NHS
Scarborough and Ryedale
Clinical Commissioning Group

Information Security Policy
November 2017

Authorship:	Information Governance Manager (eMBED)			
Committee Approved:	Audit and Governance Committee			
Approved date:	10 November 2017			
Review Date:	10 November 2020			
	Relevant	Screening	Full / Completed	Outcome
Equality Impact Assessment	Yes	Yes	No	No issues identified
Sustainability Impact Assessment	Yes		Yes	No issues identified
Privacy Impact Assessment	No	No	No	Not Applicable
Bribery Checklist	No		No	Not Applicable
Target Audience:	All CCG Staff			
Policy Reference No:	P705			
Version Number:	V2.0			
Publication/Distribution	Website	Email Staff	Others (i.e. SBC)	
	Yes	Yes	Yes	

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

POLICY AMENDMENTS

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

New Version Number	Issued by	Nature of Amendment	Approved by & Date	Date on Intranet
1.0	Barry Jackson	Approved version	Feb 2014	
1.1	IG Team	To add guidance re encryption and cloud storage	Dec 2014	
1.1	IG Officer	Reviewed no updates therefore review date reset to Sept 17	N/A	
2.0	IG Officer	To update for changes in organisational relationships (CSU to Embed) To update for the requirements of the General Data Protection Regulation	November 2017	17/11/17

Approval Record

Applicable Y/N	Committee / Group	Consultation / Ratification	Date taken to group	Date last Approved
	Governing Body	Ratification		
	Council of Clinical Representatives	Ratification		
	SMT	Ratification		
	Remuneration Committee	Ratification		
Yes	Audit and Governance Committee	Ratification	November 2017	November 2017
	Finance and Contracting Committee	Ratification		
	Business Committee	Ratification		
	Communications and Engagement Committee	Ratification		
Yes	Quality and Performance Committee	Ratification	February 2014	February 2014
	Other	Ratification		
	All Employees	Consultation		
	Public	Consultation		
	Yorkshire and Humber Social Partnership Forum	Consultation		

Contents

1 INTRODUCTION

Information and information systems are important assets to every organisation and it is essential to take all the necessary steps to ensure that they are comprehensively protected, available and accurate to support the operation and continued success of the CCG at all times.

The Information Security Policy is a key component of the CCGs overall information security management framework and is designed to:

- provide a corporate framework in which security threats to our Information Systems can be identified and managed;
- illustrate the CCGs commitment to the security information and information systems;
- provide accepted formal procedures to ensure a uniform implementation of security measures;
- introduce and formalise procedures to minimise the risk of unauthorized modification, destruction or disclosure of information; and
- align the organisation to the NHS Information Governance aims and expectations described in the Information Security Management: Code of Practice for NHS Organisations.

Note: these objectives can only be achieved if every staff member observes the highest standards of personal, ethical and professional conduct in relation to the handling and management of information.

1.1 Requirement for Security Policy.

The CCG acknowledges that information is a valuable asset, therefore it is within its interest to ensure that the information it holds is suitably protected from any threat. By protecting its information the CCG is acting in the best interests of its employees and all third parties with whom information is shared whilst minimising key risks associated with information processing:

- legal action due to non-compliance with statutory and regulatory requirements
- loss of public confidence in the CCG
- contribution to clinical or corporate negligence
- Key issues addressed by the Security Policy are:-
- Availability - information is delivered to the right person when it is needed.
- Confidentiality - data access is confined to those with specified authority to view the data;
- Integrity - all system assets are operating correctly according to specification and in the way the current user believes them to be operating; and

The CCG intends to achieve a standard of excellence in Information Governance by ensuring all information is dealt with legally, securely, efficiently and effectively in order to support the delivery of high quality patient care, service planning and operational management. For this to be achieved information processing must

comply with legislation and best practice and the CCG will establish and implement policies and procedures to ensure appropriate standards are defined, implemented and maintained.

1.2 Legal Compliance

The CCG is bound by the provisions of a number of items of legislation affecting the stewardship and control of patient and other information. The main relevant legislation is:

- The Data Protection Act 1998;
- General Data Protection Regulation 2016
- Access to Health Records Act, 1990
- Computer Misuse Act, 1990;
- Copyright, Designs and Patents Act, 1988 (as amended by the Copyright (Computer Programs) Regulations, 1992;
- Crime and Disorder Act, 1998; and
- The Human Rights Act 1998.

This policy describes the way in which information should be managed, in particular, the way in which personal or sensitive information should be protected. In addition to the above, other legislation can impact upon the way in which we should use personal information. This includes:

- Public Interest Disclosure Act 1998;
- Audit & Internal Control Act 1987;
- Public Health (Code of Practice) Act 1984;
- NHS (VD) Regulations 1974;
- National Health Service Act 1977;
- Human Fertilisation & Embryology Act 1990;
- Abortion Regulations 1991;
- The Terrorism Act 2000;
- Road Traffic Act 1988;
- Regulations under Health & Safety at Work Act 1974.
- Regulation of Investigatory Powers Act 2000.
- Freedom of Information Act 2000.

Much of the legislation mentioned is available in electronic format, via the Internet (www.legislation.hmso.gov.uk). In addition, the CCG is bound by the confidentiality aspects of common law and the Caldicott guidance on protection of patient information.

As part of, and in addition to, the above legislation the CCG is required to retain all records (health and administrative) for specified periods of time. For further information on this see the Records Management Policy.

2 ENGAGEMENT

This policy has been developed based on the knowledge and experience of the Information Governance team. It is derived from a number of national codes and policies which are considered as best practice and have been used across many public sector organisations.

3 IMPACT ANALYSES

3.1 Equality

An equality impact screening analysis has been carried out on this policy and is attached at Appendix 1.

As a result of performing the analysis, the policy, project or function does not appear to have any adverse effects on people who share *Protected Characteristics* and no further actions are recommended at this stage.

3.2 Sustainability

A sustainability assessment has been completed and is attached at Appendix 2. The assessment does not identify and benefits or negative effects of implementing this document.

4 SCOPE

- All employees of the CCG
- CCG Governing Body
- Contracted third parties (including eMBED and agency staff)
- Students and trainees
- Staff on secondment and other staff on placement with the CCG

5 POLICY PURPOSE AND AIMS

5.1 Operating Procedures and Standards

5.1.1 Compliance

It is the policy of the CCG to ensure compliance, in accordance with all the legislative obligations. The CCG also requires all employees, contractors and third parties to comply with this policy and supporting standards and procedures where appropriate.

5.1.2 Information Security Awareness and Education

It is the responsibility of all employee's and third parties of the CCG to sustain excellent information security. To comply with this, the CCG requires all employees and contractors within scope to understand the importance of information security and be familiar with this document, and supporting documents where appropriate.

To facilitate this information governance training will be included in the staff induction process and as an annual requirement in order to ensure staff awareness is refreshed and updated as necessary.

5.1.3 Contracts of Employment

Staff security requirements shall be addressed at the recruitment stage and all contracts of employment will contain a confidentiality clause. In addition information security expectations of staff shall be included within appropriate job definitions.

5.1.4 Email and Electronic Systems

The CCG has clear standards relating to the use of e-mail, Internet and intranet and the deliberate or accidental misuse of electronic systems. The procedures cover use of any systems used to store, retrieve, manipulate and communicate information (e.g. telephone, fax, e-mail, IT systems and the Internet). All employees and third parties are required to familiarise and adhere to them.

5.2 Access Controls

5.2.1 Physical Security:

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

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

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

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

5.2.2 User Access Controls:

Access to information shall be restricted to authorised users who have a bona-fide business need to access the information.

5.2.3 Computer Access Controls:

Access to computer facilities shall be restricted to authorised users who have business need to use the facilities.

5.2.4 Application Access Control:

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators.

The CCG has a procedure outlining the control of access to its premises, physical assets and electronic networks. Procedures also cover correct use of its assets. All employees and third parties are required to acquaint themselves with these standards.

5.2.5 Computer and Network Procedures

Management of computers and networks shall be controlled through standard documented procedures that have been authorised by the Associate Director of Corporate Affairs (SIRO).

5.2.6 Information Risk Assessment

Once identified, information security risks shall be managed on a formal basis. They shall be recorded within the Information Asset Register and action plans shall be put in place to effectively manage identified risks. The Information Asset Register and all associated action plans shall be reviewed quarterly by Information Asset Owners. Any implemented information security arrangements shall also be a regularly reviewed feature of the CCGs risk management programme. 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.

5.2.7 Information Security Events and Weaknesses

All information security events and suspected weaknesses are to be reported via the CCGs Incident Management process to the Associate Director of Corporate Affairs (SIRO).

All information security events shall be investigated to establish their cause and impacts with a view to avoiding similar events.

5.2.8 Classification of Sensitive Information – [Pending New Guidance]

The CCG will implement information classifications controls, based upon the results of formal risk assessment and guidance contained within the IG Toolkit to secure their NHS information assets. For more information on information classification is contained within the CCG Records Management Standard and Procedures.

5.2.9 Protection from Malicious Software

The CCG will use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff shall be expected to co-operate fully with this policy. Users will not install software on the CCGs property without permission from the Associate Director of Corporate Affairs (SIRO). Users breaching this requirement may be subject to disciplinary action.

5.2.10 User Media

The CCG will use port control software to control the use of removable media. Access to USB mass storage devices and CD/DVD writers will be restricted to approved users only.

Where removable media is received from external sources or has been used on computers systems not owned by the CCG users are required to scan the media using anti-virus software before its use.

All removable magnetic media must be encrypted. Failure to do this may result in disciplinary action.

5.2.11 Encryption

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.

To ensure data security on other media types, along with port controls described above, only encrypted removable media will be sanctioned for use. Any USB removable media will be required to meet UK eGovernment Interoperability Framework standards for encryption.

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

5.2.12 Online or Cloud Storage

The use of online or cloud storage is prohibited and staff should not use any service that has not been provided through the Embed IMT department. Some device manufactories provide cloud based storage options with their products. If you setup your work supplied device or use your own device you will be responsible for ensuring that any data on the device does not synchronise with the cloud.

5.2.13 Accreditation of Information Systems

The CCG shall ensure that all new information systems, applications and networks include a security policy and are approved by the Associate Director of Corporate Affairs (SIRO) before implementation.

System specific security policies will be developed for systems under CCG control in order to allow granularity in the security management considerations and requirements of each. This may result in specific responsibilities being assigned and obligations communicated directly to those who use the system.

5.2.14 System Change Control

Changes to information systems, applications or networks shall be reviewed and approved by the Head of IM&T or authorised officer.

5.2.15 Intellectual Property Rights

The CCG shall ensure that all information products are properly licensed and approved by the Associate Director of Corporate Affairs (SIRO).

Users shall not install software on the organisation's property without permission from the Associate Director of Corporate Affairs (SIRO). Users breaching this requirement may be subject to disciplinary action.

5.2.16 Business Continuity and Disaster Recovery Plans

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.

It is the responsibility of all employees and contractors to familiarise themselves, as appropriate, with the business continuity plan that supports this policy.

5.2.17 Reporting

The Associate Director of Corporate Affairs (SIRO) will keep the Senior Management Team informed of the information security status of the organisation by means of regular reports and presentations.

5.2.18 Policy Audit

This policy will be subject to regular independent audit and annual assessment in line with the completion of the Information Governance Toolkit by internal and external audit.

5.2.19 Physical Security

All staff are responsible for the physical security of assets, equipment and building used by the CCG. Appropriate physical security measures shall be put in place to secure information assets dependant on value and sensitivity to the organisation.

All staff are responsible for ensuring that buildings are left is a secure state when vacant.

5.2.20 Policy Violations

It is a condition of employment with the CCG that compliance should be maintained where appropriate with the information security management policy, and supporting standards and procedures.

If any procedures or policies are violated these will be treated as security incidents, and reported in accordance with the CCGs incident reporting procedure. Failure to comply with this policy, or supporting procedures, could result in disciplinary action.

6 ROLES, RESPONSIBILITES AND DUTIES

Policy review and maintenance	Chief Finance Officer / SIRO
Approval CCG	Audit and Governance Committee
Adoption	All manager, staff and contractors

Responsibility for Information Security will reside with the CCG Senior Management Team. On a day-to-day basis the Associate Director of Corporate Affairs (SIRO) will be responsible for implementing, managing, monitoring, documenting and communicating the security requirements for the organisation.

Line Managers are responsible for ensuring that their permanent and temporary staff and contractors are aware of:

- the information security policies and procedures applicable in their work areas;
- their personal responsibilities for information security; and
- how to access advice on information security matters

All staff will comply with information security policies and procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action.

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

Each member of staff will be responsible for the operational security of the information systems they use.

Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use are maintained to the highest standard.

Contracts with external contractors that allow access to the organisation'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 will comply with all appropriate security policies

7 IMPLEMENTATION

This policy will be published on the CCG website and all staff will be made aware of its publication through communications and team meetings.

8 TRAINING AND AWARENESS

Identify how staff will be made aware of the policy (via the Internet is recommended) and how any associated training needs will be provided to ensure compliance.

The Senior Management Team and line managers are responsible for ensuring that all staff are aware of the policy which will be available on the CCG intranet.

Training will be provided for individuals named in this policy. Any further training needs will be identified via the appraisal process and training needs analysis.

9 MONITORING AND AUDIT

An audit trail of system access and data use by staff shall be maintained and reviewed on a regular basis.

The CCG has in place routines to regularly audit compliance with this and other policies. In addition the CCG reserves the right monitor activity where it suspects that there has been a breach of policy.

The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system

- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- In the interests of national security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of the system
- Any monitoring will be undertaken in accordance with the above act and the Human Rights Act

10 POLICY REVIEW

State how often the policy will be reviewed and by which committee

The policy and procedure will be reviewed at least every three years by the CCG in conjunction with managers, and Trade Union representatives if appropriate, with changes made as required and the outcome published. Where review is necessary due to legislative change, this will happen immediately.

Audit and Governance Committee has delegated responsibility for monitoring and reviewing the policy and will report any concerns to the Governing Body.

11 REFERENCES AND ASSOCIATED DOCUMENTATION

The following documents are in support of the Information Security Policy:-

- Confidentiality Policy
- Network Security Policy
- Records Management Policy
- Monitoring Standards and Procedures

12 APPENDIX ONE – EQUALITY IMPACT ASSESSMENT

Equality Impact Assessment Strategy Policies

General Information		
Policy:	Information Governance Policy	
Date of Analysis:	15/11/17	
Policy Lead: **(Name, job title and department)**	Corporate Services Manager	
What are the aims and intended effects of this policy?	This standard documents the CCG's information security framework and security standards that are in place.	
Are there any significant changes to previous policy likely to have an impact on staff, patients or other stakeholder groups?	No	
Please list any other policies that are related to or referred to as part of this analysis	None	
Who is likely to be affected by this policy?	General Public	
	Service Users	X
	Staff	
What engagement / consultation has been done, or is planned for this policy and the equality impact assessment?	Not applicable	
Promoting Inclusivity and NHS Scarborough and Ryedale CCG's Equality Objectives. How does the project, service or function contribute towards our aims of eliminating discrimination and promoting equality and diversity within our organisation? How does the policy promote our equality objectives	Not applicable	

Assessing Impact

Is this policy (or the implementation of this policy) likely to have a particular impact on any of the protected characteristic groups?

(Based on analysis of the data / insights gathered through engagement, or your knowledge of the substance of this policy)

Protected Characteristic:	No Impact:	Positive Impact:	Negative Impact:	Evidence of impact and, if applicable, justification where a *Genuine Determining Reason*[1] exists (see footnote below – seek further advice in this case)
Gender	X			
Age	X			
Race / ethnicity / nationality	X			
Disability	X			
Religion or Belief	X			
Sexual Orientation	X			
Pregnancy and Maternity	X			
Transgender / Gender reassignment	X			
Marriage or civil partnership	X			

What measures have been put in place to mitigate any potential impact?

Not applicable

1. [1] *The action is proportionate to the legitimate aims of the organisation (please seek further advice)*

Action Planning:

As a result of performing this analysis, what actions are proposed to remove or reduce any risks of adverse impact or strengthen the promotion of equality?

Identified Risk:	Recommended Actions:	Responsible Lead:	Completion Date:	Review Date:
None				

Sign-off

All EIAs must be signed off by a member of SMT
I agree with this assessment
Signed off by (Name/Job Title)
Signed: Sally Brown, Associate Director of Corporate Affairs
Date: November 2017

13 APPENDIX TWO – SUSTAINABILITY IMPACT ASSESSMENT

SUSTAINABILITY IMPACT ASSESSMENT

Instructions

Sustainability is one of the CCG's key priorities and consequently the CCG has made a corporate commitment to address the environmental effects of its activities across all service areas. The purpose of the Sustainability Impact Assessment is to record any positive or negative impacts that a Policy / Board Report / Committee Report / Service Plan / Project is likely to have on each of the CCG's sustainability themes. The Sustainability Impact Assessment enables any relevant impacts to be identified and potentially managed.

The Sustainability Impact Assessment is based on assessing the impact of the activity against a series of criteria covering environmental sustainability issues. It would be most desirable for activities to score positively in as many areas as possible, although it is likely that some areas will score positively against some themes, and negatively against others.

Using the Sustainability Impact Assessment template

To complete the Sustainability Impact Assessment template, you should consider whether the Policy / Board Report / Committee Report / Service Plan / Project will have a positive or negative impact on each of the themes by placing a mark in the appropriate column. When you think there is likely to be an impact, please provide some annotations regarding the nature of the impact, and any actions that will be taken to address that impact. Users should note that not every theme will be relevant. Where this is the case the 'No Specific Impact' column should be marked. Users should also consider the following tips:

1. Make relative not absolute judgements (e.g. a new energy efficient service would score positively even if it consumes more energy than if no service were provided).
2. Be aware that small positive changes could be outweighed by negative ones (e.g. new energy efficient lighting in the short term may outweigh the benefits of maintaining current lighting).
3. If there are both positive and negative impacts, these need to be recorded in order to give a balanced view. Be objective and unbiased.
4. Concentrate on the most key significant issues - there is the potential to consider the appraisal in a very detailed way. This should be avoided at this stage.
5. Judge a proposal over its whole lifespan and remember that some impacts may change over different timescales.

If you require assistance in completing the Sustainability Impact Assessment please contact the Corporate Services Team

Domain	Review questions	Assessment of Impact Negative = -1 Neutral = 0 Positive = 1 Unknown = ? Not applicable = n/a	Brief description of impact	If negative, how can it be mitigated? If positive, how can it be enhanced?
Models of Care	Will it minimise 'care miles' making better use of new technologies such as telecare and telehealth, delivering care in settings closer to people's homes? Will it create incentives to promote prevention, healthy behaviours, mental wellbeing, living independently and self-management? Will it provide evidence-based, personalised care that achieves the best possible health and well-being outcomes with the resources available? Will it reduce avoidable hospital admissions or permanent admissions to residential care or nursing homes? Will it pay for services based on health outcomes rather than activity for example through personal budgets? Will it deliver integrated care, that co-ordinate different elements of care more effectively and remove duplication and redundancy from care pathways? More info: http://www.sduhealth.org.uk/areas-of-focus/clinical-and-care-models.aspx	**n/a**		
Travel	Will it reduce 'care miles' (telecare, care closer) to home? Will it reduce repeat appointments? Will it provide / improve / promote alternatives to car based transport (e.g. public transport, walking and cycling)? Will it support more efficient use of cars (car sharing, low emission vehicles, community transport, environmentally friendly fuels and technologies)? Will it improve access to services and facilities for vulnerable or disadvantaged groups or individuals? More info: http://www.sduhealth.org.uk/areas-of-focus/carbon-hotspots/travel.aspx	**n/a**		
Facilities Management	Will it reduce the amount of waste produced or increase the amount of waste recycled? More info: http://www.sduhealth.org.uk/areas-of-focus/carbon-hotspots/waste.aspx Will it reduce water consumption? Will it improve the resource efficiency of new or refurbished buildings (water, energy, density, use of existing buildings, designing for a longer lifespan)? Will it improve green space and access to green space? More info: http://www.sduhealth.org.uk/areas-of-focus/carbon-hotspots/energy.aspx	**n/a**		

Adaptation to Climate Change	Will it support mitigation of the likely effects of climate change (e.g. identifying proactive and community support for vulnerable groups; contingency planning for flood, heatwave and other weather extremes)? More info: http://www.sduhealth.org.uk/areas-of-focus/community-resilience/community-resilience-copy.aspx	**n/a**		
Procurement	Will it specify social, economic and environmental outcomes to be accounted for in procurement and delivery in line with the Public Services (Social Value) Act 2012? Will it stimulate innovation among providers of services related to the delivery of the organisations' social, economic and environmental objectives? Will it reduce waste, environmental hazards and toxic materials for example by reducing PVC, antibiotic use, air pollution, noise, mining and deforestation? Will it reduce use of natural resources such as raw materials, embedded water, and energy to promote a circular economy? Will it support the local economy through local suppliers, SMEs or engage with third sector or community groups? Will it promote ethical purchasing of goods or services e.g. increasing transparency of modern slavery in the supply chain globally? More info: http://www.sduhealth.org.uk/areas-of-focus/commissioning-and-procurement/procurement.aspx	**n/a**		
Workforce	Will it provide employment opportunities for local people? Will it promote or support equal employment opportunities? Will it promote healthy working lives (including health and safety at work, work-life/home-life balance and family friendly policies)? Will it offer employment opportunities to disadvantaged groups and pay above living wage? More info: http://www.sduhealth.org.uk/areas-of-focus/social-value.aspx	**n/a**		
Community Engagement	Will it promote health, increase community resilience, social cohesion, reduce social isolation and support sustainable development? Will it reduce inequalities in health and access to services? Will it increase participation including patients, the public, health professionals and elected officials to contribute to decision making? Have you sought the views of our communities in relation to the impact on sustainable development for this activity? Will it increase peer-support mechanisms? More info: http://www.sduhealth.org.uk/areas-of-focus/community-resilience.aspx	**n/a**		
Estimated carbon benefit	What is the estimated carbon benefit (in terms of tCO_2e) from the implementation of this project? As opposed to the current business as usual position. Speak with your sustainability manager and see the following guidance: More info: http://www.sduhealth.org.uk/areas-of-focus/carbon-hotspots/pharmaceuticals/cspm/sustainable-care-pathways-guidance.aspx	**n/a**		

14 APPENDIX THREE – PRIVACY IMPACT ASSESSMENT

Privacy Impact Assessment (PIA)

Screening Questions

The below screening questions should be used inform whether a PIA is necessary. This is not an exhaustive list therefore in the event of uncertainty completion of a PIA is recommended.

Please contact the Corporate Services Team of IG Manager (eMBED) if you need any assistance

Project title	**Information Security Policy**
Brief description	This standard documents the CCG's information security framework and security standards that are in place.

Screening completed by

Name	Emma Parker
Title	Corporate Services Manager
Department	Corporate Services
Telephone	01723 343691
Email	Emma.parker6@nhs.net
Review date	01/11/2020

Marking any of these questions is an indication that a PIA is required:

	Screening Questions	Tick
1	Will the project involve the collection of identifiable or potentially identifiable information about individuals?	☒
2	Will the project compel individuals to provide information about themselves? i.e. where they will have little awareness or choice.	☒
3	Will identifiable information about individuals be shared with other organisations or people who have not previously had routine access to the information?	☒
4	Are you using information about individuals for a purpose it is not currently used for or in a new way? i.e. using data collected to provide care for an evaluation of service development.	☒
5	Where information about individuals is being used, would this be likely to raise privacy concerns or expectations? i.e. will it include health records, criminal records or other information that people would consider to be sensitive and private.	☒
6	Will the project require you to contact individuals in ways which they may find intrusive? i.e. telephoning or emailing them without their prior consent.	☒
7	Will the project result in you making decisions in ways which can have a significant impact on individuals? i.e. will it affect the care a person receives.	☒
8	Does the project involve you using new technology which might be perceived as being privacy intrusive? i.e. using biometrics, facial recognition or automated decision making.	☒

Please retain a copy of this questionnaire within your project documentation.

If you have ticked any of the questions above – please complete a full Privacy Impact Assessment – The most up to date version of the form is available on the CCG website at:

http://www.scarboroughryedaleccg.nhs.uk/publications/policies-2/