NHS
North Yorkshire
Clinical Commissioning Group

Information Security Policy

February 2021

Authorship:	Senior Information Governance Specialist
Committee Approved:	NHS North Yorkshire CCG Audit Committee
Approved date:	February 2021
Review Date:	February 2024
Equality Impact Assessment:	Yes
Sustainability Impact Assessment:	Yes
Target Audience:	Governing Body and its Committees and Sub-Committees, CCG Staff, agency and temporary staff & third parties under contract
Policy Number:	NY-113
Version Number:	1.1

The on-line version is the only version that is maintained. Any printed copies should, therefore, be viewed as 'uncontrolled' and as such may not necessarily contain the latest updates and amendments.

POLICY AMENDMENTS

Amendments to the Policy will be issued from time to time. A new amendment history will be issued with each change.

New Version Number	Issued by	Nature of Amendment	Approved by & Date	Date on Intranet
0.1	Senior Information Governance Specialist	First Draft	Information Governance Steering Group (IGSG) - November 2020	
0.2	Senior Information Governance Specialist	Second Draft	Audit Committee – February 2021	
1.0	Senior Information Governance Specialist	Approved Final Version		24/02/21
1.1	Senior Information Governance Specialist	Requirement for new starters to complete Data Security training within first week of starting employment	IGSG (May 2021)	May 2021

Contents

1.0 Introduction

The CCG aspire to the highest standards of corporate behaviour and clinical competence, to ensure that safe, fair and equitable procedures are applied to all organisational transactions, including relationships with patients, their carers, public, staff, stakeholders and the use of public resources.

In order to provide clear and consistent guidance, the CCG will develop documents to fulfil all statutory, organisational and best practice requirements and support the principles of equal opportunity for all.

The CCG has a duty to meet legislative and regulatory requirements in relation to information security. These include the NHS Digital Data Security and Protection toolkit and statement of compliance and the legislation, guidance and associated policy documents listed in section 7 of this policy.

It is essential that all of the CCG's information systems are protected to an adequate level from business risks. Such risks include accidental data change, loss or release, malicious user damage, fraud, theft, failure and natural disaster. It is important that a consistent approach is maintained to safeguard information in the same way that other more tangible assets are secured, with due regard to the highly sensitive nature of some information held on both electronic and manual systems.

Information security must address both the relevance and the level and kind of threats to which information systems and their associated assets are exposed. To ensure that assets are protected against compromise, it is important that this security policy and procedures meet the following objectives;

- deal with the prevailing threats;
- be cost effective;
- add value by reducing the risks to assets;
- be incremental, that is, apply security controls appropriate to the value of the assets involved;
- be just, open and reasonable, where they impinge on the lives of employees;
- be credible and workable, that is, user-friendly, understood, respected and supported by all individuals required to use them
- be cost effective and responsive to the needs of the CCG, and not any more intrusive to on-going business and operations than is necessary;
- reflect the 'need to know' principle.

The security that can be achieved through technical means is limited, and needs to be supported by appropriate management controls and procedures. Identifying which controls should be in place requires careful planning and attention to detail. Information security management needs, as a minimum, participation by all employees in the CCG.

2.0 Purpose

This policy sets out the detailed procedures, rules and standards governing information security that all users of the CCG's information systems must comply with, the CCG's commitment to information security and overall approach to managing information security.

This policy aims to ensure that;

- information systems used in the CCG are properly assessed for security
- appropriate levels of security are in place to maintain the confidentiality, integrity and availability of information and information systems
- all staff are aware of their roles and responsibilities for information security
- a means is established to communicate an awareness of information security issues and their impact on the CCG to management, users and other staff

It is essential that all information processing systems are protected from events which may jeopardise the activities of the CCG. These events may be accidental as well as behaviour deliberately designed to cause difficulties. Adherence to this policy and related policies and procedures, will ensure that the risk of such occurrences is minimised.

This policy will ensure that all information systems, including computer systems, network components and electronically held data, are adequately protected from a range of threats.

This policy and associated guidelines cover all aspects of information security from paper-based records to IT systems, administration systems, environmental controls, hardware, software, data and networks.

3.0 Definitions / Explanation of Terms

The following terms are used in this document:

Confidentiality is defined as the restriction of information and assets to authorised individuals.

Integrity is defined as the maintenance of information systems and physical assets in their complete and proper form

Availability is defined as the continuous or timely access to information, systems or physical assets by authorised individuals.

Encryption is the process of converting information into a form unintelligible to anyone except holders of a specific key or password.

Information Asset is defined as either personal information, corporate information, computer software, hardware, system or process documentation.

Information Asset Owner (IAO) is the senior individual within the service who is responsible ensuring that specific information assets are handled and managed

appropriately. Their role is to understand and address risks to the information assets they 'own' and to provide assurance to the senior information risk owner (SIRO) on the security and use of those assets.

Information Asset Administrators (IAA) support the IAO to ensure that this procedure is followed, recognise actual and potential security incidents, and consult the appropriate IAO on incident management.

Privacy by design is a concept explained within the General Data Protection Regulations and is about considering data protection and privacy issues upfront in everything we do. It can help ensure compliance with the GDPR's fundamental principles and requirements, and forms part of the focus on accountability. See Article 25 GDPR.

Privacy by default is a concept explained within the General Data Protection Regulations and is about the Controller if data implementing appropriate technical and organisational measures to ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. See Article 25 GDPR.

Removable media is a term used to describe any kind of portable data storage device that can be connected to and removed from a computer e.g. CDs/DVDs, USB flash memory sticks or pens, PDAs.

Smartcard is a card (like a credit card) with an embedded microchip for storing information. The NHS smartcard is used to control security access to electronic patient records and patient administration systems.

4.0 Scope of the Policy

This policy applies to all staff employed by the CCG, agency workers, contractors, students, trainees, temporary placements who have access to information systems or assets belonging to the CCG.

It also applies to other individuals and agencies who may gain access to data, such as non- executive directors, volunteers, visiting professionals or researchers, and companies providing information services to the CCG.

Breaches of this policy may be investigated and may result in the matter being treated as a disciplinary offence under the CCG's disciplinary procedure

5.0 Duties, Accountabilities and Responsibilities

5.1 Accountable Officer

Overall accountability for procedural documents across the organisation lies with the Accountable Officer who has overall responsibility for establishing and maintaining an effective Information Governance Framework, for meeting all statutory requirements and adhering to guidance issued in respect of procedural documents.

5.2 Senior Information Governance Owner (SIRO)

The CCG's SIRO is responsible for overseeing the implementation of appropriate processes and procedures to ensure that individual's information can be processed and held securely.

5.3 Caldicott Guardian

The Caldicott Guardian is responsible for overseeing and advising on issues of service user confidentiality for the CCG.

5.4 Corporate Services Manager

Responsibility for the management, development and implementation of policy procedural documents lies with the Corporate Services Manager

5.5 Line Managers

Line managers are responsible for ensuring that all staff, particularly new staff, temporary staff, contractors and volunteers, know what is expected of them with respect to information security and protecting information. They are also responsible for monitoring compliance with this guidance.

5.6 All Staff

All staff are responsible for ensuring they are aware of the requirements of this policy and adhering to them.

5.7 Responsibilities for Approval

Audit Committee is responsible for the review and approval of this policy.

6.0 Policy Procedural Requirements

This policy will be supported by system-specific security policies, technical standards and operational procedures, which will ensure that its requirements are understood and met across the CCG.

6.1 Information Assets

The CCG will ensure that:

- All information assets under its control are identified and documented in an Information Asset Register in accordance with GDPR;
- All information assets for which IAOs are responsible are reviewed to identify potential threats to the system, and the likelihood of those threats occurring;
- The cost of countermeasures against perceived threats is commensurate with threats to security, the value of the assets being protected and the impact of security failure;
- System specific security policies and standard operating procedures are in place for all systems under their jurisdiction (i.e. the systems they own or are responsible for);
- All staff are fully trained in the use of the systems that they are required to operate;
- Staff must not operate systems for which they have not been trained;

- The CCG's electronic information assets are protected from the threat of viruses and other malicious software;
- Business continuity plans are in place to protect critical business processes from the effects of major failures of IT systems or other disasters.

Privacy by design and default are considered at the outset of any new project, system or process involving information assets

6.1.1 Computer Hardware and Software

Authorised hardware and software

Only hardware approved by the CCG may be used or connected to its network. Any unauthorised hardware found will be removed. Only software approved by the CCG may be used. Unauthorised software must not be used on CCG equipment or on its network. Any unauthorised software found will be removed and may result in disciplinary action.

Only authorised staff may install, modify or upgrade hardware or software belonging to, or provided by the CCG.

All software licenses must be held by the IT department as this is required for the asset register and also should any reinstall be necessary.

Use of personal equipment

Personal equipment must not be used on the CCG's network for the purpose of carrying out organisational business. Encryption controls may impact on the running of personal equipment which in turn may result in permanent damage to the device. The CCG cannot be held liable should any damage to personal equipment occur. This personal equipment may include (but is not exhaustive) PDAs, smart phones, laptops, tablets and external hard drives.

Personal equipment or equipment from other organisations could be used on a public network (if/when available) at work premises with appropriate authorisation as this does not provide any access to the organisation's data.

Personal equipment (such as laptops, PCs, tablets, and mobile phones must be locked whenever the user is away from their workspace.

Information storage and backup

Staff are responsible for ensuring their information is saved appropriately. Where a staff member has network access, all information must be saved to their network drive which is automatically backed up by the ICT provider on behalf of the CCG.

Staff are advised that the authorised encrypted memory stick is only for the transfer of information and the original content must be saved to the network.

Public key infrastructure (PKI) and secure socket layer (SSL)

The CCG's network uses digital certificates to provide additional security on the network to provide encryption using PKI algorithms. This approach which works invisibly in the background provides an additional level of security for the network by only allowing authenticated equipment with digital certificates to be a member of the network.

Web based organisational databases which contain personal information and are accessed via the web, must be secured using SSL encryption, e.g. (has https: in the address bar and a padlock icon on the toolbar).

Cloud computing

The cloud computing concept provides the ability to access data stored within the cloud by many different tools. Examples of cloud computing hosting organisations are:

- Google
- Drop Box
- Office 365 (Microsoft)
- Amazon

No data belonging to the CCG is to be stored or placed in a cloud environment without the approval of the IAO and Information Governance Service.

Some of the issues are listed below (but please note this list is not exhaustive);

- Data storage area of the cloud will not normally be known and may be based external to the UK
- Data Storage area could be shared and not segregated from another organisation's data
- No access to data if unavailable due to downtime/system failure
- No contract with the hosting organisation thereby lack of control over the data as the data controller

Internet protocol (IP) phones

IP phone systems allow telephone calls to be made across an internet connection rather than via standard telephone system IP phones are subject to similar security risks to un-secured email, for example 'eavesdropping', 'traffic sniffing' and 'unauthorised re-routing'.

The IP phone systems will transmit and receive data on their own segmented part of the network which is unavailable to other network devices.

6.2 Access Controls

All staff wishing to access the CCG's network must firstly accept the user agreement. In doing so the user agrees to abide by the terms and conditions stated as well as the policies of the CCG.

No one shall be granted access to an information system that does not require that access as part of their work for the CCG. Any access granted is following agreement with the IAO to ensure that access is limited to that required.

6.3 Passwords

The primary form of access control for the CCG's computer systems is via password. Each member of staff using a computer system will have an individual password.

Sharing of passwords by both the person who shared the password and the person who received it is an offence under the Computer Misuse Act 1990. All staff must follow robust security practices in the selection and use of passwords.

These include:

- Logon details are not to be shared or used under supervision even in training situations
- Ensuring strong passwords are used i.e. using a minimum 8 digit combination of letters, numbers and special characters (!?£&%$ etc) and to ensure that consecutive passwords are not used e.g. mypassword1, mypassword2, mypassword3 etc.
- Not writing down passwords where they can be easily found, i.e. on sticky notes next to their workstation
- Ensuring passwords are changed when prompted
- Changing their password immediately if they suspect it has been compromised and reporting the incident using the organisation incident reporting system
- Not basing their password on anything that could be easily guessed by another, such as their own name, make of car, car registration, name of pets etc.
- Not recycling old passwords

6.4 National Applications Systems Controls

National Spine enabled systems are controlled by a number of different security mechanisms including:

- **Smartcard:** Access will be restricted through use of an NHS Smartcard with a pass code, provided by the local CSU Registration Authority Service.
- **Training:** Access to the NHS Care Record Service will only be allowed following appropriate training.
- **Legitimate relationships**: Staff will only be able to access a patient's record if they are involved in that patient's care.
- **Role based access control (RBAC)**: Access will depend on staff roles/job/position functions. Roles and access privileges will be defined centrally and given locally by people designated to do this in the organisation.
- **Sealed envelopes:** Patients will be able hide certain pieces of information from normal view. This will be called a patient's sealed envelope.
- **Audit trails**: Every time someone accesses a patient's record, a note will be made automatically of who, when and what they did.

- **Alerts:** Alerts will be triggered automatically both to deter misuse of access privileges and to report any misuse when it occurs e.g. if breach of sealed envelope, or no legitimate relationship being present

6.5 Access to other Staff Members Data

Email

In cases where, for example, due to unplanned sickness there is a requirement for access then permission can only be given to Line Manager to access the account through contact with the IT Service Desk.

Staff must ensure they provide access to their Line Manager or other appropriate person in cases of planned absences.

Personal folders

In cases where there is a requirement for access to data, e.g. due to unplanned sickness, then permission must be sought from the folder owner before access can be granted by the IT Service Desk.

6.6 Remote Access and Mobile Working

Staff must not attempt to connect to the CCG's network remotely other than via the CCG's agreed remote access solution provided by the CCG's ICT service provider.

6.7 Incidents and Risks

All risks and incidents relating to information security must be reported using the CCG's standard procedures for risk and incident reporting.

The reporting of risks and incidents is important to ensure that appropriate action is taken to minimise impact, avoid reoccurrence and to share any lessons learned.

In the case of serious incidents, the CCG may have to secure digital forensic evidence, for example, on a hard drive to prevent this from being tampered with during formal disputes or legal proceedings.

6.8 Internet and Email Security

When accessing the Internet or email the following must be adhered to:

Before using the Internet, Intranet or email for the first time all staff must accept the terms and conditions of the user code of connection.

No illicit or illegal material may be viewed / downloaded or obtained via the Internet or email.

Any material downloaded must be virus checked automatically by the system's anti- virus system.

The user will make their system available at any time for audit either by the IT department, ~~or~~ internal audit or external audit.

Be mindful of cyber security and do not click links within emails from unknown or untrustworthy sources.

Usage is monitored by the CCG and any breaches of security, abuse of service or non-compliance with the NHS Code of Connection or organisational policy may result in disciplinary action, as well as the temporary or permanent withdrawal of all N3 services including email.

6.9 Transferring Information and Equipment

It is imperative that the utmost care is exercised when transferring information, especially information of a confidential nature e.g. staff, patient or service user information. This includes transferring information by telephone (voice and text), email, fax, courier and public mail.

Caldicott principles must be followed at all times where patient/person-identifiable information is concerned. These were revised following the caldicott 2 review in March 2012 and are listed at appendix A.

Regular exchanges of personal information must be governed by information sharing protocols or data processing agreements within contracts.

Staff must not leave any property belonging to the CCG, including laptops, portable devices, mobile telephones, records or files in unattended cars or in easily accessible areas for extended periods, including overnight. These must either be secured within premises under the CCG's control, or where this is not practicable secured within the employee's home. Where an overnight stay for work purposes is required the same principles apply.

In instances where equipment or records are unavoidably left unattended for short periods e.g. calling at another base, making an unscheduled stop, the staff member must assess the potential risk to the equipment whilst it is unattended. A formal written risk assessment need not be undertaken but the staff member must make a judgement on the security of the equipment.

If a staff member is required to change their office base, they must not move any desk-based IT or telephone equipment. All desk-based IT and telephone equipment must be moved by a member of the IT department.

All IT or telephone equipment intended for destruction must be securely disposed of by the IT department in accordance with agreed procedures in place at that time.

Destruction certificates will be obtained and held by the IT department.

6.10 Systems Development Maintenance and Security

The CCG must ensure that security requirements are built into systems from the outset. Suitable controls must be in place to manage the purchase or development of new

systems and the enhancement of existing systems, to ensure that information security is not compromised.

IAO and IAA implementing or modifying systems are responsible, in collaboration with the CSU ICT service for ensuring;

- The Computer Misuse Act warning is displayed on all organisation equipment prior to logging on to the network
- That all modifications to systems are logged and up to date documentation exists for their systems and follow change control procedures
- Contracts with suppliers must include appropriate confidentiality clauses
- They complete a risk assessment in liaison with the CSU ICT service
- That vendor supplied software used in systems is maintained at a level supported by the supplier, if beneficial to the service. Any decision to upgrade must take into account the security of the release e.g. software drivers that come with printers to operate the printer, and clinical safety
- Physical or logical access is only provided to suppliers for support purposes when necessary, and must be with IAO, and ICT approval
- That all supplier activity on the system is monitored
- That copies of data must retain the same levels of security and access controls as the original data

6.11 Data Protection Impact Assessments

A data protection impact assessment must be completed prior to installation, in liaison with the Information Governance Team, to ensure all information security aspects of new and modified systems are considered and risk assessed.

6.12 Business Continuity Plans

The CCG must have a business continuity plan to allow critical systems within each service area to be maintained and to restore critical systems in the event of a major disruption to systems, e.g. through a disaster or security failure. This supports the wider organisation business continuity planning.

It is the responsibility of the IAOs to ensure that their section of the CCG's business continuity plans is regularly updated to reflect changes in service delivery.

Business continuity plans should be tested annually to ensure they work. The responsibility to and undertake such exercises will lie with individual IAOs

7.0 Public Sector Equality Duty

In developing this policy an Equality Impact Analysis (EIA) has been undertaken. As a result of performing the analysis this policy, does not appear to have any adverse effects on people who share *Protected Characteristics* and no further actions are recommended at this stage.

NHS North Yorkshire 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.

7.1 Consultation

This Policy has been reviewed by Information Governance Steering Group prior to approval by the Audit Committee.

8.0 Training

Data Security Standard 3 within the Caldicott 3 review requires that all staff undertake appropriate annual data security training and pass a mandatory test, this must be completed by new employees within one week of commencement of employment. Further specific training may be required in line with job roles delegated to staff.

Staff will be made aware of this policy via the CCG Newsletter

9.0 Monitoring Compliance with the Document

Compliance will be monitored through assessment or completed Data Protection Impact Assessments a report will be produced to report and agree the implementation of appropriate controls where weaknesses are identified. It should be noted that under certain circumstances the CCG may wish to accept risks where they are not considered to be low.

Further monitoring and investigation will be undertaken through the investigation into incidents that occur. Lessons learnt from these investigations may result in updates to this policy and CCG procedures.

10.0 Arrangements for Review

The policy will undergo a full review every three years. Earlier review may be required in response to exceptional circumstances, organisational change or relevant changes in legislation/guidance, as instructed by the senior manager responsible for this policy.

11.0 Dissemination

Staff will be made aware of the policy via the Intranet. Awareness of reviewed and amended policies will be through the CCG staff newsletter.

12.0 Associated Documentation

- Data Protection and Confidentiality Policy
- Records Management Policy
- Internet and Email Acceptable Use Policy
- Mobile Woking Policy

13.0 References

- Cabinet Office. (2018) Data Protection Act 2018. London: HMSO
- Cabinet Office. (1998) Human Rights Act 1998. London: HMSO
- Cabinet Office. (1990) The Computer Misuse Act 1990. London: HMSO
- Cabinet Office. (2000) The Electronic Communications Act 2000. London: HMSO
- General Data Protection Regulation (2016)
- Department of Health, NHS Code of Practice: Information Security http://www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Informationsecurity/index.htm
- BS ISO/IEC 17799:2005 (Information technology -- Code of practice for information security management)
- BS ISO/IEC 27001:2005(Information technology - information security management systems)
- BS7799-2:2005BS7799-2:2005 (Information security management)
- NHS Connecting for Health Information Governance Toolkit: https://nww.igt.connectingforhealth.nhs.uk/

14.0 Appendices

Appendix A: Caldicott Principles

15.0 Appendix One - Caldicott2 Principles

1) Justify the purpose(s)

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

Don't use personal confidential data unless it is absolutely necessary Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

2) Use the minimum necessary personal confidential data

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

3) Access to personal confidential data should be on a strict need-to-know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

4) Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personal confidential data — both clinical and non-clinical staff — are made fully aware of their responsibilities and obligations to respect patient confidentiality.

5) Comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

6) The duty to share information can be as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles.

They should be supported by the policies of their employers, regulators and professional bodies.