Owners for each of their areas. They are responsible 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 level 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 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 have the ability to report diectly 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 Guardian plays a key role in ensuring that responsibilities with partner organisations satisfy the highest practicable standards for handling patient 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 Senior Manager will act as the Information Asset Owner for their area.

Information Asset Administrators (IAAs)
IAAs will assist the IAO for their area.

4 POLICY

4.1 Openness

As a public body NIBTS recognises the need for openness and transparency. As such the organisation will endeavour to make all relevant information available to the public as and when required, e.g. through FOI requests.

NIBTS will work towards publishing more information on the NIBTS website and in particular within the Publication Scheme section.

Individuals, including donors, patients and staff, should be able to access information held about them as per their rights under the General Data Protection Regulation (GDPR) and the Data Protection Act.

4.2 Legal Compliance

The NIBTS regards all identifiable personal information as confidential. Personal information relating to staff will be treated as confidential except where national policy on accountability and openness requires otherwise and in the public interest.

NIBTS will establish and maintain policies to ensure compliance with the GDPR, Data Protection Act, Freedom of Information Act, the DoH Code of Practice on Protecting the Confidentiality of Service User Information and the common law duty of confidentiality, as well as best practice guidance set out in DoH Good Management Good Records.

The organisation will investigate all breaches of confidentiality and security, and failure to comply with key information governance policies in line with NIBTS incident reporting processes.

4.3 Information Security

NIBTS will establish and maintain policies for the effective and secure management of its information assets and resources. The organisation will promote effective confidentiality and security practices to its staff through the dissemination of its policies, the establishment of local procedures, and staff training and awareness.

NIBTS will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.

4.4 Information Quality Assurance

NIBTS will establish and maintain policies and procedures for information quality assurance and the effective management of records.

The organisation will undertake annual assessments and audits of its information quality and records management arrangements in compliance with the DoH Information Management Assurance Checklist.

Managers are expected to take ownership of, and seek to improve, the quality of information within their services. Wherever possible, information quality should be assured at the point of collection.

The organisation will promote information quality and effective records management through policies, local procedures / user manuals and staff training and awareness.

4.5 Appropriate Information Sharing

Appropriate sharing of some personal Health & Care information, for example test results, is essential for achieving faster, safer decisions for better care outcomes. NIBTS will take account of Data Protection considerations associated with the processing and sharing of personal data and establish and maintain Data Sharing Agreements when appropriate to allow the secure and safe sharing of patient identifiable information with due consideration given to patient consent, arrangements for controlled access and governance arrangements for the shared data.

5 INFORMATION GOVERNANCE FRAMEWORK

Appendix one provides the NIBTS Information Governance Framework. The framework provides a high level summary of the key Information Governance roles, policies, reporting and oversight arrangements, training and incident management processes in place for the organisation.

6 MONITORING COMPLIANCE

NIBTS will follow this information governance policy within all relevant procedures and guidance used for operational activities. Interpretation of the policy will be monitored and there will be regular planned internal inspections to assess how the policy is being put into practice. These inspections will seek to:

- identify areas of good practice which can be used throughout NIBTS;
- highlight where non-conformance to the procedures is occurring;
- If appropriate, recommend a tightening of controls and make recommendations as to how compliance can be achieved.

This policy reflects the requirements of:

- Public Records Act (NI) 1923
- Blood Safety and Quality Regulations 2005
- Good Pharmaceutical Manufacturing Practice
- Disposal of Documents Order No 167, 1925
- Limitation Act 1980
- Freedom of Information Act 2000
- International Standard on Records Management (ISO 15489)
- Electronic Records Management: Toolkits (PRO, 2000-2002)
- General Data Protection Regulation
- Data Protection Act 2018
- Records Management Standards and Guidance (PRO, from 1998)

- Northern Ireland Records Management Standards (NIRMS) (2002) (Public Records Office of Northern Ireland)
- Good Management Good Records 2012
- The Lord Chancellor's Code of Practice on the Management of Records under Section 46 of the Freedom of Information

7 EQUALITY SCREENING AND ACCESSIBILITY

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.'

8 TRAINING REQUIREMENTS

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

Appendix 1 – Information Governance Framework

INFORMATION GOVERNANCE MANAGEMENT FRAMEWORK		
Heading	**Requirement**	**Notes**
Senior Roles	• IG Lead – Chief Executive. • Senior Information Risk Owner (SIRO) – Head of HR and Corporate Services • Personal Data Guardian – Medical Director • Data Protection Officer (DPO)	The Chief Executive is ultimately responsible for Information Governance at Board level. The Head of HR and Corporate Services is the Senior Information Risk Owner (SIRO). Medical Director is the Personal Data Guardian (PDG) for the organisation. The Information Governance Manager is the Data Protection Officer for NIBTS.
Key Policies	• POL:IGP:001 – Confidentiality and Data Protection Policy for NIBTS • POL:IGP:002 – Records Management Policy • POL:IGP:003 – Information Governance Policy • POL:IGP:004 – Security of Confidential Information Policy • POL:IGP:005 – Information Lifecycle Management Policy • POL:HP:014 - Security Policy • POL:IP:005 – NIBTS Computer Security Policy	These are the main IG related policies within NIBTS, however several other polices feed into and support the IG agenda.
Key Governance Bodies	Governance and Risk Committee	The Governance and Risk Committee is a sub-group of the Board. The HR & Corporate Services Manager reports to Governance and Risk on IG issues.

Resources	Head of HR and Corporate Services reports on IG issues to the Board, SMT and the Governance and Risk Committee. The Information Governance Manager is responsible for the day-to-day management of Information Governance within the organisation. Senior Managers have been trained as Information Asset Owners (IAOs), key staff from each department have been identified and trained as Information Asset Administrators (IAAs)	IAOs and IAAs liaise with the IG Manager to identify the information assets in their areas. They will report on risks associated with these assets through the risk management process. The IAOs and IAAs meet quarterly to discuss IG related issues and requirements.
Governance Framework	The Head of HR and Corporate Services is the senior manager responsible for IG within NIBTS, they are also the SIRO for the organisation. The Medical Director is the Personal Data Guardian The IG Manager is responsible for the day-to-day management of IG and takes the lead on advising IAOs and IAAs. SLAs and contracts with third parties refer to IG issues such as confidentiality, data protection, records management and freedom of information.	
Training & Guidance	All staff should complete the Information Governance e-learning training on commencement of employment and every two years thereafter. The IG Manager will advise those who need to complete	

	the other IG relatedtraining. Staff should be trained in local / departmental procedures involving access to personal or sensitive information prior to working with the information. The IG Manager, the SIRO and the PDG will attend specialist IG training to ensure they keep up-to-date with developments. All use / processing of personal information should be in keeping with Data Protection legislation and best practice guidelines.	
Incident Management	All staff must comply with the incident management procedure SOP:QA:070 Procedure for Reporting and Management of Quality Incidents and POL:QP:003 NIBTS Incident Management Policy. If an incident arises in relation to any aspect of IG it should be raised, the IG Manager should be informed and consulted.	