WoSCAN

Information Governance Framework

Prepared by	Carol Marshall, Information Manager
Approved by	Evelyn Thomson, Regional Manager (Cancer)
Issue date	May 2023
Review date	May 2026
Version	v1.3
Replaces previous version	v1.2

1.0 Introduction

The Information Governance Framework is formed by those elements of law and policy from which applicable information governance standards are derived, and the activities and roles which individually and collectively ensure that these standards are clearly defined and met.

Information Governance ensures necessary safeguards for, and appropriate use of, patient and personal information.

The intention of this Framework is to provide a context within which all West of Scotland Cancer Network (WoSCAN) staff and other authorised users of information can securely manage and share information. Staff who have followed this framework and the associated WoSCAN and NHS Greater Glasgow and Clyde (NHS GGC) policies and procedures, will be fully supported by WoSCAN in the event of a security breach.

This framework has been developed with cognisance of the hosting arrangements for WoSCAN within NHS GGC and its' policies and procedures.

This Framework should be read in conjunction with more detailed NHS GGC and WoSCAN Information Governance policies and guidelines (Appendix 2 refers). A list of relevant legislation on which these policies are based can be found in Appendix 1 and are also available on NHS GGC Staffnet or the WoSCAN network folder.

2.0 Purpose of Framework

The purpose of this Framework is to:

- Ensure policies and procedures are in place which promote the confidentiality, security and management of information and that staff are aware of their legal obligations.
- Set out the practices and procedures staff must follow when collecting, storing, communicating and transferring electronic and manual personal identifiable data both within and outwith NHSGGC.
- Outline the responsibilities of managers and staff in respect of Information Governance.
- Detail the approval and governance processes and structures in place to manage these policies.

3.0 Scope

This Framework concerns all aspects of information within WoSCAN, including but not limited to:

- Audit data
- Cancer data and intelligence held in NHS systems
- Patient/stakeholder information
- Staff information
- Sensitive organisational information

The scope also includes the storage, disposal and communication of such information held in any manual or computerised form, in line with the NHS Scotland Code of Practice: Protecting Patient Confidentiality , and the Scottish Government Records Management: NHS Code of Practice (Scotland).

This guidance applies to all WoSCAN staff and is also relevant to contractors, partnership organisations and visitors not employed by WoSCAN but engaged to work with WoSCAN.

This framework covers obtaining, disclosing, recording, holding, using, erasing or destroying personal, sensitive or confidential information and is primarily based on the principles outlined in the UK General Data Protection Regulation 2018 and the NHSScotland Caldicott Guardians Principles into Practice, 2012 and also reflects the WoSCAN Information Request Process.

3.1 Caldicott Requirements

All patients have a right to expect that information relating to them will be properly created and managed; that it will be handled in confidence and that patient identifiable information will only be shared with those whose justification for receiving such information has been rigorously tested.

This is based on the Caldicott Principles which are:

- Justify the purpose(s) for using confidential information
- Only use it when absolutely necessary
- Use the minimum required
- Access should be on a strict need-to-know basis
- Everyone must be aware of their responsibilities
- Understand and comply with the law
- The duty to share information can be as important as the duty to protect patient confidentiality.

Under existing hosting arrangements for WoSCAN, the NHS GGC Caldicott Guardian acts as the WoSCAN Caldicott Guardian. The role of Caldicott Guardian within NHS GGC is held by the Deputy Director of Public Health.

3.2 UK General Data Protection Regulation

UK GDPR applies to all information processed by computer or held in paper format which could identify a living individual. The key principles are that personal data shall be:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes and not further processed;
- adequate, relevant and limited to what is necessary for the purpose collected;
- accurate and where necessary kept up to date;
- kept in form which allows identification and not kept for longer than necessary; and
- processed in a manner that ensures appropriate security;

NHSGGC has a legal obligation to ensure staff are aware of the requirements of the UK GDPR and comply with its obligations under the Regulation. This is done through staff training, policies and procedures and NHS Codes of Practice.

4. Information Sharing

WoSCAN recognises the need to share information appropriately, and encourage staff to share information across departments and with partner organisations to ensure the best possible care is provided to patients. We also have a duty to ensure our staff, contractors and other users of WoSCAN managed systems and data can share information within a secure environment and are protected against the risk of a security breach occurring.

Where we are required to share information for the purposes of clinical audit, service redesign or service improvement, we will do so in line with the WoSCAN Information Request Process which has been approved by the national Public Benefit and Privacy Panel process (PBPP).

4.0 Responsibilities

Corporate accountability for the WoSCAN function is assumed by NHS GGC as host NHS Board. Policies and guidelines of NHS GGC apply to all staff employed directly to support the functioning of WoSCAN.

The Regional Manager (Cancer) is the senior accountable manager within WoSCAN for the enforcement of this Framework. This includes ensuring that staff within the department work in a manner consistent with the principles outlined in this framework and associated policies and guidelines. They also have responsibility to ensure the investigation of any security issues relating to WoSCAN.

The WoSCAN Information Manager has delegated operational responsibility for Information Governance.

When processing, storing, communicating or sending personal identifiable information it is the responsibility of all individuals working within WoSCAN to ensure it is being carried out in line with this framework and associated policies and guidelines.

Failure to comply with these principles and policies may result in disciplinary procedures being applied, which in the case of serious breaches could include disciplinary action, up to and including dismissal.

Staff are required to comply with the terms of the UK GDPR, Caldicott guidance and all Information Governance polices and guidance.

It is the responsibility of staff to ensure they have read and understood all Information Governance policies and guidelines (Appendix 2 refers)**.**

5.0 Security Breaches

All actual, potential or suspected breaches of information or IT security should be reported to

Line Management in the first instance. This should also be reported via the Datix Electronic Reporting System, and in the case of the loss of IT equipment, should also be reported to the eHealth IT Service Desk. This will allow NHS GGC to take appropriate action, monitor trends and meet reporting obligations.

6.0 Review and Maintenance

This framework will be reviewed every three years, unless the introduction of any new or amended relevant legislation or policies warrants an earlier review.

7.0 Communication anad Implementation Plan

All GGC policies nd guidelines are available on StaffNet. All WoSCAN policies and Standard Operating Procedures are available in the WoSCAN network folder.

Relevant Legislation Appendix 1

Computer Misuse Act (1990)	Created to criminalise unauthorised access to computer systems and to deter the more serious criminals from using a computer or the data it stores by inducing a computer to perform any function with intent to secure access. The Act has been modified by the Police and Justice Act 2006.
Copyright, Designs and Patents Act 1988	Grants the creators of original works exclusive rights to control the ways in which their material may be used.
UK General Data Protection Regulation	The main piece of legislation that governs protection of personal data in the UK. It provides a way that individuals can enforce the control of information about themselves.
Electronic Communications Act (2000)	Gives legal recognition for electronic signatures and makes it simpler to amend existing legislation that could hamper the development of internet services.
Freedom of Information (Scotland) Act (2002)	Provides the right of access to recorded information of any age held by public sector bodies in Scotland. There is a duty on all local authorities to adopt and maintain a publication scheme approved by the Scottish Information Commissioner.
Human Rights Act (2000)	Governs interception or monitoring of communications, most specifically article 8 which guarantees respect for an individuals' private and family life, their home and correspondence. Public authorities cannot interfere with these rights unless it's justifiable to do so.
Privacy and Electronic Communication (EC Directive) Regulations (2003)	Replacing the Telecommunications (Data Protection and Privacy) regulations 1999 and amendments 2000, these cover a range of issues relating to privacy in respect of electronic communications including telemarketing and cookies.
Public Records (Scotland) Act 2011	Makes provision about the management of records held by public authorities, including the creation of a records management plan.
Regulation of Investigatory Powers Act (2000)	Aims to ensure that various investigatory powers available to public bodies are only exercised in accordance with the Human Rights Act 1998. The Act legislates for using methods of surveillance and information gathering to help the prevention of crime and terrorism.

Appendix 2

WoSCAN Policies and Standard Operating Procedures (SOPs)
WoSCAN Audit Governance Process
WoSCAN Information Request Process
WoSCAN Internal Audit Governance SOP WoSCAN
Website Management Policy
eCASE Governance Framework

NHSGGC Information Governance Policies and Guidelines

• **Information Governance Policies/Guidance**
Clear Desk Policy
Confidentiality and Data Protection Policy
Data Breach Policy
Faxing Policy
Subject Access Policy
Information Sharing Agreement Template
NHS Scotland Code of Practice: Protecting Patient Confidentiality
Data Protection Impact Assessment Template

• **IT Security Policies/Guidance**
Acceptable Use Policy
IS Policy 1 Governance
IS Policy 2 Risk Management
IS Policy 3 Information Security
IS Policy 4 ISMS
IS Policy 5 Organisation
IS Policy 6 Human Resources
IS Policy 7 Asset Management
IS Policy 8 Access Control
IS Policy 9 Cryptographic
IS Policy 10 Physical and Environmental
IS Policy 11 Operations Security
IS Policy 12 Communications
IS Policy 13 Data Transfer
IS Policy 14 System Acquisition
IS Policy 15 Supplier Relationships
IS Policy 16 Incident Management
IS Policy 17 Business Continuity
IS Policy 18 Compliance
Email Usage Policy
Third Party Access Policy
Internet Acceptable Use Policy
Network Account Deletions Policy
Mobile Devices and Teleworking

• **Corporate Records**

Access Protocol for the Emergency Care Summary System
Guidance on the use of the CHI
Scottish Government Health & Social Care Records Management Code of Practice (Scotland)

• **Strategies**

Information Governance Strategy