NHS
Scarborough and Ryedale
Clinical Commissioning Group

Security and Transmission of Personal Confidential Data and Information (Safe Haven) Policy November 2017

Authorship:	Information Governance Manager (eMBED)			
Committee Approved:	Audit and Governance Committee			
Approved date:	November 2017			
Review Date:	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 Relevant
Bribery Checklist	No		No	Not Relevant
Target Audience:	All CCG Staff			
Policy Reference No:	P709			
Version Number:	V.3			
Publication/Distribution	Website	Email Staff	Others (i.e. SBC)	
	Yes	Yes	No	

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
0.1	IG Manager	First draft for comments	NR	
1.0	IG Manager	Approved version		
2.0	Helen Sanderson	Update for HSCIC Guidance and Caldicott 2	Audit Committee March 2016	
3.0	IG Officer	To update for changes in organisational relationships (CSU to Embed) To update for the requirements of the General Data Protection Regulation	Audit and Governance Committee November 2017	November 2017

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		
	Quality and Performance Committee	Ratification		
	Primary Care Co-Commissioning Committee	Ratification		
	Other	Ratification		
	All Employees	Consultation		
	Public	Consultation		
	Yorkshire and Humber Social Partnership Forum	Consultation		

Contents

1 INTRODUCTION 4

2 ENGAGEMENT 4

3 IMPACT ANALYSES 4

3.1 Equality 4

3.2 Sustainability 5

4 SCOPE 5

4.1 Senior Information Risk Owner (SIRO) 5

4.2 Caldicott Guardian 5

4.3 Service Managers / Line Managers 5

4.4 Nominated Safe Haven Managers (Information Asset Owners) 6

5 POLICY PURPOSE AND AIMS 6

5.1 Procedures for the Transmission of Confidential Information 6

5.2 Safe Haven Guidance 6

5.3 Caldicott Principles 7

5.4 Data Protection Principles and General Data Protection Principles 7

6 IMPLEMENTATION 8

7 TRAINING AND AWARENESS 8

8 MONITORING AND AUDIT 8

9 POLICY REVIEW 8

10 REFERENCES AND ASSOCIATED DOCUMENTATION 8

11 APPENDIX ONE - SAFE HAVEN SELF -ASSESSMENT QUESTIONNAIRE 0

12 APPENDIX TWO – EQUALITY IMPACT ASSESSMENT 0

13 APPENDIX THREE – SUSTAINABILITY IMPACT ASSESSMENT 6

14 APPENDIX FOUR – PRIVACY IMPACT ASSESSMENT 0

1 INTRODUCTION

The NHS constantly uses and transfers personal confidential data and information (PCD) between people, departments and organisations much of this information is sensitive and/or personal and requires treating with appropriate regard to its security and confidentiality. These are known as data flows and covers PCD of service users, staff and others. Safe haven requirements should also be applied when processing commercially confidential or sensitive information. It is therefore essential that all departments and services within the Scarborough and Ryedale Clinical Commissioning Group (The CCG) that transfer and/or receive PCD from other organisations and between departments have in place adequate safe haven procedures to protect these data flows:

- at the point of receipt,
- whilst held by the department,
- when transferring information to others, by whatever means,
- whilst stored in archive, and
- at the point of disposal.

The policy applies to all clinical and non-clinical areas within the organisation.

The aim of the policy is to:

- Provide staff with guidance on Safe Haven requirements for distributing PCD.
- Ensure that transfers of PCD adhere to Caldicott principles, the Data Protection Act 1998 and General Data Protection Regulation
- Protect PCD in areas accessed by the public.
- Ensure that information accessed remotely is done so securely.

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 Two.

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 Three. The assessment does not identify and benefits or negative effects of implementing this document.

4 SCOPE

This policy applies to all staff, CCG Members, temporary staff, seconded staff, contractors and others undertaking work on behalf of the CCG, etc. For those staff covered by a letter of authority/honorary contract or work experience the organisations policies are also applicable whilst undertaking duties for or on behalf of the CCG.

For the purposes of this policy, personal confidential information shall include any confidential information relating to the CCG and/or its agents, customers, prospective customers, service users, suppliers or any other third parties connected with CCG and in particular shall include, without limitation:

- service user information;
- ideas/programme plans/forecasts/risks/issues;
- finance/budget planning/business cases;
- sources of supply and costs of equipment and/or software;
- prospective business opportunities in general;
- computer programs and/or software adapted or used;

corporate or personnel information; and contractual and confidential supplier information. This is irrespective of whether the material is marked as confidential or not. Responsibilities for the implementation of this policy are as follows:

4.1 Senior Information Risk Owner (SIRO)

The SIRO has overall responsibility for the implementation of Safe Haven Policy within the CCG. Safe Haven implementation is key as it will ensure that PCD and commercially sensitive information is handled securely.

The CCG has a particular responsibility for ensuring that it corporately meets its legal responsibilities, and for the adoption of internal and external governance requirements.

4.2 Caldicott Guardian

The Caldicott Guardian is responsible for the review and agreement of internal procedures governing the protection and use of PCD by staff.

4.3 Service Managers / Line Managers

Service managers and line managers are responsible for ensuring that all PCD data flows, into or out of the organisation are included in their departments Information Asset Register. This includes:

- Identifying systems in place and nominating Information Assets Owners
- Identifying all systems that require safe haven procedures within their departments.

- Ensure all staff are aware of their duties and responsibilities in relation to keeping all relevant information confidential and secure. All departments should document and implement safe haven procedures appropriate to the information they process.

4.4 Nominated Safe Haven Managers (Information Asset Owners)

Information Asset Owners must ensure that appropriate controls are put in place to protect information by completing the Information Asset Register and associated data flow and risk assessment. When completing the Information Asset Register and associated data flows the controls detailed below (Appendix One) should be considered

- Ensure access is properly controlled to staff on a need to know basis only
- Identify routine information flows and ensure that these are mapped on a timely basis.
- Develop and document the local safe haven procedures appropriate to their service.
- Ensure all staff are aware of and understand the procedures for their area.
- Ensure all staff have completed their annual information governance training.
- Regularly review the adequacy of controls in place and implement corrective action where necessary.

5 POLICY PURPOSE AND AIMS

5.1 Procedures for the Transmission of Confidential Information

All staff have a professional responsibility for the information they handle within the organisation, and must use robust methods to keep the information secure.

It is vital that staff choose the most appropriate method of communication based on factors such as:-

- The sensitivity of the information.
- The urgency of the need to share information.
- The operating procedures of the receiving organisation.
- The reason for sending the information.
- The reason for the choice of method of transmission

Staff must not base their choice of communication on ease for them, whilst sending a fax maybe convenient and quick would that information be better safeguarded if it was communicated by telephone or secure email?

5.2 Safe Haven Guidance

Safe Haven is a requirement for there to be appropriate controls in place to ensure the secure transfer, receipt, storage and disposal of personal confidential information, to protect it from loss, damage or unauthorised access.

Access controls and registered access levels should be in place to restrict access to information on a need to know basis for staff to be able to perform their duties.

It is essential all staff members must be made aware of their own responsibility for ensuring the protection of personal information received.

Organisations should ensure that all information transfers are subject to agreed management and information security controls which comply with NHS information governance standards, including the Caldicott Principles, set out below.

This is primarily aimed at the protection of personal data but will also be necessary for other sensitive information, e.g. commercially sensitive information.

Guidance is detailed in Appendix One below, which allows a self-assessment of the controls in place within your department

5.3 Caldicott Principles

1. Justify the purpose for using the information
2. Only use identifiable information if absolutely necessary
3. Use the minimum that is required
4. Access should be on a strict need to know basis
5. Everyone must understand their responsibilities
6. Understand and comply with the Law
7. The duty to share information can be as important as the duty to protect patient confidentiality. However sharing information should be undertaken on a legal basis and in the best interests of the patient.

5.4 Data Protection Principles and General Data Protection Principles

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—
2. at least one of the conditions in Schedule 2 is met, and
3. in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
4. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
5. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
6. Personal data shall be accurate and, where necessary, kept up to date.
7. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
8. Personal data shall be processed in accordance with the rights of data subjects under this Act.
9. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
10. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of

protection for the rights and freedoms of data subjects in relation to the processing of personal data.

6 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.

Breaches of this policy may be investigated and may result in the matter being treated as a disciplinary offence under the CCG's disciplinary procedure.

7 TRAINING AND AWARENESS

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.

8 MONITORING AND AUDIT

Adherence to this policy will be monitored on an on-going basis and breaches may result in disciplinary procedures.

9 POLICY REVIEW

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.

10 REFERENCES AND ASSOCIATED DOCUMENTATION

- NHS Confidentiality Code of Practice
- NHS Code of Practice for Records Management
- HSCIC: Code of Practice on Confidential Information
- HSCIC: A Guide to Confidentiality in Health and Social Care
- HSCIC: Sending an encrypted email from NHSmail to a non-secure email address
- Report of the Caldicott2 Review - Information: To share or not to share? The Information Governance Review 2013
- Government Response to Report of the Caldicott2 Review 2013
- The Independent Information Governance Oversight Panel: Annual Report

11 APPENDIX ONE - SAFE HAVEN SELF -ASSESSMENT QUESTIONNAIRE

No.	Guidance	*Current departmental process*	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
General Security					
1	The area should be separated from the general public and unauthorised personnel by appropriate access controls when unmanned, e.g. locked doors and all personal and corporate confidential information should be locked away. In the event visitors require access to office areas they should be requested to sign in, and then be met and escorted as appropriate.				
2	The area should be protected by appropriate alarm and security systems				
3	Personal Confidential Data (PCD) and Corporate Confidential Information should be secured away when not in use, in a formal secure filing system i.e. Clear desk policy				
4	Staff should be aware that the area must be secured if it is to be left unattended.				
5	Where keypad locks are in place the codes should be changed on a regular basis, e.g. quarterly.				
Security of Manual Records					
1	Access to information must be restricted on a need to know basis appropriate to the staff members job role, this applies to all formats e.g. written records, photos, etc.				
2	All types of files containing (PCD) should be held securely when not in use, e.g. filing cabinets / drawers and computers are locked.				
3	Records should be filed in a structured manner. In addition manual records placed in a file should be secured within that file to prevent accidental loss of pages.				
4	A comprehensive tracking / tracing and monitoring system for all records and files should be place. This applies to all stages of transit, including where handovers during transit have taken place.				

No.	Guidance	*Current departmental process*	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
5	As far as possible PCD should not be visible through any file covers.				
Security of Electronic Records					
1	Monitors and other screens should be placed in such a manner as to avoid the information displayed on them being over looked, e.g. through a window or in an open reception area				
2	Electronic information should only be stored on the main server and not a local computer.				
3	Proper system access controls should be in place i.e. passwords and access levels for each user. Staff should be made aware of their responsibilities in respect the management and security of passwords and smartcards, e.g. passwords and smartcards must not be shared or left unattended.				
4	Staff should be aware that PC's, laptops etc, should be locked or switched off when leaving it unattended				
5	PCD or other confidential information should not be copied to any personal PC or media that do not belong to the organisation or is not approved by the organisation.				
Working from Home via VPN					
1	The organisation allows authorised access via a VPN, in order to provide those members of staff with a legitimate business need to have access to their authorised section of the organisation network, when working away from organisational premises. VPN access should only be used in association with equipment that has been encrypted and issued by the IM&T department for work purposes.				
2	Staff should be aware that all of the guidance set out in this document must also be applied when working from home.				
Portable Media and Encryption					

No.	Guidance	*Current departmental process*	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
1	Only equipment that has been encrypted and issued by the IM&T department should be used for work purposes.				
Transferring Information					
1	Staff should be aware of and have access to the NHS Confidentiality, Code of Practice, HSCIC Code of Practice on Confidential Information and HSCIC: A Guide to Confidentiality in Health and Social Care and Data Protection Policy & Standard.				
2	Transfers and receipt of PCD should only be undertaken by appropriately trained and authorised personnel. Where PCD is sent in password protected documents via NHS Mail the password to the document must be communicated separately preferably via a phone call directly to the person authorised to receive that information. Staff must also be aware of HSCIC: Sending an encrypted email from NHSmail to a non-secure email address				
3	Where necessary consent is obtained from the data subject for any transfers of PCD this must be recorded in the data appropriate record and be in line with documented information sharing agreement for that servicewhere applicable Where consent is not the basis for the transfer, then a legal justification must be identified and documented.				
4	Secure methods of transfer appropriate to the information being transferred have been determined and implemented.				

No.	Guidance	*Current departmental process*	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
5	Routine transfers of PCD, to and from the organisation, by whatever method, should be recorded on a data mapping spreadsheet, to ensure appropriate controls of the data at all times. An Information sharing agreement should be documented and agreed by all parties to the information sharing				
6	If information is to be transferred by means of DVD or memory stick these must be encrypted and the encryption password communicated separately, preferably via a phone call directly to the person authorised to receive that information. The DVD or memory stick should be sent via tracked mail.				
Removing Information from secure storage point, including sending to archiving					
1	Staff who are required to remove PCD from organisational premises should be approved to do so and the approval recorded? All staff approved should have signed to say they have read and understand the associated policies. e.g. mobile working, safe haven, code of confidentiality, etc.				
2	A record made of information to be taken from its storage point should be made in the tracking systems in place. NB/ This tracking system should be completed every time information is removed from its storage point, even if it remains in the office. Should records be transferred between members of staff both inside and outside the office a record of this must be made within the tracking system This should be monitored to ensure records are returned.				

No.	Guidance	*Current departmental process*	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
3	Only the minimum PCD required for the purpose should be taken when taking records off site. These records should never be left unattended.				
4	Appropriate transportation methods should be implemented, e.g. carried in a locked container or via encrypted electronic methodology.				
5	Staff should be aware that when records are to be transported this must be out of sight i.e. in the boot of the car and that they should not be left in vehicles for long periods, e.g. over night. Where records are to be left in car boots for necessary operational reasons then this should be signed off as agreed by the appropriate governing body.				
6	In situations where staff have been authorised to take records home it must be evidenced that they are aware that the records must be kept securely and not accessible to other members of the household or visitors and records must be returned to their secure storage point ASAP.				
Incoming Mail					
1	Staff should be aware that letters marked private and confidential should opened by the addressee or appropriate nominee only and opened away from public areas				
Outgoing Mail					

No.	Guidance	*Current departmental process*	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
1	Confirm from verifiable records the correct name, department, and address are being used, for the intended recipient of the correspondence. A record of information being sent should be maintained on the project or patient file, including when, to whom and by what method When necessary ask the recipient to confirm the receipt of the package. If acknowledgment is not received then it must be followed up as this may be the first indication of a potential breach.				
2	Staff should ensure packages are addressed correctly, and marked appropriately e.g. **private and confidential** where necessary. Return addresses should be annotated on all outgoing mail, to enable recipients to return incorrectly received correspondence without opening it.				
3	Staff should be aware of the correct packaging methods for PCD being sent out and a standard procedure should include a check that the contents being placed in the package are for the addressee of the package.				
4	Staff should be aware of the correct method for sending PCD e.g. courier, post, tracked /special delivery, etc. Nb. Sending an item via special delivery needs to be balanced against the risk of any confidentiality breach and practical and cost issues of using special delivery				
General Transmission by Fax					
1	It should be ensured that fax machines are situated in a secure area at both ends of the transmission and accessible / visible only to authorised staff.				

No.	Guidance	*Current departmental process*	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
2	Where PCD is to be transferred to another party all methods are considered before the use of fax, e.g. scanning and sending via NHS Mail. All staff should be aware of the HSCIC: Safe Haven Briefing: secure transfer of personal identifiable information by fax **NB**/ Fax should only be used as a last resort or in emergency situations.				
		Incoming Faxes			
1	Incoming Faxes need to be collected regularly by authorised staff.				
2	Where possible the fax machine should locked overnight/out of hours.				
3	Where faxes have been incorrectly received, the sender should be contacted to inform them and to agree that the document will be securely destroyed or securely returned for destruction.				
		Outgoing Faxes			
1	When considering faxing correspondence to another organisation first consider whether NHS Mail can be used instead. NB/ NHSMail has a facility which facilitates the secure transmission of personal confidential information to none NHS Mail account holders. Please see HSCIC: Sending an encrypted email from NHSmail to a non-secure email address				
2	Where the correspondence is to be faxed then staff should be aware that checks must be undertaken to ensure that the fax number to be used is the correct and valid number for the destination				
3	Staff should make the intended recipient aware of the transmission of a fax before sending and request acknowledgement of receipt. If acknowledgment is not received then it must be followed up as this may be the first indication of a potential breach.				

No.	Guidance	*Current departmental process*	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
4	Use a fax cover sheet marked **PRIVATE AND CONFIDENTIAL**, indicate the number of sheets being sent, and ensure the intended recipient is verified and named on the cover sheet. Include contact details of the sender.				
5	Staff should request a report sheet from the fax machine to check and confirm transmission was successful.				
		Secure Email			
1	Staff should be aware that only NHS Mail and associated secure government email systems are to be used for the transmission of PCD. Also that only the minimum PCD required for the purpose should be communicated.				
2	All secure email addresses should be checked to ensure the correct email recipient has been selected. Delivery and read receipt options should be selected to verify the message has been successfully sent and the recipient has read it.				
3	Recipients of email correspondence should be checked to ensure that it is appropriate for them to receive the PCD for the intended purpose(s) **NB**/ Only recipients with a genuine need to know should receive the PCD this includes CC's and BCC's				
4	Secure emails containing PCD should be marked confidential.				

No.	Guidance	*Current departmental process*	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
5	The organisational standard disclaimer has been placed on all emails stating 'this email is confidential and is intended for the named recipient(s) only. If you have received this email in error please delete it and notify the sender accordingly. Unauthorised copying and or use of this email if you are not the intended recipient may result in legal action being taken.'				
6	PCD sent or received via email should be safely stored and archived, as well being incorporated into the appropriate record, including an audit trail of actions.				
Telephone Conversations					
1	Staff should be aware that all telephone conversations regarding PCD should be kept to a minimum and take place in a private area where they cannot be over heard by unauthorised personnel				
2	When speaking to service users, carers and others, staff should confirm the caller's identity and their authority to receive the information requested, if in doubt check with a manager. Where applicable job title, department and organisation of the caller should be taken, and then called back using a known verifiable number. It is important to guard against people seeking information by deception this is particularly risky when using mobile telephone numbers. This can be waived where a caller is known to you.				
3	Staff should be aware to use the secrecy (mute) button when putting callers on hold.				

No.	Guidance	*Current departmental process*	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
4	Where telephone messages containing PCD are received, they should preferably be emailed via NHS Mail to the intended recipient. If this is not possible the message should be placed in an envelope, sealed and addressed to the intended recipient, marked private and confidential.				
5	In the event of requests for information by telephone, staff should confirm the identity of the requestor and their authorisation to receive the information. If in doubt staff should be aware to check with a senior manager. This could mean calling the enquirer back via a main switch board. **NB/ DO NOT** use direct lines for verification purpose as number given by callers may not be genuine.				
Incoming Voicemail and Answerphone messages					
1	When checking messages on an answer phone staff should ensure they cannot be overheard by unauthorised personnel.				
2	Where message books are used is it essential that these are held securely and access to them is on a need to know basis, as appropriate to their staff member's job role. **NB/** Messages should not contain PCD but should refer readers to proper records.				
Answerphones Outwards					
1	Staff should be aware that should they need to leave an answer phone message that they should only leave a name and phone number for call back. Do not indicate the reason for the call.				
Verbal Transfer of Information					

No.	Guidance	*Current departmental process*	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
1	Staff should be aware that whenever they are transferring information verbally they must ensure they cannot be overheard by unauthorised personnel.				
2	Where service users register at reception it should be ensured that any personal details they need to give cannot be overheard.				
3	Where discussions include PCD they must not take place in a communal areas, e.g. shared offices, or anywhere else where you can be overheard by unauthorised personnel.				
4	Where message books are used they should be held securely and access limited on a need to know basis. **NB**/ Messages should not contain PCD but should refer readers to proper records.				
Information Sharing					
1	Staff should be aware of their responsibilities in respect of information sharing and documented protocols put in place where information sharing forms a routine part of the service provision.				
2	Staff should be aware of guidance available e.g. The Confidentiality NHS Code of Practice.				
3	Responsibility for making Information sharing decisions should be delegated to appropriate senior personnel.				
Subject Access Requests					
1	Staff should be made aware of their responsibilities in respect subject access requests received and appropriate staff identified and trained to deal with these requests. All subjects access requests must be processed in line with the Subject Access Request Policy				
2	Staff should be able to advise individuals on how to apply for a copy of their information.				

No.	Guidance	*Current departmental process*	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
3	Records are reviewed by a clinician or senior manager as appropriate to ensure no exempt information is sent out and that the correct records are being sent to the correct recipient in response to the request.				
Disposal of Information					
1	Secure methods of disposing of PCD, whatever format it may be in, should be identified and implemented. This must be done in compliance with the NHS Code of Practice for Records Management.				
2	A register of records destroyed must be maintained. This must be done in compliance with the NHS Code of Practice for Records Management.				
Reporting Incidents					
1	Staff should be aware that all breaches of confidentiality and information security must be reported within 24 hours on the CCG reporting system , including near misses. Staff should trained in the corporate incident reporting system.				
Highlighting Security Weaknesses					
1	Staff should be aware that they are responsible for reporting security weaknesses identified to their manager for corrective action				
Training					
1	All staff have been briefed and are aware of information handling, transferring, sharing and security requirements. IG Statutory and Mandatory Training must be been completed annually and additional Information Governance Training Tool, training modules identified to be completed as appropriate to the job role.				
Business Intelligence Only (Implementation of Accredited Safe Haven)					
1	In order to be able to use weakly de-identified PCD the organisation must have been approved as an accredited safe haven via the HSCIC.				

No.	Guidance	*Current departmental process*	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
2	Where weakly de-identified PCD is used then the number of personnel who can trace NHS Numbers must be kept to a minimum and documented.				
3	Appropriate pseudonymisation methodologies must be implemented to pseudonymise PCD before it being released to staff to undertake their duties.				
Documented Procedures					
1	Controls and procedures put in place, in line with this standard, have been documented, made available to staff and staff trained appropriately				
Residual Risks					
1	All risks identified in this audit which cannot be mitigated must be reported to and approved by the appropriate governing body and recorded on the risk register.				

Note this list is not exhaustive other controls can be implemented if thought required

12 APPENDIX TWO – EQUALITY IMPACT ASSESSMENT

Equality Impact Assessment Strategy Policies

General Information		
Policy:	Safe Haven Policy	
Date of Analysis:	November 2017	
Policy Lead: **(Name, job title and department)**	Information Governance Manager	
What are the aims and intended effects of this policy?		
Are there any significant changes to previous policy likely to have an impact on staff, patients or other stakeholder groups?	None	
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	☐
	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	

Equality Data

Age

Data provided below is from Census 2011

Age Range	Number	%
0-14	17,672	14.9
15-44	39,530	33.2
45-64	15,427	13.0
65-74	9,083	7.6
85+	3,820	3.2

Gender

JSNA 2016

	%
Male Residents	49.6
Female Residents	50.4

Race / Nationality

BME – 2011 Census Data

	%
White	97.5
Mixed	0.8
Asian	1.2
Black	0.2
Other	0.2

Languages – 2011 Census Data

	%
English	97.5
Polish	0.8
Other EU Language	0.6
Other	1.86

Gypsy and Travellers – 2011 Census Data

Scarborough	37
Ryedale	81

Disability

2011 Census Data

	%
Long Term Health Problem/Disability	21.3
Limiting Long Term Illness	20.4

Projecting Adult Needs and Service Information (PANSI)-2017 Estimates

	Scarborough	Ryedale
Limiting Long Term Illness - day to day activities limited a little	7,507	3,455
Limiting Long Term Illness - day to day activities limited a lot	6,513	2,462
Mobility - unable to manage at least one activity on their own	5,210	2,509
Learning Disability – Including Down's syndrome	947	469
Learning Disability – Autistic Spectrum Disorders and Down's Syndrome	81	134
Visual Impairment - Moderate or severe	3,323	1,588
Hearing Impairment – some hearing loss	17,167	8,370
Hearing Impairment – Moderate or Severe	2,215	1,070
Dementia	1,973	959
Depression	2,474	1,585
Learning Disability – Baseline	1,454	708
Learning Disability – Moderate - Severe	415	1,128
Learning Disability – Autistic Spectrum Disorders	592	289
Learning Disability – Down's syndrome	38	18
Physical Disability – Moderate	5,176	2,620
Physical Disability – Serious	1,605	824
Physical Disability – Personal Care	3,198	1,639
Visual Impairment – Serious	39	19
Hearing Impairment – Some hearing loss	69,328	3,565
Hearing Impairment – Severe	395	203
Mental Health Problems	4,331	2,096

Sexual Orientation

In relation to sexual orientation, local population data is not known with any certainty. In part, this is because until recently national and local surveys of the population and people using services did not ask about an individual's sexual orientation. However, nationally, the Government estimates that 5% of the population are lesbian, gay or bisexual communities.

Gender Reassignment

There are not any official statistics nationally or regionally regarding transgender populations, however, GIRES (Gender Identity Research and Education Society - www.gires.org.uk) estimated that, in 2007, the prevalence of people who had sought medical care for gender variance was 20 per 100,000, i.e. 10,000 people, of whom 6,000 had undergone transition. 80% were assigned as boys at birth (now trans women) and 20% as girls (now trans men). However, there is good reason, based on more recent data from the individual gender identity clinics, to anticipate that the gender balance may eventually become more equal.

Religion / Belief

2011 - Census Data

	%
Christian	67
Buddhist	0.3
Hindu	H0.1
Jewish	0.1
Muslim	0.5
Sikh	0.1
Other Religion	0.4
No Religion	24.3
Religion not stated	7.4

Pregnancy and Maternity

	Live Births (ONS 2016)	Still Births (ONS 2016)
Scarborough	1,034	4
Ryedale	439	2

Marriage and civil partnership

Data provided below is from Census 2011

	Number	%
Single	32,890	28.2
Married	57,934	49.7
In registered same sex civil partnership	259	0.2
Separated (incl civil partnership)	2,866	2.5
Divorced (incl civil partnership)	12,043	103
Widowed	10,486	9

This protected characteristic generally only applies in the workplace.

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 sources of equality information have you used to inform your piece of work?
(Please refer to the JSNAs and Population data, previous engagement findings, research, patient experience reports etc.)

Not applicable

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:

Sign-off

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

13 APPENDIX THREE – 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			
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			
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			

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			
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			
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			
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			
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			

14 APPENDIX FOUR – 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	
Brief description	

Screening completed by

Name	
Title	
Department	
Telephone	
Email	
Review date	

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/