NHS
Barnsley
Clinical Commissioning Group

BARNSLEY CLINICAL COMMISSIONING GROUP'S INFORMATION SECURITY POLICY

December 2020

Version:	4.0
Approved By:	Governing Body
Date Approved:	13 February 2014 (approved) February 2016 (first review), March 2018 (second review) December 2020 (third review)
Name of originator / author:	Gershon Nubour
Name of responsible committee/ individual:	Governing Body (Initial approval) Information Governance Group & QPSC (review)
Name of executive lead:	Head of Governance & Assurance
Date issued:	March 2021
Review Date:	3 years from approval
Target Audience:	Barnsley CCG staff

THIS POLICY HAS BEEN SUBJECT TO A FULL EQUALITY IMPACT ASSESSMENT

Amendment Log

Version No	Type of Change	Date	Description of change
DRAFT		January 2014	
1.0		13 February 2014	*Approved by Governing Body*
2.0	Review	Feb 2016	*Added contents page* *Footnotes rationalised* *References to CSU changed to commissioning support services* *Added requirement not to leave confidential information in cars.* *References to obsolete equipment removed* *Section 4.4.6. Requirement to guard against inappropriate access*
3.0	Review	March 2018	*Added reference to GDPR* *Explicit 72 hour limit for incident reporting added* *PIAs referenced* *Additional IT safeguards added* *Limit on the use of internet hosted systems introduced* *CareCert Alert assurances required from IT suppliers* *Cyber security responsibilities detailed* *Deleted ownership claim to all information*
4.0	Review	December 2020	*Replaced references to EMBED* *Updated relevant legislation* *Added Section covering temporary access* *Added section on the risks of not having this policy, and also monitoring & compliance*

CONTENTS

Information Security Policy

1. Introduction

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

2. Objectives and Principles

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

i. Setting out a framework for information security;
ii. Promoting a culture of information security within the CCG and
iii. Ensuring staff understand their responsibilities in relation to information security.

2.2 The information security policy will ensure that:

- The CCG has a Governing Body approved Senior Information Risk Owner (SIRO)
- Each Information Asset has a responsible owner (Information Asset Owner)
- Information is protected against unauthorised access and/or misuse
- The confidentiality of information is assured
- The integrity of information is maintained
- Information is available when required
- Business continuity plans are produced, maintained and tested
- Compliance with regulatory, legal and contractual obligations is maintained[2]
- Training around information / data security is provided to all staff
- All breaches of information security, actual or suspected are reported and investigated through the appropriate management channels (see section 4.8)

2.3 Controls and procedures will be produced to support this policy and implement the framework. These will be maintained as part of a suite of information governance policies and posted on the CCG's intranet.

2.4 *The risks of not having this policy in place*

If the CCG did not have this policy there would be an increased risk of data security breaches with potential adverse consequences for the CCG in terms of DSP toolkit compliance, reputational risks, and an inability to carry out its functions effectively. There is also the potential for financial loss.

[1] An information asset is a system which holds or processes information and may be electronic or paper-based(manual)

[2] Including compliance with the Data Protection Act, General Data Protection Regulation, Computer Misuse Act 1990 and any other relevant legislation and regulations.

3. Scope

This policy applies to the following areas:

3.1 Systems

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

3.2 Users

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

3.3 Information

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

4. Framework for Information Security

4.1 Management of, and Responsibility for, Information and Cyber Security

- The Accountable Officer has ultimate responsibility for information security within the CCG. This is delegated to the Senior Information Risk Owner.
- The CCG's Senior Information Risk Owner is responsible for implementing, monitoring, documenting and communicating Information Security and Cyber Security Requirements for the CCG, with assistance from IT Services and the Information Governance Team.
- Departmental and line managers are responsible for information security within their area or work and for ensuring their staff[3] are aware of this policy and associated procedures and their duty to comply. They must ensure all their key information assets have an identified responsible owner (Information Asset Owner).
- Information Asset Owners are responsible for identifying and managing the risks associated with their asset. This includes carrying out Data Protection Impact Assessments (DPIAs) when new systems and processes are introduced, or significant changes are made to existing ones

[3] This includes all individuals for whom the manager is responsible including but not limited to: permanent and temporary staff, staff on secondment, contractors, students on placement, volunteers etc.

- The CCG must obtain regular assurances from core IT suppliers that CareCert alerts, covering data security and provided to all NHS organisations, are being addressed appropriately.
- IT Services will provide Cyber Security assurances for the IT systems and infrastructure it manages for the CCG.
- The CCG will ensure other third party suppliers processing data on its behalf are contractually required to put in place appropriate levels of cyber security controls and safeguards, both organisational and technical.
- Individuals have a personal responsibility for adhering to this policy and associated information governance procedures.
- Failure to comply with the policy and associated procedures may have serious consequences for the individual including civil, criminal and disciplinary proceedings.

4.2 Contracts of Employment

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

4.3 Information Security Awareness Training

- Information security awareness training is included in the staff induction process.
- An on-going programme of awareness is established to ensure that staff awareness is refreshed and updated. This includes the completion of annual Data Security Awareness e-learning.
- The Senior Information Risk Owner and Information Owners are required to undertake mandatory training as per the IG Training Strategy.

4.4 Information Security Procedures

- The security of paper and electronic records, computers and networks is controlled by procedures that have been authorised by the appropriate authority within the CCG, or commissioning support services, where the asset is provided under contract to, or managed on behalf of, the CCG.

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

4.4.1 Security of Equipment and Records

- In order to minimise loss of, or damage to, all assets, all equipment and information storage areas are physically protected from security threats and environmental hazards.
- Confidential information and laptops must not be left in cars overnight, or for extended periods of time
- Confidential information held in hard copy (paper) must be kept secure at all times.
- Confidential CCG information must not be stored on local hard drives such as PCs, lap tops or other portable devices unless authorised by the Head of Assurance.
- Any confidential information held on portable devices must be encrypted.
- Databases of personal, that is, service user information and staff information, must not be created without prior permission from the Head of Assurance.
- Current databases of personal information must be notified to the Head of Assurance.
- No unsupported, or out of warranty systems; operating systems; software or applications shall be used for CCG business without permission of the SIRO.

- All operating systems and applications used for CCG business must be kept up to date using available and appropriate software updates.
- The use of internet hosted services for handling confidential/ personal information requires the approval of SIRO / IG Group and may involve risk assessments and the completion of a DPIA.

4.4.2 Location Access Controls

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

4.4.3 User Access Controls

- Access to information and information systems, whether electronic or manual, is restricted to authorised users who have an identified need as agreed with their line manager or sponsor.
- Access to electronic information systems is given at the appropriate level for the agreed need.
- Person confidential data may only be stored within operational systems or within a safe haven/ location with restricted access.

4.4.4 Information Communication Technology (ICT) Access Controls

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

4.4.5 Connection to the CCG Network

- All devices connected to the CCG network are governed by the CCG's Information Governance Statement of Compliance.
- The connection of any equipment to the CCG network requires authorisation from IT Services.
- All electronic processing devices connecting to the CCG network must be protected by up to date anti-virus software. Where the device does not update automatically, it is the responsibility of the user to ensure that the anti-virus software is up to date.
- Personally owned devices must not be directly connected to the CCG's internal network.
    - Directly connected means either by wire (network cable) or Wi-Fi.
    - The CCG's internal network includes Library or personal drives, databases or intranet.
    - Personally owned means devices that are not provided by the CCG or other NHS organisation.
    - Devices includes home personal computers, laptops, tablet computers (for example, iPads), media players (such as iPods) and smartphones.
- The CCG has the facility to allow non-NHS provided devices to connect to the internet via a Wi-Fi connection. This should be authorised by the IT Department - Ask the IT Service Desk for advice.
- External visitors may connect to the internet via a Guest Wi-Fi account.

4.4.6 Remote Working

- Information that is taken off site must be authorised by line management, kept secure at all times and where held on portable computers, backed up regularly.

- All reasonable steps must be taken to protect against loss; theft; inappropriate access by patients their families; inappropriate access by the employee's family members.
- Portable devices must be used in line with CCG policy and protected by appropriate security (see Remote Working and Portable Devices Policy). Working from home must be authorised by line management and comply with policies relating to information governance and home working.

4.4.7 Portable Devices

- The use of portable devices for work purposes must be in line with CCG policy and authorised by your line manager (and Information Governance/IT Services where appropriate). (See Remote Working and Portable Devices Policy)
- Only portable devices that have been provided / authorised for use by IT Services may be used for work purposes. This includes, but is not limited to, laptops, tablets such as iPads, USB sticks, digital dictation machines, smart phones.
- Personally owned portable devices such as laptops and iPads must not be directly connected to the NHS Barnsley Clinical Commissioning Group network either by wire (network cable) or Wi-Fi (refer to section 4.4.5 above)
- The CCG has the facility to allow non-NHS Barnsley Clinical Commissioning Group provided portable devices to connect to the internet via a wireless connection. (refer to section 4.4.5 above).
- Portable storage devices (including CDs, DVDs and flash drives) containing software or data from external sources, or that have been used in external equipment, must be fully virus checked before being used on CCG equipment and must be protected by proper security (ask the IT Service Desk for advice).
- All portable devices must be protected by appropriate security. Portable devices such as laptops, tablets (for example, iPads), dictation machines smart phones and USB sticks must be encrypted and, where appropriate, have up to date anti-virus software.
- Portable devices used to store email from NHSMail must be encrypted and have the capacity, and be configured, to allow remote wiping.

4.5 Malicious and Unauthorised Software

- The CCG will use countermeasures and management procedures to protect itself against the effects of malicious software. All staff are expected to co-operate fully with this requirement.
- Users must not install software on CCG equipment without permission from the IT Service Desk.

4.6 Monitoring System Access and Use

- Audit trails of system access and use are maintained and reviewed on a regular basis as well as during CCG investigations.
- Dormant or unused accounts will be disabled and may be deleted when identified.
- Measures to limit suspicious logins and excessive or adverse systems use may be implemented if deemed appropriate.

4.7 Temporary IT Access for Contractors and Other Organisations

Contracts with external organisations that allow access to the CCG's information systems shall be in operation before access is allowed. These contracts shall ensure that the staff or sub-contractors of the external organisation shall comply with all appropriate security policies.

It is the responsibility of the manager who oversees the contract or employees from another organisation are properly inducted if they require access to the CCG network or information systems. They are also responsible for arranging the access to all necessary information and IT systems at an appropriate level, in line with relevant local procedures, to adequately perform their duties.

System managers are responsible for ensuring procedures are in place to issue separate individual accounts with appropriate levels of access to these users and to ensure that passwords are changed regularly and meet minimum password security standards.

Access to the Internet and NHSMail email services must be authorised by the line manager and accessed in compliance with the relevant CCG policies.

Where provided, NHSMail use should be used in accordance NHSMail Acceptable Use Policy and the CCG Email Policy.

It is the responsibility of the managers who oversees the contract or employees from another organisation, to immediately inform the IT Service Desk of any individual that no longer requires access to the CCG network or IT systems

It is good practice for the line managers and systems manager to consult when deciding on the level of access that staff require, taking into consideration such issues as segregation of duties and sharing of expertise.

4.8 Business Continuity

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

4.9 Reporting Security Incidents and Weaknesses

- All information management and technology security incidents, near misses and weaknesses must be reported immediately via CCG incident reporting procedures.
- Incidents that present an immediate risk to the CCG such as viruses should be reported to the IT Service Desk immediately.
- The CCG is required by law to report all serious Information Security Breaches within 72 Hours to the Regulatory Authorities. Delays to reporting are a breach of the law which could result in action being taken against the CCG

4.10 Reporting to the Information Governance Group

- The Head of Governance and Assurance (the SIRO) will keep the Information Governance Group and / or Quality and Patient Safety Committee informed of the information security status of the CCG by means of regular reports.

5. Legislation and Guidance

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

- Common Law Duty of Confidentiality
- Data Protection Act 2018
- UK General Data Protection Regulation
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Protection of Freedoms Act 2012
- Health and Social Care Act 2012
- Regulation of Investigatory Powers Act 2000
- Copyright, Designs and Patents Act 1998
- Statement of Compliance
- Confidentiality: NHS Code of Practice
- Records Management: NHS Code of Practice
- Information Security: NHS Code of Practice

And any relevant guidance related to the following:

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

6. Further information

Further information can be obtained from the CCG's Information Governance Lead.

Questions about the use of portable devices or any problems in accessing the CCG system should be directed to the IT Service Desk. Support is available during opening hours. There is no out of hours or home support.

7. Monitoring and compliance

This policy will be reviewed every three years by the CCG's IG Lead in accordance with the CCG's corporate approach, or sooner if necessary in the light of regulatory or legislative changes. Updates to the policy will be approved via the IG Group and Quality & Patient Safety Committee. Compliance with the policy will be assured through the annual DSP Toolkit self-assessment and audit process.

Equality Impact Assessment

NHS Barnsley Clinical Commissioning Group

Title of policy or service:	Information Security Policy	
Name and role of officer/s completing the assessment:	Gershon Nubour	
Date of assessment:	10 Dec 2020	
Type of EIA completed:	**Initial EIA 'Screening'** ☒ ***or*** **'Full' EIA process** ☐	*(select one option)*

1. Outline	
Give a brief summary of your policy or service • including partners, national or regional	• Setting out a framework for information security; • Promoting a culture of information security within the CCG and • Ensuring staff understand their responsibilities in relation to information security.
What Outcomes do you want to achieve	• Key Safeguards to maintain IT security are documented • The confidentiality, integrity and availability of the CCG's information is assured • Compliance with regulatory, legal and contractual obligations is maintained
Give details of evidence, data or research used to inform the analysis of impact	A draft of this policy has been circulated for review by the following:- • BCCGs Information Governance Group, • BCCGs Quality Patient Safety Committee, The final policy has been signed off by BCCGs Chief Nurse, the Head of Governance and Assurance and the Information Governance Manager (eMBED)

Give details of all consultation and engagement activities used to inform the analysis of impact	As above

Identifying impact:

- **Positive Impact:** will actively promote the standards and values of the CCG.
- **Neutral Impact:** where there are no notable consequences for any group;
- **Negative Impact:** negative or adverse impact: causes or fails to mitigate unacceptable behaviour. If such an impact is identified, the EIA should ensure, that as far as possible, it is eliminated, minimised or counter balanced by other measures. This may result in a 'full' EIA process.

2. Gathering of Information

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

	What key impact have you identified?			**For impact identified (either positive or negative) give details below:**	
(Please complete each area)	**Positive Impact**	**Neutral impact**	**Negative impact**	**How does this impact and what action, if any, do you need to take to address these issues?**	**What difference will this make?**
Human rights	☐	☒	☐		
Age	☐	☒	☐		
Carers	☐	☒	☐		
Disability	☐	☒	☐		
Sex	☐	☒	☐		

Race	☐	☒	☐		
Religion or Belief	☐	☒	☐		
Sexual Orientation	☐	☒	☐		
Gender Reassignment	☐	☒	☐		
Pregnancy and Maternity	☐	☒	☐		
Marriage and Civil Partnership (only eliminating discrimination)	☐	☒	☐		
Other Relevant Groups	☐	☒	☐		
HR Policies Only:	☐	☐	☐		

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

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

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

4. Monitoring, Review and Publication			
When will the proposal be reviewed and by whom?	The EIA will be reviewed when the policy is reviewed. The Head of Assurance is responsible for ensuring the review takes place.		
Lead / Reviewing Officer:	Richard Walker	**Date of next Review:**	March 2020

Once completed, this form **must** be emailed to the Equality Lead barnsleyccg.equality@nhs.net for sign off:

Equality Lead signature: 
Date: 13.07.18