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

# October 2019

**Important:** This document can only be considered valid when viewed on the CCG's website.

If this document has been printed or saved to another location, you must check that the version number on your copy matches that of the document online.

**If you need this document in a different format or language (e.g. large print, Braille, audio or easy read), please contact us on 01482 344700, or email HULLCCG.contactus@nhs.net, or write to: NHS Hull Clinical Commissioning Group, 2nd Floor, Wilberforce Court, Alfred Gelder Street, Hull HU1 1UY.**

| | |
|---|---|
| Name of Policy: | Security and Transmission of Personal Confidential Data and Information (Safe Haven) Policy |
| Date Issued: | November 2019 |
| Date to be reviewed: | 2 years from approval date |

| | | |
|---|---|---|
| **Policy Title:** | Security and Transmission of Personal Confidential Data and Information (Safe Haven) Policy | |
| **Supersedes: (Please List)** | Security and Transmission of Personal Confidential Data and Information (Safe Haven) Policy v0.1 and Security and Transmission of Personal Confidential Data and Information (Safe Haven) Policy v1.0<br><br>Security and Transmission of Personal Confidential Data and Information (Safe Haven) Policy v1.1 | |
| **Description of Amendment(s):** | Updates to reflect GDPR and DPA 18.<br>Updates to Data Protection Principles<br>Update to reference materials<br>Removal of fax guidelines – (no longer appropriate to use fax).<br><br>Addition of Caldicott2 Requirements, in respect of information sharing arrangements and patient information leaflets.<br>Addition of HSCIC Guidance in respect of Confidentiality and Handling Confidential Information. | |
| **This policy will impact on:** | All Staff | |
| **Policy Area:** | Data Protection | |
| **Version No:** | 2.0 | |
| **Author:** | IG Team | |
| **Effective Date:** | November 2019 | |
| **Review Date:** | October 2021 | |
| **Equality Impact Assessment Date:** | October 2019 | |
| **APPROVAL RECORD** | | **Date:** |
| | Integrated Audit and Governance Committee | November 2019 |
| **Consultation:** | Information Governance Steering Group Members | October 2019 |
| | Heads of Teams / Relevant Others | October 2019 |

## 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 Website |
|---|---|---|---|---|
| 1.0 | Barry Jackson | Approved version | | |
| 1. 1 | Helen Sanderson | Update for HSCIC Guidance and Caldicott 2 | | |
| 2,0 | Hayley Gillingwater | Updates to reflect GDPR & DPA 18.<br>Updates to Data Protection Principles<br>Update to reference materials<br>Removal of fax guidelines – (no longer appropriate to use fax). | Integrated Audit and Governance Committee 12 November 2019 | November 2019 |

**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. This 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 Hull 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.

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 2018 and the General Data Protection Regulation (GDPR).
- Protect PCD in areas accessed by the public.
- Ensure that information accessed remotely is done so securely.

## 2. SCOPE

This policy applies to all staff, CCG Members, temporary staff, seconded staff, 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:

### 2.1. 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.

### 2.2 Caldicott Guardian

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

### 2.3 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.

### 2.4 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 (Annex A) 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.
- 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.

The IAR is sent to IAOs to be updated on a quarterly basis, IAOs are required to respond to the call for updates even if there are no changes to their assets.

## 3. POLICY PURPOSE AND AIMS

### 3.1 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 some methods may be convenient and quick would that information be better safeguarded if it was communicated by telephone or secure email?

### 3.2 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 Annex A below, which allows a self-assessment of the controls in place within your department

### 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.

**Data Protection/ General Data Protection Regulation Principles**

1. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfullness, fairness and transparency');
   (a) at least one of the conditions in Article 6 of the GDPR is met, and
   (b) in the case of sensitive personal data, at least one of the conditions in Article 9 of the GDPR or Schedule 1 of the DPA 18 is also met.
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 shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. ('data minimisation');
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 ('accuracy');
5. kept in a form which permits identification of the data subject 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 in accordance with Article 89(1) subject to the implementation of appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
6. 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 ('integrity and confidentiality').
7. Personal data shall be processed in accordance with the rights of data subjects under this Act.
8. 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.

## 4. IMPACT ANALYSIS

### 4.1 Equality

This Policy forms part of the CCG's commitment to create a positive culture of respect for all staff and service users. The intention is to identify, remove or minimise discriminatory practice in relation to the protected characteristics (race, disability, gender, sexual orientation, age, religious or other belief, marriage and civil partnership, gender reassignment and pregnancy and maternity), as well as to promote positive practice and value the diversity of all individuals and communities. As part of its development this Policy and its impact on equality has been analysed and no detriment identified.

An equality impact screening analysis has been carried out on this protocol.

As a result of performing the analysis, the protocol does not appear to have any adverse effects on people who share Protected Characteristics and no further actions are recommended at this stage; details are available alongside this protocol on the CCG's website.

### 4.2 Sustainability

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

### 4.3 Bribery Act 2010

NHS Hull Clinical Commissioning Group has a responsibility to ensure that all staff are made aware of their duties and responsibilities arising from The Bribery Act 2010.

The Bribery Act 2010 makes it a criminal offence to bribe or be bribed by another person by offering or requesting a financial or other advantage as a reward or incentive to perform a relevant function or activity improperly performed. The penalties for any breaches of the Act are potentially severe. There is no upper limit on the level of fines that can be imposed and an individual convicted of an offence can face a prison sentence of up to 10 years.

For further information see http://www.justice.gov.uk/guidance/docs/bribery-act-2010-quick-start-guide.pdf.

If you require assistance in determining the implications of the Bribery Act please contact the Local Counter Fraud Specialist on telephone number 01482 866800 or email at nikki.cooper1@nhs.net.

Due consideration has been given to the Bribery Act 2010 in the development of this policy (or review, as appropriate) of this policy document and no specific risks were identified.

## 5. NHS CONSTITUTION

5.1 The CCG is committed to: Designing and implementing services, policies and measures that meet the diverse needs of its population and workforce, ensuring that no individual or group is disadvantaged.

5.2 This Policy supports the NHS Constitution as follows:
The NHS aspires to the highest standards of excellence and professionalism in the provision of high-quality care that is safe, effective and focused on patient experience; in the planning and delivery of the clinical and other services it provides; in the people it employs and the education, training and development they receive; in the leadership and management of its organisations; and through its commitment to innovation and to the promotion and conduct of research to improve the current and future health and care of the population.

:

## 6. IMPLEMENTATION

The policy will be disseminated by being made available on the website and highlighted to staff at team meetings and by managers.

*'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

Staff will be made aware of the policy via the website and internal distribution lists.

## 8. MONITORING AND EFFECTIVENESS

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

## 9. POLICY REVIEW

This policy will be reviewed in 2 years. 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.

## 10. 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 - https://s3-eu-west-1.amazonaws.com/comms-mat/Training-Materials/Guidance/encryptionguide.pdf
- 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
- The General Data Protection Regulation (GDPR)
- The Data Protection Act 2018

## APPENDICES

### Safe Haven Self -assessment Questionnaire

**Annex A**

| 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.<br><br>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 | | | | |

| No. | Guidance | *Current departmental process* | Adequate YES/NO | Corrective action identified (Where Applicable) | Action Date and officer nominated |
|---|---|---|---|---|---|
| | 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.<br><br>In addition manual records placed in a file should be secured within that file to prevent accidental loss of pages. | | | | |

| No. | Guidance | *Current departmental process* | Adequate YES/NO | Corrective action identified (Where Applicable) | Action Date and officer nominated |
|---|---|---|---|---|---|
| **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. | | | | |
| **3** | Proper system access controls should be in place i.e. passwords and access levels for each user.<br><br>Staff should be made aware of their responsibilities in respect the management and security of passwords and smartcards, e.g. passwords and | | | | |

| No. | Guidance | *Current departmental process* | Adequate YES/NO | Corrective action identified (Where Applicable) | Action Date and officer nominated |
|---|---|---|---|---|---|
| | 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.<br><br>VPN access should only be used in association with equipment that has been encrypted and issued by the IT department for work purposes. | | | | |

| No. | Guidance | *Current departmental process* | Adequate YES/NO | Corrective action identified (Where Applicable) | Action Date and officer nominated |
|---|---|---|---|---|---|
| **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*** | | | | | |
| **1** | Only equipment that has been encrypted and issued by the IT 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.<br><br>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 | | | | |

| No. | Guidance | *Current departmental process* | Adequate YES/NO | Corrective action identified (Where Applicable) | Action Date and officer nominated |
|---|---|---|---|---|---|
| | directly to the person authorised to receive that information.<br><br>Staff must also be aware of HSCIC: Sending an encrypted email from NHSmail to a non-secure email address<br><br>https://s3-eu-west-1.amazonaws.com/comms-mat/Training-Materials/Guidance/encryptionguide.pdf | | | | |
| **3** | Where necessary consent is obtained from the data subject for any transfers of PCD in line with the documented information sharing agreement for that service<br><br>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. | | | | |
| **5** | Routine transfers of PCD, to and from the organisation, by whatever method, should be recorded on a data mapping spreadsheet, to ensure appropriate | | | | |

| No. | Guidance | *Current departmental process* | Adequate YES/NO | Corrective action identified (Where Applicable) | Action Date and officer nominated |
|---|---|---|---|---|---|
| | controls of the data at all times.<br><br>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.<br><br>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.<br><br>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.<br><br>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<br><br>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.<br><br>These records should never be left unattended. | | | | |
| **4** | Appropriate transportation methods should be implemented, e.g. carried in a container or via encrypted electronic methodology. | | | | |

| No. | Guidance | *Current departmental process* | Adequate YES/NO | Corrective action identified (Where Applicable) | Action Date and officer nominated |
|---|---|---|---|---|---|
| **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.<br><br>A record of information being sent should be maintained on the project or patient file, including when, to whom and by what method<br><br>When necessary ask the recipient to confirm the receipt of the package.<br><br>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.<br><br>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 | | | | |

| No. | Guidance | *Current departmental process* | Adequate YES/NO | Corrective action identified (Where Applicable) | Action Date and officer nominated |
|---|---|---|---|---|---|
| | 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.<br><br>**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 | | | | |
| ***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.<br><br>Guidance on the use of NHS Secure Mail can be found at: https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including- | | | | |

| No. | Guidance | *Current departmental process* | Adequate YES/NO | Corrective action identified (Where Applicable) | Action Date and officer nominated |
|---|---|---|---|---|---|
| | extractions/publications-and-notifications/standards-and-collections/dcb1596-secure-email | | | | |
| **2** | All secure email addresses should be checked to ensure the correct email recipient has been selected.<br><br>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)<br><br>**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<br><br>'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 | | | | |

| No. | Guidance | *Current departmental process* | Adequate YES/NO | Corrective action identified (Where Applicable) | Action Date and officer nominated |
|---|---|---|---|---|---|
| | 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.<br><br>It is important to guard against people seeking information by deception this is particularly risky when using mobile telephone numbers.<br><br>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.<br><br>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.<br><br>**NB/** Messages should not contain PCD but should refer readers to proper records. | | | | |

| No. | Guidance | *Current departmental process* | Adequate YES/NO | Corrective action identified (Where Applicable) | Action Date and officer nominated |
|---|---|---|---|---|---|
| ***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.<br><br>Do not indicate the reason for the call. | | | | |
| ***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. | | | | |

| No. | Guidance | *Current departmental process* | Adequate YES/NO | Corrective action identified (Where Applicable) | Action Date and officer nominated |
|---|---|---|---|---|---|
| **4** | Where message books are used they should be held securely and access limited on a need to know basis.<br><br>**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 requests received and appropriate staff identified | | | | |

| No. | Guidance | *Current departmental process* | Adequate YES/NO | Corrective action identified (Where Applicable) | Action Date and officer nominated |
|---|---|---|---|---|---|
| | and trained to deal with these requests. | | | | |
| **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. | | | | |
| ***Reporting Incidents*** | | | | | |

| No. | Guidance | *Current departmental process* | Adequate YES/NO | Corrective action identified (Where Applicable) | Action Date and officer nominated |
|---|---|---|---|---|---|
| **1** | Staff should be aware that all breaches of confidentiality and information security must be reported, including near misses.<br><br>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.<br><br>IG Statutory and Mandatory Training must be been completed annually and additional Information Governance Training Needs Analysis, training modules identified to be completed as appropriate to the job role. | | | | |
| ***Business Intelligence Only (Implementation of Accredited Safe Haven)*** | | | | | |

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

| No. | Guidance | *Current departmental process* | Adequate YES/NO | Corrective action identified (Where Applicable) | Action Date and officer nominated |
|---|---|---|---|---|---|
| | governing body and recorded on the risk register. | | | | |

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

Please refer to the EIA Overview & Navigation Guidelines located in *Y:\HULLCCG\Corporate Templates and Forms\Equality and Diversity Information* before completing your EIA)

| HR / Corporate Policy Equality Impact Analysis: | |
|---|---|
| **Policy / Project / Function:** | Security and Transmission of Personal Confidential Data and Information (Safe Haven) Policy V2.0 |
| **Date of Analysis:** | 07/10/2019 |
| **Completed by:**<br>**(Name and Department)** | Hayley Gillingwater – Senior Information Governance Specialist |
| **What are the aims and intended effects of this policy, project or function?** | This document provides justification and defines guidance for the transfer of personal confidential data in a secure way. |
| **Are there any significant changes to previous policy likely to have an impact on staff / other stakeholder groups?** | No significant changes:<br>Updates to reflect GDPR & DPA 18.<br>Updates to Data Protection Principles<br>Update to reference materials<br>Removal of fax guidelines – (no longer appropriate to use fax). |
| **Please list any other policies that are related to or referred to as part of this analysis** | N/A |
| **Who will the policy, project or function affect?** | Staff employed by Hull CCG and relevant others |
| **What engagement / consultation has been done, or is planned for this policy and the equality impact assessment?** | Consultation will take place with Information Governance staff at the Information Governance Steering Group, Senior Leadership Team and relevant others |
| **Promoting Inclusivity and Hull CCG's Equality Objectives.**<br><br>How does the project, service or function | The policy does not directly promote inclusivity but provides a framework for the secure handling and transfer of personal data ensuring staff are supported by |

| | |
|---|---|
| contribute towards our aims of eliminating discrimination and promoting equality and diversity within our organisation?<br><br>How does the policy promote our equality objectives:<br>1. Ensure patients and public have improved access to information and minimise communications barriers<br><br>2. To ensure and provide evidence that equality is consciously considered in all commissioning activities and ownership of this is part of everyone's day-to-day job<br><br>3. Recruit and maintain a well-supported, skilled workforce, which is representative of the population we serve<br><br>4. Ensure the that NHS Hull Clinical Commissioning Group is welcoming and inclusive to people from all backgrounds and with a range of access needs | management and health professionals. |

| Equality Data | |
|---|---|
| **Is any Equality Data available relating to the use or implementation of this policy, project or function?**<br><br>Equality data is internal or external information that may indicate how the activity being analysed can affect different groups of people who share the nine *Protected Characteristics* – referred to hereafter as *'Equality Groups'.*<br><br>Examples of *Equality Data* include: (this list is not definitive)<br><br>1: Recruitment data, e.g. applications compared to the population profile, application success rates<br>2: Complaints by groups who share / represent protected characteristics<br>4: Grievances or decisions upheld and dismissed by protected characteristic group<br>5: Insight gained through engagement | No ☐<br><br>Where you have answered yes, please incorporate this data when performing the *Equality Impact Assessment Test* (the next section of this document). If you answered No, what information will you use to assess impact?<br><br>**Please note that due to the small number of staff employed by the CCG, data with returns small enough to identity individuals cannot be published. However, the data should still be analysed as part of the EIA process, and where it is possible to identify trends or issues, these should be recorded in the EIA.** |

| | |
|---|---|
| | |

## 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)**

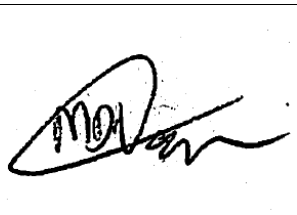
| Protected Characteristic: | Neutral Impact: | Positive Impact: | Negative Impact: | Evidence of impact and, if applicable, justification where a *Genuine Determining Reason*[1] exists (see footnote below – seek further advice in this case) |
|---|---|---|---|---|
| **It is anticipated that these guidelines will have a positive impact as they support policy writers to complete meaningful EIAs, by providing this template and a range of potential issues to consider across the protected characteristics below. There may of course be other issues relevant to your policy, not listed below, and some of the issues listed below may not be relevant to your policy.** | | | | |
| **Gender** | x | | | Policy applies to all staff regardless of gender. |
| **Age** | x | | | Policy applies to all staff regardless of age. |
| **Race / ethnicity / nationality** | x | | | Policy applies to all staff regardless of race, ethnicity or nationality. |
| **Disability** | x | | | Policy applies to all staff regardless of disability. |
| **Religion or Belief** | x | | | Policy applies to all staff regardless of religion or belief. |
| **Sexual Orientation** | x | | | Policy applies to all staff regardless of sexual orientation. |
| **Pregnancy and Maternity** | x | | | Policy applies to all staff regardless of pregnancy or maternity. |
| **Transgender / Gender reassignment** | x | | | Policy applies to all staff regardless of transgender/ gender reassignment. |

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

| | | | | |
|---|---|---|---|---|
| **Marriage or civil partnership** | x | | | Policy applies to all staff regardless of marriage or civil partnership. |

| **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:** |
| It is recognised that this Policy is written in English and there is therefore a risk to the staff whose first language is not English for misunderstanding. | The CCGs internal 'portal' and external website signpost individuals to alternative formats such as large print, braille or another language. | CCG Communications | Updating of this facility is ongoing | 2 years from approval date. |
| | | | | |
| | | | | |

| **Sign-off** |
|---|
| **All policy EIAs must be signed off by Mike Napier, Associate Director of Corporate Affairs** |
| **I agree with this assessment / action plan** |
| **If *disagree*, state action/s required, reasons and details of who is to carry them out with timescales:** |



**Signed:**

**Date: 30.10.19**