Approved Sept 2020

NHS
North West London
Collaboration of
Clinical Commissioning Groups

Information Security Policy

Version Control

Version Number	Reviewing Committee / Officer	Date
1.0	NHS NW London Clinical Commissioning Group, IT Security & Cyber Security Team	21/3/19
1.2	Altaf Suleman added section 19	08/10/19
1.3	Reviewed and amended by Abhilash Abraham	04/11/19
1.4	Reviewed by Local Counter Fraud Specialist team (RSM) amended 7.6.4 by Altaf Suleman	19/11/19
1.5	Felicia Ayo-Ajala (Data Protection Officer)	26/02/20

Reviewers

This document must be reviewed by the following:

Name	Signature	Title / Responsibility	Date	Version
Ernest Norman-Williams		NWL GPs - Data Protection Officer (DPO)	05/11/19	1.3
Abhilash Abraham		IT Security & Cyber Security Lead	19/11/19	1.4
Felicia Ayo-Ajala		Corporate Data Protection Officer	26/02/20	1.5

Approvals

This document must be approved by the following:

Title	Signature	Title / Responsibility	Date	Version
Jenny Greenshields		SIRO	21.09.20	1.5
NWL CCGs Governing Bodies	---------------	NWL CCGs Governing Bodies	Sept 2020	1.5

Contents

1. Introduction

1.1 This policy ensures that all information and information systems within NHS CCG are secured in such a way that it would be highly unlikely that unauthorised persons would have access to the data contained therein.

1.2 This policy is written as an overarching Information Security Policy. Individual detailed policies for each aspect of information security are referenced from this policy. New referenced policies will be added or amended as and when appropriate.

1.3 The main headings in this policy are taken from the Information Security Management (ISMS) System ISO 27001 standards and are used to group our detailed policies into a meaningful structure.

1.4 The CCG recognises the need for appropriate sharing of information whilst maintaining confidentiality of personal information. The CCG supports the principles of corporate governance and recognises its public accountability in the use of commercially sensitive information and personal information about patients and staff.

1.5 The CCG recognises the need to share patient information with other health organisations and other agencies in a controlled manner, consistent with the interests of the patient and with the public interest. Accurate, timely and relevant information support the delivery of high quality health care.

2. Purpose

2.1 The purpose of this Policy is to ensure that the CCG complies with legislation and NHS standards in respect of information security and in particular the requirements of the NHS in respect of securing electronic data through encryption. However, this overarching policy is not specific to electronic data and also applies to manually held records. It is necessary to ensure that any information, but personally identifiable data in particular, is secure and unable to be seen by any unauthorised person.

2.2 This Policy aims to ensure that information processing systems, and electronic or paper based information, are protected from events that may jeopardise staff and patients' rights to confidentiality, other healthcare activities or, the business objectives of the organisation.

2.3 The rules, measures and procedures described herein determine the protection of the CCG's information and assets by ensuring that:-

- Information systems are properly assessed for security
- Availability is ensured (information is delivered to the right person, when needed and adhering to the organisation's business objectives)
- Integrity is maintained (all system assets are operating correctly according to specification, protected from unauthorised or accidental modification, and Ensuring accuracy and completeness of the organisation's assets)
- Confidentiality is preserved (assets are protected against unauthorised disclosure).
- Accountability is enforced (staff are made aware of and held to account for their roles and responsibilities in regard to information security)
- Breaches of security are detected and resolved.

3. Scope

3.1 This policy applies to all employees (permanent, seconded, contractors, management and clinical trainees, apprentices, temporary staff and volunteers) of the CCG. Third Parties with whom the CCG may agree information sharing protocols will be governed by the associated information sharing agreements and will be made aware of this policy.

3.2 This policy covers all information systems purchased, developed and managed by or on behalf of the CCG and its partners. It also applies to any person directly employed, contracted or volunteering to the CCG.

3.3 The policy covers all aspects of information within the CCG, including but not limited to:

- Patient/client/service user information
- Personnel information

The policy covers all aspects of handling information including, but not limited to

- Structured record systems – paper and electronic
- Transmission of information – email, post and telephone
- Storage systems including cabinets, servers etc. for both paper and electronic information
- Electronic information including computer disc, USB memory stock, CD, DVD, internet files

4. Key Principles

4.1 To ensure staff are aware of the need to ensure the confidentiality and security of information and that they understand and comply with any legislation referred to in this and associated references.

4.2 To ensure systems are in place to monitor all aspects of information security and that these are reflected in the Data Security and Protection Toolkit assessment.

4.3 To ensure monitoring of compliance is undertaken.

4.4 To ensure there is a CCG wide culture for ensuring the confidentiality and security of personal data.

4.5 To protect information assets under the control of the CCG.

4.6 To ensure training is in place to inform all staff of information security and to ensure they are aware of all their responsibilities with respect to information.

4.7 To utilise this overarching information security policy to support on-going policy, procedure and guidelines development as newer information security technologies become available.

5. Legal Considerations

5.1 UK Data Protection Legislation states that personal information is confidential. The CCG will audit its compliance with relevant legal requirements.

5.2 The seven key principles of the GDPR and the seven Caldicott Principles will be upheld via the development of policies and procedures relating to confidentiality and processing of data within the CCG and partner organisations.

5.3 The CCG has policies for the control and appropriate sharing of patient information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act 2001, Crime and Disorder Act 1998, Protection of Children Act 1989/04).

5.4 The CCG has policies to comply with the Data Protection Act 2018, General Data Protection Regulation (GDPR), Human Rights Act 1998 and the Common Law Duty of Confidentiality.

5.5 The CCG regards all identifiable personal information as confidential. Confidential information will not be disclosed without appropriate consent or other Legal basis as required by (Articles 6(1) for confidential Information and Articles 9(2) for “Special Categories of data”, unless national policy requires otherwise, or where this is requested by legal authorities.

6. Openness

6.1 Non-confidential information about the CCG and the services it delivers are made available to the public via the CCG's websites.

6.2 The CCG's policies and procedures ensure compliance with the Freedom of Information Act (2000).

6.3 Patients should have ready access to information relating to their own healthcare, their options for treatment and to their rights.

6.4 The Caldicott Guardian oversees the CCG's procedures for handling access to personal/confidential information or the sharing of this information. The Information Governance Manager/leads is responsible for overseeing subject access requests process, supported by the DPO.

6.5 The communication strategy gives the arrangements for liaison with the press and broadcasting media.

7. Information Security

The CCG has policies for management of its information assets and resources and will undertake risk assessments and audits of its IT and network security arrangements, to ensure compliance with legal requirements.

The CCG supports the establishment of an organisation-wide information asset register which lists the organisation's information assets, including risk assessments and action plans for each information asset. All information assets will have an owner and an administrator.

The CCG maintains incident reporting procedures, and investigates all reported breaches of information security or confidentiality.

The CCG will promote information security and confidentiality practices to all employees, through the organisation's policies and procedures.

The CCG will provide training to raise staff awareness of information confidentiality and security.

Any location where information is stored, whether that be in computer systems or in paper based records, will be physically secure. This level of security will be determined through risk assessments. However the physical security is only as good as the diligence of staff to enable it to operate. Wedging open of doors, leaving windows open and allowing unknown people to "tailgate" through security doors unchallenged all contribute to a breakdown in those security measures.

7.1 Security of information

Visitors, some temporary and contract staff, security and cleaning staff, are examples of people with authorised access to secure, access controlled sites, who are not authorised to view confidential or sensitive data. The nature of the data and not site location dictates how and when this Policy is applied.

Where confidential (patient identifiable) or other commercially sensitive information is involved, users must, as and when appropriate:-

- Remove all sensitive information from the workplace and lock away, in a drawer or preferably in a fire resistant safe or cabinet. This includes all patient identifiable information, as well as other sensitive (personal or business) information such as salaries and contracts
- Store visit, appointment or message books in a locked area when not in use
- Angle computer screens away from visitors

- When leaving a workstation either log out or, in the case of a PC, lock the screen. (Press keys ctrl, alt, del at the same time, or the Windows key (next to alt) and L).
- Store paper and data storage media in secure cabinets or safes.
- Locate photocopiers and printers so as to avoid unauthorised use, using the locked pin function.
- Ensure that post-it notes and sticky labels holding identifiable or other sensitive information are not left to view

7.2 Security of premises

Physical security measures must be applied to premises ensuring that;

- Office doors and are locked when the area is unmanned;
- Windows in ground floor offices are locked;
- Blinds are drawn (where fitted) on ground floor offices overnight;
- And that equipment is not easily seen from outside

7.3 Servers

The CCG's servers should only be accessible by appropriate IT members of staff.

7.4 Removable media

Since the organisations computers are all connected to a network which allows sharing of data within the organisation, the use of removable media such as memory sticks and CDs implies that information is going to leave the organisation's premises. If there is a need to use removable media, the following must be adhered to;

- CDs, DVDs and any other removable storage device such as USB memory sticks/pens which contain personal or confidential data must be encrypted to Department of Health and Care’s standards
- Confidential or personal data should only be written to encrypted memory sticks/pen drives which have been issued by the IT Service Desk.
- Any bulk extracts of confidential or sensitive data must be authorised by the responsible senior manager for the work area
- Line managers are responsible for the day to day management and oversight of removable media used within their work areas to ensure this Policy is followed; the secure storage of all unallocated removable media and its related control documentation as required by this Policy
- Staff that have been authorised to use removable media for the purposes of their job roles are responsible for the secure use of those removable media as highlighted in this Policy. Failure to comply with this removable media may endanger the information services and the organisation and will be investigated under HR policies
- Removable media may only be used to store and share NHS information:
  - That is required for a specific business purpose. When the business purpose has been satisfied, the contents of removable media must be removed from that media through a destruction method that makes recovery of the data impossible. Alternatively the removable media and its data should be destroyed and disposed of beyond its potential reuse. In all cases, a record of the action to remove data from or to destroy data should be recorded in an auditable log file;
  - Removable media e.g. USB memory sticks should not be taken or sent off-site unless a prior agreement or instruction exists. A record must be maintained of all removable media taken or sent off-site, or brought into or received by the organisation. This record should also identify the data files involved;

- Removable media must be physically protected against loss, damage, abuse or misuse when used, when stored and in transit;
- Data archives or back-ups taken and stored on removable media, either short-term or long-term, must take account of any manufacturer's specification or guarantee and any limitations therein;
- All incidents involving the use of removable media must be reported to the Service Desk
- Equipment should not be taken off site (for example repair) when the device contains disk drives or memory cards.

7.5 Disposal of equipment

Great care must be exercised when disposing of any equipment which has been used in the processing of information if there is any possibility that some information may remain on it.

Any stored electronic data must be removed or destroyed through a method that makes the recovery of the data impossible. The IT team will arrange for any such removal or destruction.

The disposal of electronic equipment must be carried out in accordance with current NHS minimum standards, and confirmation should be obtained that destruction is total and there is no possibility of reconstruction or recovery.

7.6 NWL Agile working

This section is to support staff who use organisation supplied mobile data devices or paper records at any site other than their normal place of work or at home, by ensuring that they are aware of the information security issues. In order to protect staff and other people, organisational assets and systems, staff who work at home or other sites must take appropriate security measures. Please refer to the NWL Agile working policy.

7.6.1 Use in any public access area

The use of information in these areas must be kept to an absolute minimum, due to the threats of ‘overlooking’ and theft. Any member of staff choosing to use information and/or devices in these areas that results in any related incident will be required to state why the usage was required in that situation and the efforts they made to protect the information and any equipment

Equipment in use must not be left unattended at any time.

7.6.2 Use in areas not generally accessible to the public (including other NHS premises)

Staff are responsible for ensuring that unauthorised individuals are not able to see information, access systems or remove equipment or information. If equipment is being used outside of its normal location and might be left unattended, the user must secure it by other means (such as security cable, locked cabinet or room).

7.6.3 Occasional use at home

It is recognised that staff will have to hold organisational information at home.

- Only members of staff are allowed access to information being used at home in any form, on any media.
- Use of any information at home must be for work purposes only and on CCG equipment
- Staff must ensure the security of information within their home. Where possible it should be stored in a locked container (filing cabinet, lockable briefcase). If this is not possible, when not in use it should be neatly filed and stored in a way that it is not obvious to other members of the household.
- Any personal/sensitive (including patient and staff information) or commercially sensitive information that has to be taken home must only be in

circumstances where appropriate senior manager approval has been given and that the information must not be seen by other members of the household

7.6.4 Using equipment supplied by the Organisation

- Any member of staff allowing access by an unauthorised person, deliberately or inadvertently may be subject to the Organisation's disciplinary procedure.
- Organisation equipment must not be connected to any phone line, internet connection or network via a secure remote link (VPN) other than to access NHS resources.
- Any equipment supplied for remote access to NHS resources must be stored securely when not in use. Where a system requires a PIN number and a 'security token' these must be stored separately.
- The Organisation's IT department is responsible for ensuring that access to supplied equipment requires a username and password and that anti-virus software is installed.
- Portable equipment (i.e. a laptops, tablets or similar devices), supplied by the organisation must be connected to the organisation's network every 30 days (maximum) for upgrade of anti-virus software and security updates .
- Provided all policy statements above are applied, any supplied equipment may be used for any type of work which would normally be done on an organisation's desktop PC. This includes the use of confidential information provided the general regulations on handling and storing confidential data are complied with.
- Joiner and leavers to be reported to the Service Desk to be advised of the process so all/ any equipment is collected and accounts deactivated in a timely manner so that access is restricted/ removed.

7.7 Email and offsite working

The organisation has an Email Policy to refer to but the following points apply directly to staff working from home.

7.7.1 Confidential Data contained in an email

Under no circumstance should staff send emails containing patient or staff identifiable data, or any other confidential email, to their personal email accounts.

Internet email services of any sort are not secure and must not be used to send personal identifiable data or other confidential information,

7.7.2 Auto forwarding

Staff must not automatically forward their email to a commercial ISP (internet service provider) such as Hotmail, to enable access at home.

7.8 Transport of Equipment, Files and Paper Documents

When equipment, files and/or data are removed from the Organisation's premises the individual removing them is responsible for ensuring its safe transport as far as is reasonably practical.

- Equipment and paper files must be kept out of sight (in car boots), locked away and ideally not be left unattended at any time. Equipment and paperwork must not be left in a vehicle overnight.
- IT equipment must be transported in a secure environment
- Appropriate packing (such as sealed envelopes, bubble wrap etc.) must be used to prevent physical damage
- When a courier service is used to transport packages containing sensitive information, tamper proof packing must be used. Courier firms should

guarantee the safe arrival of parcels and the confidentiality of any contained information.

7.9 Disaster Recovery/Major Incident planning

In the event of a major incident or disaster, refer to the CCG’s Business Continuity Policy.

8. Information Quality Assurance

8.1 The CCG will promote information quality and records management via policies, procedures, guidelines, user manuals and training.

8.2 Data standards will be set through clear and consistent definitions of data, adhering to national standards.

8.3 The CCG will establish and maintain policies and procedures for information quality and the effective management of records, including an annual corporate records audit.

8.4 The CCG will undertake or commission annual assessments and audits of its information quality and records management arrangements.

9. Records Management

9.1 The CCG will comply with Records Management: NHS Code of Practice, so that:-

- records (both live and archived) are available when needed;
- records can be located and displayed, and the current version can be identified, where multiple versions exist;

- records can be interpreted in context, i.e. who created/amended the record, and when;
- records can be trusted – their authenticity can be demonstrated;
- access to records is secure; disclosure is controlled, and audit trails track use and changes;
- records are retained, as specified in the retention schedule; records are disposed of appropriately;
- staff are trained, and aware of their responsibilities for records management.

10. Duties

10.1 Duties within the CCG

10.1.1 The Chief Accountable Officer is the Accountable Officer for Information Security and the system of internal controls.

10.2 Specific responsibilities

10.2.1 A Caldicott Guardian has been appointed as the Board member responsible for ensuring the confidentiality of patient based information.

10.2.2 The Caldicott Guardian will ensure that there are robust policies in place to ensure that patient information will remain confidential and be seen only by those clinicians authorised to see that data. The Caldicott Guardian will ensure breaches of this policy in respect of patient information are investigated and that Information Governance is duly regarded at Board level when appropriate.

10.2.3 The Chief Financial Officer is the Senior Information Risk Officer (SIRO) and takes ownership of information risk and is a key factor in successfully raising the profile of information risks and to embedding information risk management into the CCG's culture.

10.2.4 Their responsibilities are:-

- To oversee the development of an Information Risk Management Policy;
- To take ownership of risk assessment processes for information risk, including review of the annual information risk assessment to support and inform the Annual Governance Statement;
- To review and agree action in respect of identified information risks;
- To ensure that the CCG's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff;
- To provide a focal point for the resolution and/or discussion of information risk issues;
- To ensure the Board is adequately briefed on information risk issues;
- The Information Governance Lead will, through the Data Security and Protection Toolkit, ensure that the CCG has robust policies, procedures, strategies, training and awareness programmes and monitoring schedules in place to ensure the confidentiality, integrity and availability of data and ensure that the CCG complies with relevant current legislation;
- The Head of IT will ensure that technical solutions are in place to protect all personal and otherwise sensitive electronic information, wherever this information is accessed;
- The Information Asset Administrator (IAA) who will typically be the member of staff who manages the local systems on a day to day basis will be responsible for ensuring System level security policies are in place and through these policies will ensure most risks are mitigated.

Any remaining risk will be advised to the Information Asset Owners (IAO) and SIRO.

10.3 Responsibilities of other staff

10.3.1 All staff will ensure that they have read this policy and have undertaken the relevant mandatory training in the E- learning enrolments .

10.3.2 In addition all staff will abide by the policies and the procedures, regarding information governance ratified by the CCG as well as all legislation and law.

11. Information Security Management

11.1 The following sections represent the sections identified in the ISO 27001 standard for Information Security Management Systems.

12. Information Security

12.1 The CCG needs a culture to be instilled whereby the security and confidentiality of information, whether personal or corporate, is paramount. This is done through having enforceable policies and procedures in place, as well as having training available to all staff. This enables staff to understand the issues and be monitored in their understanding.

12.2 Data Security Awareness Level 1 training is mandatory for all staff. Training is required annually for all staff which ensures they are kept up to date with any changes.

13. Human Resources Security

13.1 It is necessary that the CCG has robust policies and procedures in place such that when a breach occurs, there are sufficient grounds for disciplinary action to be brought. It is also necessary that staff have adequate contractual conditions set. Any breaches of this policy and associated detailed procedures and guidelines will be investigated thoroughly in accordance with the CCGs disciplinary procedure.

14. Communications and Operations Management

14.1 For the CCG to operate it has to communicate information internally, between departments, and externally with other CCGs. This has to be done in a secure and confidential manner.

14.2 Again the need to communicate information can apply to both electronically held data and paper based information. Email in particular provides great organisational potential, but used inappropriately can also greatly increase the potential risk to the CCG.

14.3 Only authorised users will be given access to corporate IT systems and they will need to have a genuine need before access will be granted. Line Managers will organise access to other systems as appropriate.

15. Incident Management

15.1 The incident management systems used for reporting incidents concerning information are the same systems used for reporting any other type of incident within the CCG, in line with NHS Digital's 'Guide to the Notification of Data Security and Protection Incidents'.

16. Business Continuity

16.1 There must be processes (Business Continuity Plans) in place so that if a situation occurs whereby information or information systems become unavailable, a documented method of providing the service by alternative means is available. This may be short term method, may be because of a temporary power failure, or more long term methods because of loss of premises through fire etc.

17. Dissemination, Implementation and Access

17.1 Dissemination of this policy will be undertaken by publishing on the CCG's Intranet page.

18. Monitoring Compliance

18.1 Staff are expected to comply with the requirements set out within the Information Security Policy and related policies. Compliance will be monitored via Manager and Information Governance Team reports of spot checks, completion of staff questionnaires, incidents reported, electronic audit trails and submission of the Data Security and Protection Toolkit.

18.2 Non-adherence to the Information Security Policy and related policies will result in local disciplinary policies being implemented.

18.3 This Policy will be reviewed every three years unless there are changes in legislation, standards and/or risk issues are identified.

19. Secure Device Configuration

Risk owners and administrators agree a configuration which balances business requirements, usability and security.

Following architectural choices that meet the National Cyber Security Centre (NCSC) guidelines will be implemented where applicable:

- Users will have accounts with no administrative privileges. Exceptions – users such as IT Admin staff and support analysts with the appropriate security approval to carry out their job roles.
- Local Administrator accounts will have a unique strong password per device
- Local Administrator password will change on a daily basis, except where the local administrator password solution cannot be implemented.
- Users will have domain user accounts only to login into desktop computers and laptops. Exceptions – users such as IT Admin staff and support analysts with the appropriate security approval to carry out their job roles.
- Security policy will be enforced and settings applied through Group Policy which cannot be modified by unprivileged users.
- Users will only be able to save documents on a redirected folder to a file server and not save on the local device. Exceptions – When Offline folders are set up on devices.
- An enterprise configuration will be applied to implement application control. Applications will be whitelisted and only authorised applications will be installed and deployed via a trusted mechanism.
    - Applications that are not on the approved list will have to be submitted through the Change Management Process with appropriate justification for

consideration. Addition of any application classed as an “Exception” shall be assessed on the merits of its outcome based on the clinical or business requirements being met.

- External interface protection will be applied. Hardware will be whitelisted and users will not be able to add additional hardware.
- Malicious code detection and prevention will be applied in terms of a corporate Antivirus Solution and Enterprise Detection and Response will be carried out by Microsoft Advanced Threat Protection.
- Vulnerability assessment and management of devices.
- All devices will be encrypted to provide data at rest protection.
- A VPN solution will be provide data in transit protection to access clinical and internal services.
- Disk quotas will be applied.
- Generic accounts should be created or enabled because there is a business requirement for such accounts. Such accounts need to be audited on a regular basis for its usage and access levels.
- Generic accounts to have limited access to clinical system only/basic internet access and NO network shares