NHS
Urgent Care 24
safe • caring • effective

Information Governance Framework

Version	1.3
Location	Policy Folder – Information Governance
Approving Committee:	Leadership Team
Date Ratified:	March 2017 (this version)
Reference Number:	UC24POL7
Name/Department of originator/individual:	Margaret Swinson Information Governance Lead
Name/Title of responsible committee/individual:	Information Governance Steering Group
Date issued:	March 2015
Review date:	November 2017
Target audience:	All employees, Associate GPs

Version	Date	Control Reason
1.1	November 2012	Framework re-formatted to reflect changes to job roles and responsibilities.
1.2	February 2014	Changes to roles and responsibilities
1.3	February 2017	Updated by IG lead to reflect changes in roles and responsibilities and new policies

Contents

1.0 INTRODUCTION

The availability of reliable information is an essential element in the delivery of appropriate and effective healthcare. It is used in the use of:

- Management of individual patient/client care
- Efficient management of services and resources
- Monitoring of the organisation's performance
- Day to day running of Urgent Care 24

Information Governance is a framework that enables Urgent Care 24 to:

- Establish good practice around the handling of information
- Promote a culture of awareness and improvement
- Comply with legislation and other mandatory standards

This Information Governance framework identifies how the organisation will meet the key requirements of a wide range of Information Governance related matters.

2.0 AIM

The purpose of this framework is to set out and promote a culture of good practice around the processing of information and use of information systems that supports the provision of high quality care to users of our services. To ensure that information is handled to ethical and quality standards in a secure and confidential manner. Urgent Care 24 requires all employees to comply with the extant Policies, Procedures and Guidelines which are in place to implement this framework.

3.0 LEGISLATION

There are several acts and national guidance that Information Governance abides by. These include:

- The Public Records Act 1958
- The Data Protection Act 1998
- The Freedom of Information Act 2000
- The Computer Misuse Act 1990
- The Common Law Duty of Confidentiality
- The NHS Confidentiality Code of Practice
- Mental Capacity Act 2005
- Records Management: NHS Code of Practice
- Caldicott Guidance

- Current Performance Standards (NHS IG Toolkit)
- Copyright, Designs and Patents Act 1988

4.0 SCOPE

This framework covers the following for Urgent Care 24:

Systems – All Information Systems with within the Organisation (both electronic and paper based) fall within the scope of this framework. Urgent Care 24 Information systems include Patient Information Systems, Finance, Risk, Human Resources and Payroll databases.

Staff – All users of Urgent Care 24 information and /or systems including Urgent Care 24 employees and non-Urgent Care 24 employees who have been authorised to access and use such information and / or systems.

Information – All information and data collected or accessed in relation to any Urgent Care 24 activity whether by Urgent Care 24 employees or Associates and organisations under a contractual relationship with Urgent Care 24. All information stored on facilities owned or managed by the organisation or on behalf Urgent Care 24. All such information belongs to Urgent Care 24 unless proven otherwise.

5.0 POLICIES

Urgent Care 24 will have the following policies which will be available on the organisation's intranet:

- Information Risk Policy
- Confidentiality, Data Protection & Caldicott Policy
- Email and Internet Policy
- Remote Working and Mobile Devices Policy
- Records Management Policy
- Information Security Policy
- Information Governance Corporate Policy and Strategy
- Policy for Managing Incidents and Serious Incidents
- Change Control Procedure
- Information Asset Policy
- Forensic Readiness Policy

6.0 PROCEDURES AND GUIDELINES

The organisation will achieve implementation of the policies through detailed Procedures and Guidelines for staff as appropriate and required.

7.0 IMPLEMENTATAION AND RESPONSIBILITIES

The Information Governance Steering Group leads on the implementation of this framework and related policies. Progress, review and issues are reported to the Urgent Care 24 Board via the Quality & Workforce Committee.

The Chief Executive

The Chief Executive has the ultimate responsibility for compliance with the Data Protection Act 1998 within UC24.

Information Governance Lead (IG Lead)

The Company Secretary is the Information Governance Lead and is responsible for overseeing completion of the Department of Health's Information Governance Toolkit, including those elements pertaining to confidentiality and data protection.
The Company Secretary will:

- Lead the co-ordination and implementation of the Data Protection and Confidentiality work programme, chairing the Information Governance Steering Group
- Monitor and ensure UC24's compliance with the principles contained within the Data Protection Act (1998), Caldicott Report and Confidentiality: NHS Code Of Practice
- Oversee the provision of adequate training and awareness of all staff in relation to their responsibilities for Data Protection and Confidentiality, including specialist training in relation to their role as IG Lead
- Ensure that Information Asset Owners are identified, are aware of their areas of responsibility and attend the Information Governance Steering Group.

Senior Information Risk Owner (SIRO)

The Director of Finance is the UC24 SIRO. The responsibilities of this role are:

- To ensure that UC24 achieves monitors and embeds a culture of good information governance, across the organisation and with its business partners
- To work closely with the IG Lead and the Caldicott Guardian
- To attend the Information Governance Steering Group
- To complete appropriate specialist training for this role

- To understand the organisation's business goals with particular emphasis on the use of, and dependency upon internal and external information assets
- To ensure UC24's Information Asset Owners (IAOs) understand their role
- To initiate and oversee an information risk awareness/training programme and to communicate the importance and maintain impetus on identifying and managing information risk
- To ensure that good information governance assurance practice is shared within UC24 and to learn from good practice developed and practiced within the NHS locally and nationally.

Caldicott Guardian

This role is undertaken by the Director of Patient Quality & Safety. The Caldicott Guardian is responsible for agreeing and reviewing processes and procedures governing the transfer and disclosure of personal confidential data within UC24 and with external agencies. They will:

- Develop and maintain knowledge of confidentiality and data protection matters and act as the organisational expert on confidentiality
- Ensure the Caldicott work plan is incorporated into the IG Framework, which will be managed through the Information Governance Steering Group
- Ensure that the Caldicott principles are appropriately reflected in organisational strategies, policies and working practices for staff
- Undertake appropriate specialist training for their role
- Attend the Information Governance Steering Group
- Be the first point contact within UC24 for data protection and Caldicott issues
- Work closely with the IG Lead and when information owned by UC24 needs to be transmitted to an external agency
- Ensure adequate governance over the issuing of Smartcards by the Registration Authority
- Oversee patient information audit.

Information Governance Steering Group

The Information Governance Steering Group is chaired by the IG Lead. The group is responsible for:

- Ensuring that UC24 complies with the Data Protection Act 1998, ongoing NHS guidance and mandatory requirements in relation to Information Governance
- Progressing and embedding information governance processes at UC24
- Allocating appropriate IG indicators and work streams to the appropriate personnel

- Developing and monitoring action plans supporting the development of good practice at UC24
- Ensuring all staff receive training in IG appropriate to their roles and responsibilities
- Discussing matters of concern in relation to IG
- Keeping IG policies and Standard Operating Procedures, including this policy, under review
- Monitoring the outcomes of Information Asset Risk assessments and audits.

All Managers

All managers are responsible for ensuring compliance with policies, that their staff successfully undertake annual mandatory IG training and that IG breaches are properly recorded through the Datix system.

Information Asset Owners

IAO's are Data Custodians, as referred to in the DPA and are responsible for ensuring that the data protection and Caldicott Principles are fully observed and complied with by staff within their department or Service Delivery Unit (SDU). IAOs are required to ensure that all data flows and processing of data, for which they are responsible, complies with UC24 Information Governance policies. To this end they will:

- Promote Data Protection and Caldicott Principles on an on-going basis, including posters, articles and local briefings
- Support managers with local induction for new starters and temporary staff to ensure they are given instruction on the Data Protection and Caldicott principles as part of their first week/day
- Ensure all staff know the procedure for reporting IG and IT security incidents
- Be the lead individuals for the completion of their particular aspects of the IG Toolkit
- Attend meetings of the Information Governance Steering Group.

IT Manager

The IT Manager has a particular role in respect of the interface between Information Management & Technology, and the information handled and stored by UC24. The IT manager will:

- Provide an advisory service to the IG group and team
- Monitor and report on the state of Information Management & Technology security within the organisation
- Ensure the Information Security Policy and all Information Technology policies are maintained, up to date and implemented throughout the organisation
- Lead on issues with regard to Cyber Security issues
- Be the lead individual for the completion of the relevant aspects of the IG Toolkit

- Attend the Information Governance Steering Group.

Responsibilities of all UC24 staff

- Everyone working in the NHS has a legal duty to keep information about patients, clients and other individuals such as staff or volunteers confidential, and to protect the privacy of individuals. They are required to adhere to confidentiality agreements i.e. common-law of confidentiality, contract of employment, NHS Confidentiality Code of Practice
- UC24 places the utmost importance upon patient confidentiality
- UC24's patient confidentiality guidance is governed by the NHS Caldicott rules. The Director of Quality & Patient Safety is the designated Caldicott Guardian with responsibility for ensuring adherence to these guidelines
- All UC24 staff and visitors are required to sign a confidentiality agreement on commencement of employment with UC24 or on visiting the premises
- In the course of their work UC24 staff may be called upon to handle and process patient-identifiable information whether it is stored on paper or on computer. They are responsible for safeguarding the confidentiality of all personal and corporate information, transmitted or recorded by any means. Such information must not be disclosed, except to authorised personnel
- All notes, memoranda, records and other material in permanent form made or created by UC24 staff relating to the business of UC24 in pursuance of their duties (including all copies) shall be and remain the property of UC24 and must be handed over on demand and in any event at the end of the employment, term of office or contracting relationship
- UC24 staff must not at any time, either during employment, term of office or contracting relationship, or afterwards, use, or divulge to any person, firm or company, except in the proper course of their duties, confidential information relating to the business of any patient or customer of UC24 which may have come to their knowledge as a result of their relationship with UC24
- UC24 staff must not use or divulge any information, relating to or concerning UC24, details of patients, general practitioners, or suppliers of UC24, or any computer programmes and related manuals or documentation, the intellectual property rights of which belong to UC24, or the prices charged or quoted by any such suppliers which they may possess or which may come to their knowledge
- UC24 staff must keep confidential all information entrusted to them which they know, or ought reasonably to know, to be confidential or secret, and not use or attempt to use any such information which they know, or ought reasonably to know, to be confidential or secret, in any manner which may injure or cause loss either directly or indirectly to UC24 or its patients, or may be likely to do so. This restriction will continue to apply at the end of the formal relationship with UC24, save to the extent that any such confidential information shall have come into the public domain.

8.0 TRAINING

As part of the UC24 mandatory training programme, each member of UC24 staff will undertake Information Governance training using the approved training tool, on an annual basis. This training will be recorded by the training department. Managers have a responsibility to ensure all their staff are up to date with mandatory training requirements and that additional training needs, related to particular responsibilities, are agreed as part of the Appraisal process. See Training Needs Analysis in **Appendix 1.**

Policies and procedures supporting Data Protection and Confidentiality are available and accessible on the local UC24 intranet.

9.0 INCIDENT MANAGEMENT

Information Governance incidents must be reported on the Datix system and managed in accordance with the Policy for the Management of Incidents and Serious Incidents.

10.0 COMPLIANCE AND EFFECTIVENESS

The compliance and effectiveness of this policy will be monitored by a combination of:

- Analysis of incidents and reported breaches to identify common themes of failure in process or procedure
- Audits at Wavertree HQ and at Urgent Care Centres to assess the adequacy of information security measures and staff understanding of their responsibilities relating to Data Protection and Confidentiality
- The work of the Information Governance Steering Group
- The annual review of Information Governance compliance through completion of the IG Toolkit.
- Completion and review of Privacy Impact Assessments
- Annual Information Governance mandatory training for all staff
- Annual performance review of all staff.

11.0 REVIEW

This framework will be reviewed in November 2017 or when changes are required if sooner.

APPENDIX 1 Training Needs Analysis

Training requirement	Frequency	Course length	Delivery method	Facilitators	Recording Attendance	Strategic & Operational Responsibility
Information Governance	On appointment	N/A	e-learning	N/A	Training Dept.	
Information Governance Refresher	Annually	N/A	e-learning	N/A		
Senior Information Responsible Owner Training	Annually					
Information Asset Owner	Annually					
Caldicott Training	Annually					
Staff Groups	**Target Audience**					
Out of Hours Urgent and Community services	All staffing					
Corporate	All staffing					
NHS 111	All staffing					
SIRO	Yes					
Information Governance Lead	Yes					
Information Asset Owners	Yes					