NHS
West Essex
Clinical Commissioning Group

Information and Cyber Security Policy

Policy Reference: IG11

Brief Summary:
This policy is intended to inform all staff of their responsibilities in protecting information and information systems from unauthorised access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

Compliance with all CCG policies, procedures, protocols, guidelines, guidance and standards is a condition of employment. Breach of policy may result in disciplinary action.

Document Management

Version	Date Issued	Details	Brief Summary of Change	Author
0.1	03/11/2014	Draft	New Document. This Policy replaces South West Essex PCT IM&T Information Security Policy	CCGs Information Governance Team (Hosted by Basildon and Brentwood CCG)
0.2	03/12/2014	Draft	Amendments made following comments from the IG Steering Group	CCGs Information Governance Team (Hosted by Basildon and Brentwood CCG)
0.3	18/12/2014	Draft	Key Contacts Added following amendments	CCGs Information Governance Team (Hosted by Basildon and Brentwood CCG)
0.4	05/03/2015	Final	Approved by West Essex CCG	CCGs Information Governance Team (Hosted by Basildon and Brentwood CCG)
3.0	07/10/2016	Final	Review approved by West Essex CCG's Executive Committee	CCGs Information Governance Team (Hosted by Basildon and Brentwood CCG)

For more information on the status of this policy, please contact:	
NHS West Essex CCG	Information Governance Team
Approved by	Executive Committee
Approval Date	7th October 2016
Next Review Date	March 2019

Responsibility for Review	CCG's Information Governance Team
Audience	All NHS West Essex CCG officers and staff (which includes temporary staff, contractors and seconded staff).

Contents

1. Introduction

Information and cyber security has critical importance to NHS service users and to patient care, information assets and other related business processes. High quality information underpins the delivery of high quality evidence – based healthcare. Without effective security, NHS information assets may become unreliable, may not be accessible when needed, or may be compromised by unauthorised third parties. Information, whether in paper or electronic form, is of high importance to NHS West Essex Clinical Commissioning Group (the CCG), therefore the organisation must ensure that the information is properly protected and is reliably available.

Information security is primarily about people but is facilitated by the appropriate use of technology. The business benefits of this policy and associated guidance are:

- Assurance that information is being managed securely and in a consistent and corporate way
- Assurance that the CCG is providing a secure and trusted environment for the management of information used in delivering its business
- Clarity over the personal responsibilities around information security expected of staff (as defined in the scope) when working on the CCG business
- 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)
- Demonstration of best practice in information security
- Assurance that information is accessible only to those authorised to have access.

2. Purpose

The purpose of this policy is to protect, to a consistently high standard, all information assets, including patient and staff records (as defined in the scope) and other NHS corporate information, from all potentially damaging threats, whether internal or external, deliberate or accidental. The CCG has a legal obligation to ensure that there is adequate provision for the security management of the information resources the organisation own, control, or use.

3. Scope

This policy applies to all CCG staff. Compliance and responsibility also extends to those employed by the CCG as contractors, NHS professionals, temporary staff, voluntary organisations and anyone duly authorised to view or work with the CCG's information.

All references to information security are inclusive of cyber security measures.

The policy covers all forms of information held by the CCG, including but not limited to:

- Information about members of the public, service users and patients
- Non-CCG staff on CCG premises
- Staff (as defined in the scope) and personnel information
- Organisational, business and operational information

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

- Structured Record Systems – paper and electronic
- Information Recording and Processing Systems – Paper, Electronic, Video, Photographic and Audio Recordings
- Information Transmission Systems such as fax, e-mail, portable media, post and telephone.

4. Definitions and terms

Asset
Anything that has value to the organisation, their business operations and continuity.

Authentication
The organisation must ensure that the identity of a subject or resource is the one claimed.

Availability
The property of being accessible and usable upon demand by an authorised entity.

Business Impact
The result of an information security incident on business functions and the effect that a business interruption might have upon them.

Confidentiality
The property that information is not made available or disclosed to unauthorised individuals, entities or processes.

Cyber Security
Information and Cyber Security concerns the comprehensive risk management, protection and resilience of data processing and the digital networks that connect them.

Impact
The result of an information security incident, caused by threat, which affects assets.

Information Assurance

The confidence that information assets will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users.

Personal Confidential Data (PCD) is where an individual can be identified:
(a) From the data, or

(b) From the data and other information which is in the possession of, or is likely to come into the possession of the data controller and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual (Data Protection Act 1998).

5. Roles and Responsibilities

Accountable Officer for NHS West Essex CCG

The Chief Officer (CO), as the Accountable Officer, has overall responsibility for information governance within the CCG. The CO is responsible for the management of Information Governance and for ensuring appropriate mechanisms are in place to support service delivery and continuity.

The CO has delegated operational responsibility for information governance to the Director of Finance, Contracting and Performance.

Senior Information Risk Owner (SIRO) for NHS West Essex CCG

The role of Senior Information Risk Owner (SIRO) in the CCG has been assigned to the Director of Finance, Contracting and Performance. The SIRO takes ownership of the organisation's information risks policy and acts as advocate for information risk on the CCG Governing Body and Audit Committee. This includes oversight of information security incident reporting and response arrangements.

Caldicott Guardian for NHS West Essex CCG

The Caldicott Guardian has particular responsibilities for protecting the confidentiality of patients / service users information and enabling appropriate information sharing. For the CCG, this is an executive, the Chief Medical Officer. Acting as the 'conscience' of the organisation, the Caldicott Guardian will actively support work to enable information sharing where it is appropriate to share and will advise on options for lawful and ethical processing of information.

All Staff

All staff are required to comply with information security procedures including the maintenance of data confidentiality and data integrity. Each member of staff is responsible for the operational security of the information systems they use. Failure to do so may result in disciplinary action.

It is important that software on the PCs / systems used for work purposes must not be copied and used for personal use that may infringe on the organisation's system.

Staff must not load software onto their computer before first seeking advice / agreement from the IG Lead or ICT service provider – NEL CSU.

In order to ensure business continuity in the event of individual unavailability, all staff must ensure that information belonging to the organisation should not be stored on personal drives, in "My Documents", on the desktop or e-mail accounts.

Information Asset Owners (IAOs)

Information Asset Owners (IAOs) will act as nominated owner of one or more information assets they own. Their responsibilities will include:

- Documenting, understanding and monitoring 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
- Identifying information necessary in order to respond to incidents or recover from a disaster affecting the information asset
- Taking ownership via input, of their department / service area Information Asset Register, carrying out risk assessments on their local asset and management processes for the information assets they own, including the identification, review and prioritisation of perceived risk and oversight of actions agreed to mitigate those risks
- Providing support to the SIRO to maintain awareness of risks to all information assets
- Ensuring their staff are aware of, and comply with, Information Governance working practices.

Information Asset Administrators (IAAs)

Information Asset Owners can appoint Information Asset Administrators (IAAs) to support in the delivery of their information risk management responsibilities. Information Asset Administrators ensure that policies and procedures are followed, recognise actual or potential security incidents and take steps to mitigate those risks, consult with their Information Asset Owner on incident management and ensure that information asset registers are accurate and up to date.

Line Managers

Line Managers will take responsibility for ensuring that their staff are aware of:-

- Information security policies applicable in their work areas
- Personal responsibilities for information security
- How to access advice on information security matters

Line managers are responsible for the security of their physical environments where information is processed or stored.

6. Process Requirements

This policy will achieve a consistent approach to the security management of information throughout the CCG and will aim to deliver continuous business capability and minimise both the likelihood of occurrence and the impacts of information security incidents.

Security of our information is paramount and the protective measures put in place must ensure that Information Governance (IG) requirements are satisfied. The aim of this process is maintaining the confidentiality, integrity and availability of CCG information. To conform to the Information Security Assurance requirements of Health & Social Care Information Centre IG Toolkit the CCG shall:

Maintain the Confidentiality of Personal Information including patients and staff (as defined in the scope) identifiable information by protecting it in accordance with NHS Information Security Code of Practice, Data Protection Act, Caldicott Principles and other legal and regulatory framework criteria.

Ensure the integrity of the CCG information by developing, monitoring and maintaining it to a satisfactory level of quality for use within the relevant areas.

Implement the necessary measures to maintain availability of the CCG information systems and services. This includes putting in place contingency measures to ensure the minimum of disruption caused to the CCG information systems and services.

The CCG will provide specific guidance and instruction to staff in the relevant policies and procedural documents. For example security of personal information is explained in the ***Safe Haven Policy and Information Governance Resource Guide.***

Safety uses of computers and other electronic communications including portable and mobile device systems can be found on the CCG's policy on ***Acceptable Use of Electronic Communications and Portable Devices.***

Some key areas of information security and risk management include:
Physical Security

The physical security of the organisation's information is the responsibility of all staff. The protection of both personal and non-personal information is paramount in maintaining confidentiality and users of the organisation's information must comply with the suite of Information Governance documentation. This is a local information security policy to protect the information stored, processed and exchanged between the CCG and its partner organisations.

The physical environment must be recognised as providing a layer of protection to data and information. This is achieved by the following means:

- Controlling access to sites, buildings and offices

- Ensuring desks and work areas are clear at the end of each day
- Use of locked cabinets within offices to restrict access to information
- Checking that visitors to sites are authorised to be there
- Ensuring that when information is carried off site, it is held securely in a locked case
- Always wearing your ID badge when on site.

Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain an appropriate confidentiality clause. Information security expectations of staff shall be included within appropriate job definitions.

Mobile Devices

- Portable devices, for example, laptops must be encrypted and kept in locked storage. Removable media must be encrypted and must not be the only source of the information (that is the information must also be stored in a secure folder on the shared drive). Such media must be kept in locked storage.

- Removable media must only be installed by the ICT service provider. Personally owned removable media devices must not be used to store or transfer any confidential information without seeking permission. Each user of such media is responsible for the appropriate use and security of data stored on the media.

Viruses and Malware

All IT equipment used by staff is protected by countermeasures and management procedures to protect against the threat of malicious software. All staff shall be expected to co-operate fully with this policy. Users shall not install software on the organisation's property without permission from the IT service provider.

Preventing Information Security Breaches

Each department/service area is responsible for regularly monitoring the information they hold and use. An annual mapping exercise of information flows in and out of the teams will be undertaken. This exercise will allow any information risks to be identified by each team and appropriate action to mitigate those risks should be taken. It is the responsibility of the Information Asset Owner (IAO) to ensure that this takes place.

Protection against unauthorised access or disclosure

Staff have a responsibility to ensure that information is kept secure when being processed or transferred by adhering to the following:

- Screens should be locked when unattended even for short periods of time

- Acceptable Use of Electronic Communications and Portable Devices Policy.
- Guidance provided on the use of fax, 'phones and post which can be found within the Safe Haven Policy.

The ICT service provider – North East London CSU will ensure that all computer software supplied used is regulated by license agreements and that new operational software is quality assured.

The CCG will ensure that paper information is secure by following adequate records management procedures and processes. Staff should have access to secure storage areas and if possible, a clear desk routine should be followed. Should a legitimate need arise for local storage or a non-routine transfer of confidential information then a risk assessment must be undertaken first and the justification approved by the Caldicott Guardian and recorded by the line manager. All staff must also ensure when moving away from desks that they do not leave person identifiable / sensitive information available for others to view by putting it in a drawer or covering it up.

Any non-routine bulk extracts (50+ records) or transfers of particularly confidential or sensitive data must be authorised by the responsible Information Asset Owner (IAO) for the work area and may require approval by the Senior Information Risk Owner (SIRO).

Potential or Actual Information Security Breaches

All staff are responsible for ensuring that no potential or actual security breaches occur as a result of their actions.

The IAO must be informed of all security issues in order to ensure that the appropriate investigations are carried out.

Depending on the impact of the incident, external organisations such as NHS Digital (formerly HSCIC), NHS England and the Information Commissioner's Office (ICO) may be informed.

The resulting root cause analysis (RCA) report will specify details of the suspected incident, the assets affected or compromised and the investigation conducted. Recovery / contingency plans, damage and risk classification and recommendations will be provided.

All incidents will be investigated immediately and reported in a timescale appropriate to the initial risk assessment. Reports and recommendations will be approved and monitored by the IG Lead.

7. Risk

The CCG will ensure that adequate audit provision is in place to ensure continuing effectiveness of information security management arrangements.

Any security measures must be viewed as necessary protection against a risk of an event occurring or to reduce the impact of such an incident. Some of these events may be deliberate acts of damage and others may be accidental. Nevertheless, a range of security measures can be deployed to address:

- The ***threat*** of something damaging the confidentiality, integrity or availability of information held on systems or manual records.
- The ***impact*** that such a threat would have if it occurred.
- The ***likelihood*** of such a threat occurring.

All staff should consider the risks associated with the computers they use and the information that is held on them, as well as information held in manual records

All staff are responsible for reporting any apparent shortcomings of security measures currently employed to address these risks to the risk lead within the organisation.

8. Information Disposal

Electronic

Computer assets must be disposed of in accordance with the IT service provider disposal of confidential waste procedure. This includes removable computer media such as tapes and disks.

All data storage devices must be purged of sensitive data before disposal. Where this is not possible, the equipment or media must be destroyed by a technical waste service provider.

For further information, please contact the IT service provider.

Paper

Printed matter should be confidentially destroyed using an appropriate method such as shredding.

9. Access Controls

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

User access controls information will be restricted to authorised users who have a bona-fide business need to access the information.

Computer access control facilities will be restricted to authorised users who have a business need to use them.

Application access control to data, system utilities and program source libraries will be controlled and restricted to authorised users who have a legitimate business need, for example systems or database administrators.

Authorisation to use an application will be dependent upon the availability of a license from the supplier.

10. Use and Installation of Software

The IT service provider – NEL CSU will ensure that:

- Security issues are considered and documented during the requirements phase and the procurement phase of all system procurements and developments. Minimum security standards must be incorporated in all new systems
- System test and live data are separated and adequately protected. All changes to the system must pass through a formal change control procedure
- Computer assets such as removable media, backup tapes and disks are adequately disposed of.

11. Data and Information Backup

NEL CSU will ensure that data located upon network servers is backed up in accordance with the written network back-up procedure. Such information is to be stored off-site as required to facilitate a maximum loss of one calendar week of information destroyed as a result of local building or system damage.

12. Audit and monitoring compliance

The CCG will use a variety of methods to monitor compliance with the processes in this policy, including as a minimum the following method/s:

IG Incidents

Information Governance compliance will be monitored quarterly through the monitoring of reported IG incidents by the IG Steering Group.

The IG Steering Group has responsibility for providing assurances that this policy is adequate for providing clear guidance in the event of significant changes which may affect it. The IG Lead will ensure that adequate arrangements exist for:

- Reporting incidents and Caldicott issues.
- Analysing and upward reporting of incidents and adverse events.
- Reporting IG work programs and progress reports.

- Reporting Information Governance Toolkit (IGT) assessments and improvement plans.
- Communicating IG developments.

In addition to the monitoring arrangements described above the CCG may undertake additional monitoring of this framework as a response to the identification of any gaps, or as a result of the identification of risks arising from the framework prompted by incident review, external reviews or other sources of information and advice.

13. Dissemination and implementation

The policy will be published on the organisation's intranet. Managers are required to ensure that their staff understand its application to their practice. Awareness of any new content or change in process will be through electronic channels e.g. through email, in bulletins etc.

Where a substantive revision is made then a separate plan for communicating and implementing this change will be devised by the SIRO.

14. Training

All staff likely to be in post 3 months or longer (permanent, temporary, contracted or seconded) are required to complete the online mandatory IG training modules (https://www.igtt.hscic.gov.uk/igte/index.cfm) within one month of joining, with further training required for managers / team leaders, staff who process personal information, and staff with specific information roles. A Training Needs Analysis (TNA) has been developed for staff in key roles, as part of effective delivery of training program.

However, should staff have access to personal identifiable information, training should be completed within 1 week, regardless of intended service length.

15. Related documents

The following documentation relates to the management of information and together underpins the CCG's Information Governance Assurance Framework. This policy should be read in conjunction with other policies:

- Information Governance Policy
- Confidentiality and Data Protection Policy
- Information Lifecycle Management Policy, Procedures and Strategy

- Acceptable Use of Electronic Communication and Mobile Devices Policy
- Safe Haven Policy

16. Equality and Diversity

The CCG recognises the diversity of the local community and those in its employment. The CCG aims to provide a safe environment free from discrimination and a place where all individuals are treated fairly, with dignity and appropriately to their need. This document has been assessed for equality impact on the protected groups, as set out in the Equality Act 2010.

This Policy is applicable to every member of staff within the CCG irrespective of their age, disability, sex, gender reassignment, pregnancy, maternity, race (which includes colour, nationality and ethnic or national origins), sexual orientation, religion or belief, marriage or civil partnership.

17. Key Contacts within the CCG

Senior Information Risk Owner	Director of Finance, Contracting and Performance
Caldicott Guardian	Chief Medical Officer
CCG IG Champion	Governance and Risk Manager

Information Governance Team

Jane Marley	Head of Information Governance	jane.marley@nhs.net
Tracey van Wyk	IG Lead	tracey.vanwyk@nhs.net
Ian Gear	FOI Lead	iain.gear@nhs.net
Debbie Smith-Shaw	Information Governance Adviser	debbie.smith-shaw@nhs.net