The World Health Net

# Information Governance

# Information Governance Policy

Policy Reference: TWHN/IG/IGP V1.1

| | | |
|---|---|---|
| **Policy Title** | Information Governance Policy | |
| **Author/Contact** | Holly Hellstrom – Information Assurance Director | |
| **Document Ref** | TWHN/IG/IGP | |
| **Version** | 1.1 | |
| **Status** | Approved | |
| **Publication Date** | January 2022 | |
| **Review Date** | January 2024 | |
| **Approved by** | Mrs Holly Hellstrom – IG Lead<br>Dr Javed Mohungoo SIRO | 26th January 2022 |
| **Ratified by** | Information Governance Team | 26th January 2022 |

| Version | Date | Comments | Author | Notes |
|---|---|---|---|---|
| 1 | 7/1/2020 | Approved by IGT | Information Assurance Director | |
| 1.1 | 26/1/22 | Approved by IGT | Information Assurance Director | Added aims<br>Changed UKGDPR<br>Caldicott eight principles<br>Use of data |
| | | | | |

## Table of Contents

## Introduction

Information Governance ensures necessary safeguards for, and appropriate use of, patient and personal information. Information is a vital asset, both in terms of the management of individual patients and the efficient management of the service and resources. It plays a key part in governance, service planning and performance management and decision-making. It is therefore of paramount importance that information is effectively managed with appropriate policies and procedures in place, and that management accountability is identified to provide a robust information governance framework to support the organisation. The company Information Governance Policy is built on the work carried out in relation to the Information Governance agenda, including Information Quality Assurance, the Caldicott, Data Protection and Information. Information governance needs to be allied closely with advice and guidance and also includes initiatives such as Confidentiality: NHS Codes of Practice, The Freedom of Information Act 2000, Data Protection act 2018 and the UK General Protection Regulation and has been established in line with work carried out by the DSP. The Information Governance Lead within The World Healthnet (WHN) is via the Information Governance team which meets on a bi-monthly basis and includes the Caldicott Guardian.

The aims of this policy are;
To maximise the value of organisational assets by ensuring that data is:

- Held securely and confidentially;
- Obtained fairly and lawfully;
- Recorded accurately and reliably;
- Used effectively and ethically; and
- Shared and disclosed appropriately and lawfully.

To protect the organisation's information assets from all threats, whether internal or external, deliberate or accidental. The organisation will ensure:

- Information will be protected against unauthorised access;
- Confidentiality of information will be assured;
- Integrity of information will be maintained;
- Information will be supported by the highest quality data;
- Regulatory and legislative requirements will be met;
- Business continuity plans will be produced, maintained and tested;
- Information security training will be available to all staff; and

- All breaches of information security, actual or suspected, will be reported to, and investigated.

## Objective

This document will detail the processes that must be adhered to in ensuring that Information Governance is maintained within the World Health Net comply with all guidance and legislation relating to this area. This policy will be reviewed every two years or should there be any major legislation changes.

## Scope of Policy

This policy applies to all staff employed by World HealthNet, including bank, agency and locum staff, students, voluntary staff, contractors and trainees on temporary placement.

## Policy

World HealthNet recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. World HealthNet is accountable and needs to ensure that the principles of corporate governance are fully supported. An equal importance must be placed on the need to ensure high standards of information assurance, data protection and confidentiality to safeguard personal and commercially sensitive information. World HealthNet also recognises the need to share information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and in some circumstances, the public interest. Underpinning this is the need for information to be accurate, relevant, available when required and processed appropriately, and measures must be taken to keep in line with the information security agendas to safeguard personal data.

There are 4 key interlinked areas within Information Governance:

## Protection of Information

This includes the implementation and maintenance of standards associated with the Data Protection Act, the Freedom of Information Act, Information Security Management: NHS Code of Practice, the Confidentiality: NHS Code of Practice and the Caldicott eight principles. There is a high overlap with the Lifecycle & Records Management Policy that details the requirements for record retention and destruction.

In order to ensure high standards in this area:

- WHN will establish and maintain policies and procedures to ensure the implementation of the Data Protection Act 2018, UKGDPR, Freedom of Information Act 2000, The Computer Misuse Act 1990, and any further related legislation and NHS guidance for the effective and secure management and processing of its information, it's information assets and resources
- WHN will undertake or commission annual assessments and audits of its levels of protection of information using the DSP Toolkit
- WHN will promote effective confidentiality, data protection and security practice to staff through policies, procedures and various methods of training
- WHN will ensure information assets are obtained and documented throughout the organisation.

- WHN will deliver a confidentiality and security work Programme in line with the DSP Toolkit.
- WHN will establish and maintain protocols for the controlled and appropriate sharing of personal information with other agencies, taking account of relevant legislation.

### Management of Records

There is a high level of overlap with the Protection of Information and with Lifecycle and Record Management Policy. In order to ensure high standards in this area:

- WHN will establish and maintain policies and procedures to ensure compliance with the Data Protection and Freedom of Information Act, any further related legislation.
- WHN will undertake or commission annual assessments and audits of its policies and arrangements for openness and records management using the DSP Toolkit and other available mechanisms
- WHN will have a strategy for dealing with Records Management with their partners
- WHN will promote effective records management to staff through policies, procedures/user manuals and training.

### Information Quality Assurance

This includes the implementation of information quality standards for electronic and manual patient/staff information. It has a high level of overlap with Protection of Information and with Management of Records.

In order to ensure high standards in this area:

- WHN will undertake or commission annual assessments and audits of its information quality using the DSP Toolkit and other available mechanisms.
- WHN will promote information quality to staff through policies, procedures/user manuals and training.

### Risk

WHN will ensure that it operates within a robust Information Governance framework to reduce the risk of both potential litigation and compromise to patient care. Risk assessments will be carried out in the individual component areas as required by the DSP Toolkit.

### Roles and Responsibilities

The SIRO is the named director with responsibility and this policy has been ratified by the IG team.

The Information Assurance Director is responsible for ensuring the policy and its supporting standards and guidelines are built into the local processes and that there is ongoing compliance.

It is the responsibility of all staff to familiarise themselves with this policy and all related Informatics policies and documentation where applicable. Staff must ensure at all times that high standards of information quality, data protection, integrity,

confidentiality and records management are met in compliance with the relevant legislation. All staff must promote high standards of Information Governance.

### Training & Resources

The implementation of policies in this area will be carried out across the organisation by all involved staff and will be led by the Information Assurance Director/ IG Lead & Caldicott Guardian. Information Governance elements will be included in standard induction, mandatory training programmes, specific data protection training packages and electronic learning packages. Managers will ensure that the relevant paragraphs are included in staff job descriptions.

### Monitoring and Audit

The Information Governance team is the organisations committee with responsibility for the ratification of Information Governance Policies and approval of work programmes. It receives regular reports from the Information Assurance Director and responsible staff dealing with all aspects of the agenda as outlined above, and approves central returns required by the DSP Toolkit. The DSP Toolkit will be used by the company to conduct baseline audit and construct action plans for future compliance with this agenda.

### Incident Reporting

WHN has a robust Information Incident Reporting Procedure in place. All actual or potential breach of confidentiality and information security must be reported to the Information Governance Team on 01482 908208 option 5.

### Awareness

WHN will use staff share-point in the HRFile on the World Healthnet platform, newsletters and training in sessions to advise staff of information governance.

### Associated documentation and references

This policy should be read in conjunction with all Informatics policies, which include:

- Information Access & Security Policy
- Information Incident Reporting Procedures
- Password Policy
- Data Protection & Confidentiality Policy
- Records Management & Lifecycle Policy
- Sending and Transferring Information Securely

Legislation to restrict disclosure of personal identifiable information:

- The Freedom of Information Act 2000
- The General Data Protection Regulation 2018
- The NHS Code of Confidentiality
- UK General Data Protection Regulation