Working with you to make Sheffield HEALTHIER

NHS Sheffield Clinical Commissioning Group

Information Security Policy

November 2021

Version:	7.0
Date ratified:	31 August 2021
Policy Number	CO013/06/2022
Name of originator/author:	IG Manager
Name of Sponsor:	Deputy Director of Performance, Information, Performance and PMO
Name of responsible committee	Governance Sub-committee
Date issued:	November 2021
Review date:	30 June 2022
Target audience:	All staff working within or on behalf of NHS Sheffield CCG

To ensure you have the most current version of this policy please access via the NHS Sheffield CCG Intranet Site by following the link below:

http://www.intranet.sheffieldccg.nhs.uk/policies-procedure-forms-templates.htm

disability confident EMPLOYER

MINDFUL EMPLOYER

Policy Audit Tool

To be completed and attached to any document which guides practice when submitted to the appropriate committee for consideration and approval.

Please give status of Policy: Revised

1.	**Details of Policy/Procedural Document**	
1.1	Policy No:	CO013/06/2022
1.2	Title of Policy/document:	Information Security Policy
1.3	Sponsor	Information Governance Group
1.4	Author:	Gershon Nubour, IG Manager
1.5	Lead Committee	Governance Sub-committee
1.5	Reason for policy/document:	
1.6	Who does the policy affect?	All CCG Staff
1.7	Are the National Guidelines/Codes of Practice etc issued?	
1.8	Has an Equality Impact Assessment been carried out?	Yes
2.	**Information Collation**	
2.1	Where was Policy information obtained from?	Existing policy
3.	**Policy Management**	
3.1	Is there a requirement for a new or revised management structure for the implementation of the Policy?	No
3.2	If YES attach a copy to this form.	
3.3	If NO explain why.	
4.	**Consultation Process**	
4.1	Was there external/internal consultation?	No
4.2	List groups/persons involved	
4.3	Have external/internal comments been included?	
4.4	If external/internal comments have not been included, state why.	
5.	**Implementation**	
5.1	How and to whom will the policy be distributed?	Intranet
5.2	If there are implementation requirements such as training please detail.	
5.3	What is the cost of implementation and how will this be funded	
6.	**Monitoring**	
6.1	How will this be monitored	Number of adverse incidents reported. Number of complaints received.
6.2	Frequency of Monitoring	Annually

Version Control

VERSION CONTROL				
Version	Date	Author	Status	Comment
1.0	July 2014	Information Governance Group		
2.0	July 2016	EMBED IG Team	Review	Footnotes rationalised Information Ownership statement removed from 3.3 Added requirement to not leave confidential info in cars Added requirement to guard against lost, theft and inappropriate access when working remotely CSU references changed to EMBED Additional minor corrections *Note sections 4.4.5-4.4.7 will be updated / added when the "Remote Working & Portable Devices Policy" has been finalised.*
3.0	October 2017	EMBED IG Team		Amended in line with GDPR, NHS Cyber Security Standards.
4.0	November 2019	EMBED IG Team/NHS Sheffield CCG	Review	Minor corrections and amendments
5.0	December 2019	Sheffield CCG IG Team	Review	Included details of how temporary IT access is monitored. Amendments made as part of the review process.
6.0	Jan 2021	Sheffield CCG IG Team	Review	Updated Reference to UK-GDPR Added Reference to new Network Security Policy Explicitly stated that suspicious behaviour is now monitored
7.0	Nov 2021	Sheffield CCG IG Team	Review	No significant changes

Contents

1. Introduction & Purpose

The objective of information security is to protect the CCG's information assets[1] from a wide range of threats, whether deliberate or accidental, internal or external, in order to ensure business continuity and minimise the impact of adverse events on patients, staff and the CCG. Information security is achieved through the implementation of controls and procedures that ensure the secure use of information and the identification and effective management of risk. This policy should be cross-referenced with other information governance and procedural documents. An up-to date list of documents is available on the CCG intranet page. Staff should ensure that they are familiar with the content of this policy.

The purpose of this policy is to enable the CCG to protect its information assets by:

- Setting out a framework for information security
- Promoting a culture of information security within the CCG and
- Ensuring staff understand their responsibilities in relation to information security

The information security policy will ensure that:

- The CCG has a board approved Senior Information Risk Owner (SIRO).
- Each Information Asset has a responsible owner (Information Asset Owner).
- Information is protected against unauthorised access and/or misuse.
- The confidentiality of information is assured.
- The integrity of information is maintained.
- Information is available when required.
- Business continuity plans are produced, maintained and tested.
- Regulatory, legal and contractual requirements are complied with appropriate training around information governance (IG) and data security is provided for and completed by all staff.
- All breaches of information security, actual or suspected are reported immediately and investigated through the appropriate management channels (see section 4.8).

Controls and procedures will be produced to support this policy and implement the framework.

2. Scope

This policy applies to the following areas:

2.1 Systems

- All manual and electronic information systems owned, operated or managed by the CCG, including networks and application systems, whether or not such systems are installed or used on CCG premises.
- Other systems brought onto CCG premises including, but not limited to, those of contractors and 3rd Party suppliers, which are used for CCG business.

[1] An Information asset is any formal business system which holds or comprises information or is used to support the processing of such information. It may be electronic or paper-based in nature.

2.2 Users

- All users of CCG information and/or systems including CCG employees and non-CCG employees who have been authorised to access and use such information and/or systems.

2.3 Information

- All information collected or accessed in relation to any CCG activity whether by CCG employees or individuals and organisations under a contractual relationship with the CCG.
- All information stored on facilities owned or managed by the CCG or on behalf of the CCG.

2.4 Contracts of Employment

- Security requirements are addressed at the recruitment stage and all contracts of employment contain a clause relating to confidentiality and data protection.

3. Roles & Responsibilities

Management of, and Responsibility for, Information Security

- The Accountable Officer has ultimate responsibility for information security within the CCG. This is delegated to the Senior Information Risk Owner.
- The CCG's Senior Information Risk Owner is responsible for implementing, monitoring, documenting and communicating information security requirements for the CCG.
- Departmental and line managers are responsible for information security within their areas and for ensuring their staff, whether permanent, temporary or contractors, are aware of this policy and associated procedures and their duty to comply – Each Information Asset will have an identified responsible owner (Information Asset Owner).
- Individuals have a personal responsibility for adhering to this policy and associated procedures.
- Failure to comply with the policy and associated procedures may have serious consequences for the individual including civil, criminal and disciplinary proceedings.
- The IG Team and IT Service desk will provide specialist advice as required on IT security issues.

4. Process/Requirements

4.1 Information Security Awareness Training

- Annual online Data Security Awareness Training is mandatory for all staff. Line managers must ensure that staff complete more advanced information security modules or receive external training where appropriate for their role and responsibilities.
- The IG Team will support the provision, either internally or externally, of specialist training for roles such as the SIRO, Caldicott Guardian and Information Asset Owners

4.2 Information Security Procedures

- The security of paper and electronic records, computers and networks is controlled by procedures that have been agreed with the relevant service leads, heads of departments or the IG Group

Areas of information security covered include, but are not limited to:

4.3 Security of Equipment and Records

- In order to minimise loss of, or damage to, all assets, all equipment and information storage areas are physically protected from security threats and environmental hazards.
- Confidential information and laptops must not be visible in unattended cars; left in cars overnight; or for extended periods of time.
- Confidential information held in hard copy (paper) must be kept secure at all times.
- Confidential CCG information must not be stored on local hard drives such as PCs, laptops or other mobile devices unless authorised by the CCG IG Lead or SIRO.
- All portable devices must be encrypted.
- Databases of personal, service user information or staff information, must not be created without prior permission from the CCG IG Lead, through the submission of a Data Protection Impact Assessment (DPIA).
- Current databases of personal information must be recorded on the CCGs Information Asset register and the CCG IG Lead notified.
- Patient Confidential Data sourced from NHS Digital is managed according to Data Sharing Agreements between the CCG and NHS Digital. Data management, including DSCRO services, (provided by the North of England Commissioning Support Unit at the time of writing) will be covered by contract.
- The use of internet hosted services to store or process confidential / personal information requires prior approval of the IG Group or SIRO. Risk assessments and DPIAs will be required for any such proposals.

4.4 Location Access Controls

- Only authorised personnel who have an identified need are given access to restricted areas containing information systems such as server rooms.

4.5 User Access Controls

- Access to information and information systems, whether electronic or manual, is restricted to authorised users who have an identified need as agreed with their line manager or sponsor.
- Access to electronic information systems is given at the appropriate level for the agreed need.
- Electronic Personal Confidential Data may only be stored within “live” operational systems.
- A limited number of named staff may have access to confidential data in line with the arrangements agreed for processing of data to support essential secondary functions of the CCG. They may also process personal data on behalf of other organisations under agreement. This will be managed and authorised in

accordance with legislation, statutory regulations and any applicable data processing agreements.

- Dormant or unused accounts will be disabled and deleted by the IT team after an agreed period of time
- Controls will be implemented to restrict simultaneous logins and repeated login attempts
- Systems are in place that can alert to and restrict suspicious and excessive use of CCG IT resources

4.6 Information Communication Technology (ICT) Access Controls

- Access to ICT equipment, for example, PCs and terminals is restricted to authorised users who have an agreed requirement to use those facilities.

4.7 Connection to the CCG Network

- All devices connected to the CCG network are governed by the Network Security Policy and the HSCN Connection Agreement, in line with rules set out by the NHS Digital.
- The connection of any equipment to the internal CCG network requires authorisation from the IT department.
- Personally owned devices – Their use within the CCG is governed by the Remote Working & Portable Devices Policy which details accepted practice for CCG staff. Please see this policy for information relating to non-CCG equipment.
- External visitors may connect to the internet temporarily, via a Guest Wi-Fi account.

4.8 Definitions

Remote Working

- Access to the CCGs information and IT resources away from the CCG's premises is governed by this policy, the Remote Working & Portable Devices Policy" as well as the "Confidentiality Code of Conduct".

Portable Devices

- The use of portable devices is governed by the "Remote Working & Portable Devices Policy". This contains details of expected behaviour for all staff when using portable devices such as memory sticks, laptops and smartphones.
- The prime requirement however for all portable devices, is that they must be encrypted to protect confidential information held on them.

4.9 Temporary Staff

- Managers are responsible for requesting user accounts for temporary staff.
- Managers must ensure that staff are inducted, appropriately trained and supervised.
- When staff leave / come to the end of their contract, Managers must follow agreed processes with the IT Team in closing accounts and removing access.
- Any account which is dormant for over 90 days will be automatically suspended.
- An account which has been suspended for a further 9 months, maybe automatically deleted
- The CCG IG Team will work with the IT Team to review all User Accounts on a regular basis.

4.10 Visitors

- Physical Security - Visitors will be required to sign into and out of the building.
- File access - Visitors will be enabled to access to their own systems only via secure VPN connectivity over guest WiFi
- Internet Access - Visitors will only be allowed guest WiFi access.
- CCG files access – If the CCG requires a visitor to have access to CCG files then appropriately managed secure arrangements will be put in place on a case by case basis.

4.11 Unsupported Systems, Software and Updates

- No unsupported, or out of warranty systems; operating systems; software or applications shall be used for CCG business without permission of the SIRO.
- All operating systems and applications used for CCG business must be kept up to date using available and appropriate software updates.

4.12 Monitoring System Access and Use

- Audit trails of system access and use are maintained and reviewed on a regular basis. They will also be used to investigate any potential concerns that require further investigation.

4.13 Business Continuity

- The CCG will ensure that business continuity and disaster recovery plans are produced for all critical information, applications, systems and networks.

4.14 Reporting Security Incidents and Weaknesses

- All information management and information security (Cyber) incidents and weaknesses must be reported immediately in line with the CCG Incident Reporting Policy.
- Incidents that present an immediate risk to the CCG such as viruses should also be reported to the IT Service Desk immediately.

- Information Security Incidents, especially those involving the loss of sensitive or confidential data, or any incident involving unencrypted portable devices may need to be reported as a Serious Incident and/ or to the Information Commissioner via the Data Security and Protection Toolkit reporting system. See the Incident Reporting policy for more details.
- There is a legal requirement to report any such serious incidents to the authorities within 72 hours of being identified.

4.15 Assurances from IT Services

- The CCG will obtain regular assurance from the IT Service and Core IT providers that CareCert Alerts are being acted upon and are being addressed appropriately

5 Monitoring effectiveness of the policy/procedural document

Reporting to the Information Governance Group

- The Information Governance Manager will keep the Information Governance Group and/ or Governance Sub-Committee informed of the information security status of the CCG by means of automated incident reports to the CCG IG Lead and the IG team.
- It is the responsibility of the SIRO to bring information security risks or incidents to the attention of the Governing Body.

6 Review

This document may be reviewed at any time at the request of either staff side or management but will automatically be reviewed after twelve months and thereafter on a bi-annual basis or when a change in legislation dictates.

7 References and links to other documents

Legislation and Guidance

The CCG and its employees, including non-CCG employees authorised to access CCG information and systems, are obliged to comply with the legislation and national guidance including, but not limited to:

- CCG Network Security Policy
- Common Law Duty of Confidentiality
- Data Protection Act 2018
- UK General Data Protection Regulation
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Protection of Freedoms Act 2012
- Health and Social Care Act 2012
- Regulation of Investigatory Powers Act 2000
- Copyright, Designs and Patents Act 1998
- NHS Code of Connection

- Confidentiality: NHS Code of Practice
- Records Management: NHS Code of Practice
- HSCIC Guide to Confidentiality in Health and Social Care
- Caldicott Guidance

And any relevant guidance related to the following:

- Information Quality Assurance
- Information Security
- Information Governance Management
- National systems

8 Equality & Diversity Statement

NHS Sheffield CCG aims to design and implement services, policies and measures that meet the diverse needs of our service population and workforce, ensuring that none are placed at a disadvantage over others. It takes into account the Human Rights Act 1998 and promotes equal opportunities for all. This document has been assessed to ensure that no-one receives less favourable treatment on grounds of their gender, sexual orientation, marital status, race, religion, age, ethnic origin, nationality, or disability. Members of staff, volunteers or members of the public may request assistance with this policy if they have particular needs. If the person requesting has language difficulties and difficulty in understanding this policy, the use of an interpreter will be considered.

NHS Sheffield CCG embraces the six staff pledges in the NHS Constitution. This policy is consistent with these pledges.

9 Disability Confident

NHS Sheffield CCG has been accredited with the Disability Confident Award – level 1. This is in recognition of meeting the commitments regarding employment of disabled people and permits the organisation to use the Disability Confident logo on all of its stationery. The Disability Confident symbol should be added as a footer to all policies / procedural documents.

NHS Sheffield Clinical Commissioning Group

NHS Sheffield CCG Equality Impact Assessment 2016

Equality Impact Assessment

Title of policy or service:	Information Security Policy	
Name and role of officer/s completing the assessment:	Sandie Buchan, Deputy Director of Commissioning & Performance (SCCG) Gershon Nubour, Information Governance Manager (eMBED)	
Date of assessment:	26st January 2021	
Type of EIA completed:	**Initial EIA 'Screening'** ☒ ***or*** **'Full' EIA process** ☐	**Type of EIA completed:**

1. Outline	
Give a brief summary of your policy or service • Aims • Objectives • Links to other policies, including partners, national or regional	Informs staff on how the organisation manages Information Security and informs them of their responsibilities to keep information secure Links to other policies are within the policy

Identifying impact:

- **Positive Impact:** will actively promote or improve equality of opportunity;
- **Neutral Impact:** where there are no notable consequences for any group;

- **Negative Impact:** negative or adverse impact causes disadvantage or exclusion. If such an impact is identified, the EIA should ensure, that as far as possible, it is justified, eliminated, minimised or counter balanced by other measures. This may result in a 'full' EIA process.

2. Gathering of Information
This is the core of the analysis; what information do you have that might *impact on protected groups, with consideration of the General Equality Duty*.

	What key impact have you identified?			For impact identified (either positive an or negative) give details below:	
(Please complete each area)	**Positive Impact**	**Neutral impact**	**Negative impact**	**How does this impact and what action, if any, do you need to take to address these issues?**	**What difference will this make?**
Human rights	☐	☒	☐		
Age	☐	☒	☐		
Carers	☐	☒	☐		
Disability	☐	☒	☐		
Sex	☐	☒	☐		
Race	☐	☒	☐		
Religion or belief	☐	☒	☐		
Sexual orientation	☐	☒	☐		
Gender reassignment	☐	☒	☐		
Pregnancy and maternity	☐	☒	☐		
Marriage and civil partnership (only eliminating discrimination)	☐	☒	☐		
Other relevant groups	☐	☒	☐		
HR Policies only: Part or Fixed term staff	☐	☒	☐		

IMPORTANT NOTE: *If any of the above results in '**negative'** impact, a 'full' EIA which covers a more in depth analysis on areas/groups impacted must be considered and may need to be carried out.*

Having detailed the actions you need to take please transfer them to onto the action plan below.

3. Action plan				
Issues/impact identified	**Actions required**	**How will you measure impact/progress**	**Timescale**	**Officer responsible**

4. Monitoring, Review and Publication				
When will the proposal be reviewed and by whom?	**Lead / Reviewing Officer:**	**Information Governance Manager** **Information Governance Group (Sheffield CCG)**	**Date of next Review:**	**January 2023**