NHS
Vale of York
Clinical Commissioning Group

SECURITY AND TRANSMISSION OF PERSONAL CONFIDENTIAL DATA AND INFORMATION (SAFE HAVEN) POLICY
December 2017

Authorship :	Barry Jackson – Information Governance, Security and Compliance Manager
Reviewing Committee :	Emergency Planning, Business Continuity and Information Governance Steering Group
Date :	December 2017
Approval Body :	Executive Committee
Approved Date :	20 December 2017
Review Date :	December 2019
Equality Impact Assessment :	Yes
Sustainability Impact Assessment :	Yes
Related Policies :	• IG02 Data Protection and Confidentiality • IG03 Internet, Email and Acceptable Use • IG04 Freedom of Information Act • IG05 Information Security • IG06 Information Risk • IG07 Corporate Records Management Standards and Procedures • IG08 Mobile Working • IG09 Subject Access Request Policy • IG11 Information Governance Strategy • IG12 Clinical Records Keeping Standards
Target Audience:	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.
Policy Reference No:	IG10
Version Number:	3.0

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 and Date	Date on Internet
0.1	Barry Jackson	First draft for comments	NR	
1.0	Barry Jackson	Approved version		
2.0	Helen Sanderson	Secure email section 5.1, Sending an encrypted email from NHSmail to a non-secure email address. Update for HSCIC Guidance and Caldicott 2	SMT Approved February 2016	
2.1 (3.0 when approved)	IG Officer	• To update for changes in organisational relationships (CSU to Embed) • To update for the requirements of the General Data Protection Regulation	Executive Committee 20 December 2017	26 January 2018

To request this document in a different language or in a different format, please contact :
01904 555 870 or valeofyork.contactus@nhs.net

CONTENTS

1. INTRODUCTION

1.1. 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 includes 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 Vale of York 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.

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

2. POLICY STATEMENT

2.1. 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

Equality

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

3.2. 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.

Sustainability

3.3. 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

4.1. 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.

4.2. 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.

5. POLICY PURPOSE / AIMS AND FAILURE TO COMPLY

5.1. The aim of the policy is to :

- Provide staff with guidance on Safe Haven requirements for whilst using, distributing and storing PCD.
- Ensure that transfers of PCD adhere to Caldicott principles and current Data Protection Legislation

6. PROCEDURES FOR THE TRANSMISSION OF CONFIDENTIAL INFORMATION

6.1. 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

6.2. 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 ?

6.3. **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.

Safe Haven Guidance

6.4. 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.

6.5. 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.

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

6.7. 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.

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

6.9. Guidance is detailed in Annex A below, which allows a self-assessment of the controls in place within your department

Caldicott Principles

- Justify the purpose for using the information
- Only use identifiable information if absolutely necessary
- Use the minimum that is required
- Access should be on a strict need to know basis
- Everyone must understand their responsibilities
- Understand and comply with the Law
- 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.

Data Protection Act Principles valid until 25 May 2018 (these will be replaced by the General Data Protection Regulation Principles from this date and are detailed below)

- Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless :
- (a) at least one of the conditions in Schedule 2 is met, and

- (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
- 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.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- Personal data shall be processed in accordance with the rights of data subjects under this Act.
- 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.
- 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.

General Data Protection Regulation Principles (valid from 25 May 2018)

6.9.1- processed lawfully, fairly and in a transparent manner in relation to individuals

6.9.2 - collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes

6.9.3 - adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

6.9.4 - accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

6.9.5 - kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals

i. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

7. ROLES / RESPONSIBILITIES / DUTIES

Senior Information Risk Owner (SIRO)

7.1. 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.

Caldicott Guardian

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

Service Managers / Line Managers

7.3. 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.

Nominated Safe Haven Managers (Information Asset Owners)

7.4. 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 3) 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.

8. POLICY IMPLEMENTATION

8.1. Following approval by the Executive Committee/Governing Body the policy will be sent to :

- The Communications Manager who will disseminate to all staff via the team newsletter process
- The Chairs of the Governing Body, the Council of Members and any other committees and sub committees for dissemination to members and attendees, as appropriate.
- The Practice Managers of all member practices for information, (if appropriate).

8.2. 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'.

9. TRAINING AND AWARENESS

9.1. This policy will be published on the CCG's website and staff will be briefed regarding amendments to policy.

9.2. The policy will be brought to the attention of all new employees as part of the induction process.

10. MONITORING AND AUDIT

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

11. POLICY REVIEW

11.1. This policy will be reviewed on a bi-annual basis. Earlier review may be required in response to exceptional circumstances, organisational change or relevant changes in legislation/guidance, as instructed by the senior manager responsible for this policy.

12. REFERENCES

- 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

13. ASSOCIATED POLICIES

- IG02 Data Protection and confidentially Policy
- IG03 Internet, Email and Acceptable Use Policy
- IG04 Freedom of Information Act
- IG05 Information Security Policy
- IG06 Information Risk Policy
- IG07 Corporate Records Management Standards and Procedures
- IG08 Mobile Working Policy
- IG09 Subject Access Request Policy
- IG11 Information Governance Strategy

14. CONTACT DETAILS

NHS Vale of York Clinical Commissioning Group, West Offices,
Station Rise, York. Y01 6GA
Telephone : 01904 555870
Email : valeofyork.contactus@nhs.net

15. APPENDIX 1 : EQUALITY IMPACT ANALYSIS FORM

1.	**Title of policy/ programme/ service being analysed**
	Security and Transmission of Personal Confidential Data and Information (Safe Haven) Policy
2.	**Please state the aims and objectives of this work.**
	This document provides justification and defines guidance for the transfer of personal confidential data in a secure way.
3.	**Who is likely to be affected? (e.g. staff, patients, service users)**
	Staff, patients and service users.
4.	**What sources of equality information have you used to inform your piece of work?**
	IGT 14.1, in particular Requirement 351 https://digital.nhs.uk/cyber-security/policy-and-good-practice-in-health-care/data-handling/good-practice-guide NHS Digital Exemplar Policies and Procedures
5.	**What steps have been taken ensure that the organisation has paid due regard to the need to eliminate discrimination, advance equal opportunities and foster good relations between people with protected characteristics**
	The analysis of equalities is embedded within the CCG's Committee Terms of Reference and project management framework.
6.	**Who have you involved in the development of this piece of work?**
	Internal involvement: Emergency Planning, Business Continuity and Information Governance Steering Group **Stakeholder involvement**: eMBED Healthcare Consortium **Patient / carer / public involvement**: This is an Internal policy aimed at staff employed by the CCG and contractors working for the CCG. The focus is on compliance with statutory duties and NHS mandated principals and practice.
7.	**What evidence do you have of any potential adverse or positive impact on groups with protected characteristics? Do you have any gaps in information?** **Include any supporting evidence e.g. research, data or feedback from engagement activities** **(Refer to** Error! Reference source not found. if your piece of work relates to commissioning activity to gather the evidence uring all stages of the commissioning cycle)

Disability People who are learning disabled, physically disabled, people with mental illness, sensory loss and long term chronic conditions such as diabetes, HIV)	Consider building access, communication requirements, making reasonable adjustments for individuals etc.
N/A	
Sex Men and Women	Consider gender preference in key worker, single sex accommodation etc.
N/A	
Race or nationality People of different ethnic backgrounds, including Roma Gypsies and Travellers	Consider cultural traditions, food requirements, communication styles, language needs etc.
N/A	
Age This applies to all age groups. This can include safeguarding, consent and child welfare	Consider access to services or employment based on need/merit not age, effective communication strategies etc.
N/A	
Trans People who have undergone gender reassignment (sex change) and those who identify as trans	Consider privacy of data, harassment, access to unisex toilets & bathing areas etc.
N/A	
Sexual orientation This will include lesbian, gay and bi-sexual people as well as heterosexual people.	Consider whether the service acknowledges same sex partners as next of kin, harassment, inclusive language etc.
N/A	
Religion or belief Includes religions, beliefs or no religion or belief	Consider holiday scheduling, appointment timing, dietary considerations, prayer space etc.
N/A	
Marriage and Civil Partnership Refers to legally recognised partnerships (employment policies only)	Consider whether civil partners are included in benefit and leave policies etc.
N/A	

Pregnancy and maternity Refers to the pregnancy period and the first year after birth	Consider impact on working arrangements, part-time working, infant caring responsibilities etc.
N/A	
Carers This relates to general caring responsibilities for someone of any age.	Consider impact on part-time working, shift-patterns, options for flexi working etc.
N/A	
Other disadvantaged groups This relates to groups experiencing health inequalities such as people living in deprived areas, new migrants, people who are homeless, ex-offenders, people with HIV.	Consider ease of access, location of service, historic take-up of service etc.
N/A	

8.	**Action planning for improvement** Please outline what mitigating actions have been considered to eliminate any adverse impact? Please state if there are any opportunities to advance equality of opportunity and/ foster good relationships between different groups of people? An Equality Action Plan template is appended to assist in meeting the requirements of the general duty

Sign off
Name and signature of person / team who carried out this analysis Governance Team
Date analysis completed December 2017
Name and signature of responsible Director Chief Finance Officer, (SIRO)
Date analysis was approved by responsible Director

16. APPENDIX 2: SUSTAINABILITY IMPACT ASSESSMENT

Staff preparing a policy, Governing Body (or Sub-Committee) report, service development plan or project are required to complete a Sustainability Impact Assessment (SIA). The purpose of this SIA is to record any positive or negative impacts that this is likely to have on sustainability.

Title of the document	Security and Transmission of Personal Confidential Data and Information (Safe Haven) Policy
What is the main purpose of the document	CCG policy document to implement arrangements to comply with statutory duties.
Date completed	13th December 2017
Completed by	Risk and Assurance Manager

Domain	**Objectives**	**Impact of activity** **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?**
Travel	Will it provide / improve / promote alternatives to car based transport ?	N/A			
	Will it support more efficient use of cars (car sharing, low emission vehicles, environmentally friendly fuels and technologies) ?	N/A			
	Will it reduce 'care miles' (telecare, care closer) to home ?	N/A			
	Will it promote active travel (cycling, walking) ?	N/A			
	Will it improve access to opportunities and facilities for all groups ?	N/A			
	Will it specify social, economic and environmental outcomes to be accounted for in procurement and delivery?	N/A			

Procurement	Will it stimulate innovation among providers of services related to the delivery of the organisations' social, economic and environmental objectives?	N/A			
	Will it promote ethical purchasing of goods or services ?	N/A			
	Will it promote greater efficiency of resource use?	N/A			
	Will it obtain maximum value from pharmaceuticals and technologies (medicines management, prescribing, and supply chain) ?	N/A			
	Will it support local or regional supply chains ?	N/A			
	Will it promote access to local services (care closer to home) ?	N/A			
	Will it make current activities more efficient or alter service delivery models ?	N/A			
Facilities Management	Will it reduce the amount of waste produced or increase the amount of waste recycled ?	N/A			
	Will it reduce water consumption ?	N/A			
Workforce	Will it provide employment opportunities for local people?	N/A			
	Will it promote or support equal employment opportunities ?	N/A			
	Will it promote healthy working lives (including health and safety at work, work-life/home-life balance and family friendly policies) ?	N/A			
	Will it offer employment	N/A			

	opportunities to disadvantaged groups ?				
Community Engagement	Will it promote health and sustainable development?	N/A			
	Have you sought the views of our communities in relation to the impact on sustainable development for this activity?	N/A			
Buildings	Will it improve the resource efficiency of new or refurbished buildings (water, energy, density, use of existing buildings, designing for a longer lifespan)?	N/A			
	Will it increase safety and security in new buildings and developments?	N/A			
	Will it reduce greenhouse gas emissions from transport (choice of mode of transport, reducing need to travel)?	N/A			
	Will it provide sympathetic and appropriate landscaping around new development?	N/A			
	Will it improve access to the built environment?	N/A			
Adaptation to Climate Change	Will it support the plan for the likely effects of climate change (e.g. identifying vulnerable groups; contingency planning for flood, heat wave and other weather extremes)?	N/A			
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?	N/A			
	Will it promote prevention and self-management?	N/A			

	Will it provide evidence-based, personalised care that achieves the best possible outcomes with the resources available?	N/A			
	Will it deliver integrated care, that co-ordinate different elements of care more effectively and remove duplication and redundancy from care pathways?	N/A			

17. APPENDIX 3: 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.				

No.	Guidance	*Current departmental process*	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
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.				
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.				

No.	Guidance	*Current departmental process*	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
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.				

No.	Guidance	*Current departmental process*	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
Portable Media and Encryption					
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 subjects record and be in line with the documented information sharing agreement for that service, where applicable Where consent is not the basis for the transfer, then a legal justification must be identified and documented.				

No.	Guidance	*Current departmental process*	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
4	Secure methods of transfer appropriate to the information being transferred have been determined and implemented.				
5	Routine transfers of PCD, to and from the organisation, by whatever method, should be recorded on a data mapping spread sheet, 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.				

No.	Guidance	*Current departmental process*	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
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.				
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.				

No.	Guidance	*Current departmental process*	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
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					
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.				

No.	Guidance	*Current departmental process*	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
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.				
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 intended.				

No.	Guidance	*Current departmental process*	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
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.				
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. 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				

No.	Guidance	*Current departmental process*	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
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.				
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.				

No.	Guidance	*Current departmental process*	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
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.				
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.				

No.	Guidance	*Current departmental process*	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
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.				

No.	Guidance	*Current departmental process*	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
Verbal Transfer of Information					
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.				

No.	Guidance	*Current departmental process*	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
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 of 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.				
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.				

No.	Guidance	*Current departmental process*	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
Reporting Incidents					
1	Staff should be aware that all breaches of confidentiality and information security must be reported within 24 hours of identification on the CCG incident reporting system, including near misses. Staff should be 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.				
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.				

No.	Guidance	*Current departmental process*	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
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.					