NHS
Corby
Clinical Commissioning Group

NHS
Nene
Clinical Commissioning Group

Information Security Policy

Policy Number: IG08

Version:	3.0
Approved by:	Information Security Policy
Date approved:	May 2018
Ratified by:	Audit and Risk Committee
Date ratified:	July 2018
Name of originator/author:	Louise Chatwyn – Information Manager
Name of responsible individual:	Neil Boughton – Deputy Director of Corporate Affairs
Review date:	May 2020
Target audience:	All Staff

Version Control Sheet

Version	Date	Who	Change
1.0	03/12		Reviewed by IM&T Policy Committee, 6/3/12 (on behalf of CMT). Approved subject to format changes on front page, diagram amendment 2.1,
1.1	06/13		Update to reflect NHS organisational changes
1.2	07/13	M Griffiths	Review for CCG ownership
1.3	02/14	M Griffiths	5.4 Updated to reflect an accurate detail of disposal of Media
2.0	04/16	L Chatwyn	Review and update to current
2.1	09/16	L Chatwyn	Question 14 of Appendix 1 – word changed following Audit and Risk Panel
3.0	05/18	L Chatwyn	Revisions to reflect • Provider changes • changes in legislation under the General Data Protection Regulations (GDPR) and Data Protection Act • Incorporate Corby CCG

Contents

1. Introduction

Robust Information Governance requires clear and effective management and accountability structures, governance processes, documented policies and procedures, trained staff and adequate resources.

Corby and Nene CCGs are public bodies, with information processing as a fundamental part of their purpose. It is important, therefore, that the organisation has a clear and relevant Information Security Policy, and Information Security practices are implemented throughout the CCG for the current and future management of information to ensure compliance with all appropriate legislation, and standards.

The CCGs are assessed against their Information Security policy and practices within the annual Data Security and Protection Toolkit Return. This document provides a summary of how the CCGs will protect, to a consistently high standard, all information assets by assuring:

- That information is being managed securely and in a consistent and corporate way.
- That the CCG is providing a secure and trusted environment for the management of information used in delivering its business
- That information is accessible only to those authorised to have access
- That risks are identified and appropriate controls are implemented and documented
- Breaches of security are detected and resolved
- Clarity over the personal responsibilities around information security expected of staff
- Demonstration of best practice in information security
- A strengthened position in the event of any legal action that may be taken against the CCG (assuming the proper application of the policy and compliance with it)

2. Purpose

This document is a statement of the approach and intentions for the CCGs to fulfil their statutory and organisational responsibilities. It will enable management and staff to make correct decisions, work effectively and comply with relevant legislation and the organisations aims and objectives.

The CCG is accountable for the confidentiality, integrity and availability of the information which it holds and information which is held by third parties (such as Commissioning Support Units, CSU's) on its behalf.

The objective of this Policy is to outline how the CCGs will preserve:

Confidentiality	Data access shall be confined to those with appropriate specified authority to view the data
Integrity	Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification
Availability	Information shall be available and delivered to the right person, at the time when needed and adhering to the organisation's business objectives

A Commissioning Support Unit provides a managed security service to Corby and Nene CCGs for Information Management & Technology (IM&T). This includes support to the Senior Information Risk Officer on security and asset and risk management.

The CSU will manage security along current best practice guidelines as provided by DH and in accordance with applicable legislation.

The CCGs acknowledge that information is a valuable asset, therefore it is within its interest to ensure that the information processing systems, and electronic or paper based information held is suitably protected from any threat.

The CCGs will achieve a standard of excellence in Information Security by minimising key risks associated with information processing. It will ensure all information is dealt with legally, securely, efficiently and effectively in the best interests of its employees and all third parties with whom information is shared in order to support the delivery of high quality patient care, service planning and operational management.

3. Scope

This document applies to all staff, whether permanent, temporary or contracted. They are responsible for ensuring that they are aware of all relevant requirements and that they comply with them on a day to day basis.

Furthermore, the principles of this document apply to all third parties and others authorised to undertake work on behalf of Corby and Nene CCGs.

This document covers all aspects of handling information, in both paper and electronic format

4. Key Roles and Responsibilities

Role	Responsibility
Accountable Officer	The Accountable Officer and the Board have ultimate accountability for actions and inactions in relation to this document

Senior Information Risk Officer	The CCG's SIRO is responsible for having overall accountability for Information Governance; this includes the Data Protection and Confidentiality function. The role includes briefing the Board and providing assurance through the Audit and Risk Committee that the IG approach is effective in terms of resource, commitment and execution. The SIRO for Corby CCG and Nene CCG is the Chief Finance Officer
Caldicott Guardian	The Caldicott Guardian has responsibility for ensuring that there are adequate standards for protecting patient information and that all data transfers are undertaken in accordance with Safe Haven guidelines and the Caldicott principles. The Caldicott Guardian for Corby CCG is a Clinical Executive The Caldicott Guardian for Nene CCG is the GP Chair
Data Protection Officer	The DPO has responsibility for Data Protection compliance The DPO for the CCGs is fulfilled by NEL CSU Email: nelcsu.dpo@nhs.net Phone: 03000 428438
Deputy Director of Corporate Affairs	The Deputy Director of Corporate Affairs has overall day to day responsibility for the Information Governance in the CCG. The role includes briefing the Board, including the SIRO and Caldicott Guardian of information risks and information incidents
Information Manager	The Information Manager has day to day responsibility for implementing and monitoring procedures to ensure compliance with relevant information legislation The Information Manager is responsible for completion of the IG Toolkit, actions arising to ensure compliance and subsequent workplans for continuing improvement
Information Security Lead	CSU provide a managed security service to Nene CCG for Information Management & Technology (IM&T) The CSU Information Security Lead will work closely with the CCG Information Team
Information Asset Owners	Information Asset Owners (IAO) will act as nominated owner of CCG information assets. Their responsibilities will include:

	• Identify Information Asset Administrators to assist them with their duties, where this is appropriate and necessary. • Document, understand and monitor what information assets are held, and for what purpose, how information is created, amended or added to, who has access to the information and why
Managers	Managers and supervisors are responsible for ensuring that staff who report to them have suitable access to this document and it's supporting policies and procedures and that they are implemented in their area of authority. Managers are also responsible for ensuring the initial training compliance of all staff reporting to them
All staff	Have a responsibility to: • Be aware of the Information Governance requirements • Support the CCG to achieve Toolkit Compliance • Complete annual Data Security and Protection training • Report information Incidents appropriately
CSU IT Service	Will provide support to CCG users Email: nelcsu.itservicedeskanglia@nhs.net Tel: 01604 978089

5. Security Measures

Management of computers and networks shall be controlled through CSU IM&T standard documented policies and procedures.

5.1 Registration

The CCGs will maintain an asset register of key Information Technology (IT) assets; this will include all IT hardware and software.

The CCGs will maintain an asset register of information systems, use risk management procedures to estimate threat probability, including security risks, their vulnerability to damage, and impact of any damage caused.

Each IT asset, (hardware, software, application or data) shall have a named custodian who shall be responsible for the information security of that asset.

Measures will be taken to ensure that each system is secured to an appropriate and cost effective level and that data protection principles are implemented.

The Information Asset Register will be reviewed regularly to ensure it remains current and accurate and will be subject to internal audit and annual assessment in line with completion of the Data Security and Protection Toolkit.

See Information Asset Management Procedures.

All initiatives requiring business case approval will be subject to a Data Protection Impact Assessment DPIA (see Data Protection Impact Assessment Procedure) which will consider information security.

5.2 Physical Security

Separate CSU guidance will exist for the security of servers and server rooms.

All staff are responsible for the physical security of assets, equipment and building used by the CCGs and will ensure that buildings are left in a secure state when vacant. Appropriate physical security measures shall be put in place to secure information assets dependant on value and sensitivity to the organisation.

Physical security measures include:

- Windows in ground floor offices are locked;
- Blinds are drawn (where fitted) on ground floor offices overnight;
- That equipment is not easily seen from outside

In order to minimise loss of, or damage to, assets equipment will be physically protected from threats and environmental hazards.

Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.

Visitors, some temporary and contract staff, security and cleaning staff, are examples of people with authorised access however this does not confer authority to view confidential or sensitive data.

Users should adopt a clear desk and clear screen practice for confidential or personal data to reduce the risks of unauthorised access, or accidental damage to or loss of sensitive or confidential information.

Laptop computers used in offices (which are not considered public areas) should be locked away overnight. Laptop computers must not be left on a desk top overnight unsecured.

Where confidential (patient identifiable) or other sensitive (employee personnel) information is involved, users must:

- Lock away when not in use all sensitive information, in a drawer or preferably in a fire resistant safe or cabinet

- Store visitor, appointment or message books in a locked area when not in use
- When leaving a workstation either log out or, lock the computer screen. (Press keys ctrl,alt,del at the same time, or the Windows key (⊞) and L)
- Store paper and computer media in secure cabinets or safes

Where possible equipment should be clearly marked as being the property of the Organisation.

Where a courier service is used to transport packages containing sensitive information tamper proof packaging must be used. Courier firms should guarantee the safe arrival of parcels and the confidentiality of any contained information.

See the Safe Haven Procedure.

5.3 Computer Security

Management of computers shall be controlled through standard documented procedures that have been authorised by CSU (IM&T).

All computers will operate up to date anti-virus software.

All laptops are encrypted using an appropriate encryption tool. End users must not install software. All software must be installed by a member of the CSU IM&T Team. Software licensing applies to all organisational devices, only licensed software provided for that purpose must be used. The security arrangements for equipment and software must not be circumvented.

Access to data, system utilities and shared drives including individual folders within shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators.

Removable media may only be used to store and share NHS information that is required for a specific business purpose.

Confidential or personal data should only be written to encrypted memory sticks/pen drives which have been approved by CSU IM&T.

External hard drives are only to be used with the prior approval of CSU IM&T Team. If approval is given, the device must be encrypted.

Following Department of Health requirements all mobile computing equipment will be encrypted to ensure data security. This ensures if the device is lost or stolen only pre-approved users will be able to access any content stored locally.

An audit trail of system access and data use by staff will be managed by CSU IM&T Team. Access of the audit trail for investigatory purposes will be carried out in accordance with CSU (IM&T) documented procedures[1] which conform to the Regulation of Investigatory Powers Act (2000) and the Human Rights Act (1998).

5.4 Passwords

Passwords should:

- Be changed regularly
- Not be shared
- Contain a mix of upper and lower case letters, numbers and symbols
- Contain a minimum of 8 characters
- Must be changed immediately if it is suspected that it has been compromised
- Not be default – for example the word "password"

5.5 Network Security

Only devices provided by the organisation must be connected to the organisation's network, wireless network and equipment.

Devices which have not been issued by the CSU or CCG must not be connected to CCG equipment, e.g. personal mobile phones, ipods, etc. as they could introduce viruses which could corrupt or destroy CCG information held within the network.

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, following Department of Health requirements all mobile computing equipment will be encrypted to ensure data security. This ensures if the device is lost or stolen only pre-approved user will be able to access and content stored locally.

Where data of a personal confidential nature is to be written to CD or DVD media then this will also require encryption. The CSU will ensure software is made available to use that allows the encryption of data before it is copied to the disk

Removable media must be physically protected against their loss, damage, abuse or misuse when used, where stored and in transit

[1] NEL CSU ICT Equipment: Acceptable Use Policy

5.6 Email Security

NHSmail provides a secure method of exchanging sensitive information with other NHSmail users and public sector contacts that use one of the other secure Government email services (e.g. .gcsx.gov.uk for Local Authorities).

NHS mail is the platform made available to staff and new user requests can be arranged by contacting the IT Helpdesk.

Emails sent from and to NHSmail accounts, or to other secure email systems are protected to UK Government standards. This ensures that sensitive and confidential information is kept safe.

NHSmail users can find best practice guidance on emailing securely in the NHSmail Training and Guidance pages, in the section 'Policy and procedure/Emailing sensitive and patient identifiable data'.[2]

Patient or staff identifiable or other confidential data must not be routinely sent to a personal email address as internet e-mail services of any sort are not secure.

Where this is the **only** option NHSmail users can securely exchange sensitive information with users of non-accredited or non-secure email services.

Further guidance can be found by following this link https://www.igt.hscic.gov.uk/KnowledgeBaseNew/HSCIC_Sending%20an%20encrypted%20email%20from%20NHSmail%20to%20a%20non-secure%20email%20address.pdf

5.7 Security When Working Remotely

This section aims 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.

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).

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

[2] Source: HSCIC

Under no circumstances is the user to permit the use of their remote access connection by any third party including colleagues, friends and family. The authorised user will be held responsible for all activities performed using their remote access account [4]

Any equipment supplied for remote access to NHS resources must be stored securely when not in use.

A virtual private network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. A VPN enables users to send data between two computers across a shared or public internet work in a manner that emulates the properties of a point-to-point private link. The act of configuring and creating a virtual private network is known as virtual private networking.

CCG 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.

Equipment, and paper files must be kept out of sight (in car boots) whilst in transit, locked away and ideally not be left unattended at any time. Equipment and paperwork must not be left in a vehicle overnight.

Any member of staff allowing access by an unauthorised person, deliberately or inadvertently may be subject to CCG disciplinary proceedings.

The CSU IT Team is responsible for ensuring that access to supplied equipment requires a username and password and that anti-virus software is installed.

Portable device users must regularly connect to the network to ensure that appropriate anti-virus and software updates are applied. Failure to do so could result in unnecessary virus outbreaks.[6]

It is an offence to use a hand-held phone whilst driving, even when stationary, which incurs a fixed penalty[7]. Should a fixed penalty be incurred, this penalty charge will not be reimbursed by the CCG.

Police can use other legislation (for failing to have proper control) if a driver is distracted by a call on a hands-free phone. If there is an incident and the driver is using any phone (hand-held or hands-free) or similar device, then there is a risk of prosecution for careless or dangerous driving.

When on CCG business, staff must only use their phone when it is safe to do so.

[4] Source: NELCSU Use of Mobile Devices Policy

[6] Source: NELCSU Security Policy and NELCSU Patch Management Process

[7] https://www.gov.uk/using-mobile-phones-when-driving-the-law

To ensure compliance with the law and to ensure your safety and the safety of other road users, staff should use voicemail or divert calls so that messages can be left for you while you are driving. Check for messages and deal with any calls once you are safely parked with the engine switched off. Guidance may be issued to mobile device users from time to time regarding health and safety and security in relation to their use and must be observed at all times.

5.8 Termination Decommission or Disposal

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 in/on it.

At the termination of employment, employees shall commit to return all data processing equipment, tokens, smartcards & data stored on devices supplied for that purpose.

All computers and electronic media must be disposed of through the CSU IM&T Team. This includes computer disks.

Disposal guidance is included in the Information Asset Management Procedure.

In cases where the information is held electronically, reference must be made to the CSU IM&T Team for the appropriate action to be taken (Note – formatting a disk and/or overwriting a tape does not necessarily destroy the information held on it). The CSU IM&T Team will arrange for the physical destruction of the media.

CSU IM&T Team will dispose of media containing personally identifiable or organisationally sensitive information on behalf of the CCGs. They will dispose of the equipment in an authorised, appropriate, legal and environmentally sound manner adhering to the WEEE (The Waste Electrical and Electronic Equipment Directive) standard and provide the CCG with a certificate of disposal. Non sensitive information may be disposed of offsite.

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

In cases where confidential information is held on hard copy (paper, film, etc.), when no longer required the media must be disposed of via the Confidential Waste process. Shredding machines and Confidential Waste sacks are made available throughout the unit and there are regular collections whereby confidential data is disposed of appropriately

6. Incident Management and Audit

Clear guidance on incident management procedures will be documented and published on the CCG intranet where this is in place and made available to all staff via shared drive documents.

All information security events shall be investigated to establish their cause and impact. Once identified, information security risks shall be managed on a formal basis. The Information team will co-ordinate analysis, investigation and upward reporting of events and recommendations for remedial action with a view to avoiding similar events.

They shall be recorded within the Team and Corporate Risk Registers as appropriate and action plans shall be put in place to effectively manage identified risks.

Information Security risks relating to Cyber Security will be referred to the CSU IM&T Team and the Information Security Manager.

The Risk Register and all associated action plans shall be reviewed regularly. Any implemented information security arrangements shall also be a regularly reviewed feature of the CCG Information Governance Working Group. These reviews shall help identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed.

An audit trail of system access and data use by staff will be managed by CSU IM&T Team. Access of the audit trail for investigatory purposes will be carried out in accordance with CSU (IM&T) documented procedures which conform to the Regulation of Investigatory Powers Act (2000)[8] and the Human Rights Act (1998).[9]

7. Business Continuity Planning

The CCG shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.

In the event of a major incident or disaster, the Organisation may recall all equipment on loan to provide core services.

[8] http://www.legislation.gov.uk/ukpga/2000/23/contents

[9] http://www.legislation.gov.uk/ukpga/1998/42/contents

8. Failure to Comply

Any failure to comply and/or breaches of this Policy and associated procedures and guidelines will be investigated thoroughly in accordance with the organisation's disciplinary policies.

9. Monitoring and Review

Performance against key performance indicators will be reviewed on an annual basis through the DSP Toolkit submission and used to inform the development of future documents.

Toolkit Data Security Standards 2, 4, 6, 8, 9 and 10

Data Security Standard 2

> All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.
>
> All staff understand what constitutes deliberate, negligent or complacent behaviour and the implications for their employment. They are made aware that their usage of IT systems is logged and attributable to them personally. Insecure behaviours are reported without fear of recrimination and procedures which prompt insecure workarounds are reported, with action taken.

Data Security Standard 4

> Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.
>
> The principle of 'least privilege' is applied, so that users do not have access to data they have no business need to see. Staff do not accumulate system accesses over time. User privileges are proactively managed so that there is, as far as is practicable, a forensic trail back to a specific user or user group. Where necessary, organisations will look to non-technical means of recording IT usage (e.g. sign in sheets, CCTV, correlation with other systems, shift rosters etc).

Data Security Standard 6

Basic safeguards are in place to prevent users from unsafe internet use. Anti-virus, anti-spam filters and basic firewall protections are deployed to protect users from basic internet-borne threats.

Data Security Standard 8

No unsupported operating systems, software or internet browsers are used within the IT estate.

Data Security Standard 9

A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.

Data Security Standard 10

IT suppliers understand their obligations as data processors under the GDPR, and the necessity to educate and inform customers, working with them to combine security and usability in systems. IT suppliers typically service large numbers of similar organisations and as such represent a large proportion of the overall ‘attack surface’. Consequently, their duty to robust risk management is vital and should be built into contracts as a matter of course. It is incumbent on suppliers of all IT systems to ensure their software runs on supported operating systems and is compatible with supported internet browsers and plug-ins.

The Information Governance agenda is supported by adequate information security skills, knowledge and experience which meets the organisation’s assessed needs

Unless there is major legislation or policy changes, this document will be reviewed every two years

10. Training

Appropriate training will be provided to all Staff commensurate with their role profile as necessary.

Training is available through ESR which can be found here http://www.esrsupport.co.uk/access.php

11. Distribution and Implementation

A full set of policy and procedural documents to support Information Governance will be made available via the intranet where this is in place.

Staff will be made aware of procedural updates as they occur via team briefs, management communications, shared drive availability and notification via the CCG staff intranet where this is in place.

12. Associated Legislation and Documents

To include but not limited to:

- IG01a – Framework CSU Information Governance Framework
- IG01b – Policy CSU Information Governance Policy
- IG02a – CCG Physical Assets
- IG02b – Data Assets (application provider guide)
- IG03 – CCG Information Disclosure and Sharing Policy and Procedure
- IG04 – CCG Email and Internet
- IG05 – CCG Data Security and Protection Incidents Reporting Procedure
- IG06 – CSU Confidentiality & Data Protection Policy
- IG07 – CCG/CSU Data Protection Impact Assessment Procedure
- IG08a – Framework CSU Information Security Framework
- IG09 – CCG Safe Haven Procedure
- IG10a – Framework CSU Information Quality Framework
- IG10b – CCG Records Management Policy
- IG11 – CCG Subject Access Request
- IG12 – CSU Freedom of Information Policy and Procedure

The following references and areas of legislation should be adhered to.

- Confidentiality NHS Code of Practice
- Data Protection Act 2018
- Caldicott Guardian principles
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Access to Health Records 1990
- Records Management NHS Code of Practice
- Computer Misuse Act 1990
- Electronic Communications Act 2000
- Regulation of Investigatory Powers Act 2000
- General Data Protection Regulation (GDPR)

13. References

Data Security and Protection Toolkit
https://www.dsptoolkit.nhs.uk/

Data Protection Act 2018
http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Freedom of Information Act 2000
http://www.legislation.gov.uk/ukpga/2000/36/contents

Data Security and Protection Incident Reporting tool
https://www.dsptoolkit.nhs.uk/News/31

The NHS Constitution for England
https://www.gov.uk/government/publications/the-nhs-constitution-for-england/the-nhs-constitution-for-england

NHS Code of Confidentiality
https://www.england.nhs.uk/wp-content/uploads/2013/06/conf-policy-1.pdf

NHS Care Record Guarantee
http://systems.hscic.gov.uk/rasmartcards/documents/crg.pdf

NHS Information Risk Management
http://systems.hscic.gov.uk/infogov/security/risk

The Caldicott Review: Information Governance in the Health and Social Care System
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf

Access to Health Records Act 1990
http://www.legislation.gov.uk/ukpga/1990/23/contents

Government guidance Home and Mobile Working
https://www.gov.uk/government/publications/10-steps-to-cyber-security-advice-sheets/10-steps-home-and-mobile-working--11

General Data Protection Regulation (GDPR)
https://www.eugdpr.org/