****

DATA PROTECTION AND CONFIDENTIALITY POLICY

**June 2023**

|  |  |
| --- | --- |
| **Authorship:** | Corporate Affairs |
| **Committee Approved:** | SIRO & Information Governance Groups |
| **Approved date:** | June 2023 |
| **Equality Impact Assessment:** | March 2023 |
| **Target Audience:** | ICB Board and its Committees and Sub-Committees, ICB Staff, agency, and temporary staff & third parties under contract |
| **Policy Number:** | ICB39 |
| **Version Number:** | 1.0 |

**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.**

**AMENDMENTS**

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **New Version Number** | **Issued by** | **Nature of Amendment** | **Approving body** | **Approval date** | **Date published on website** |
| 1.0 | Executive Director of Corporate Affairs | New policy for ICB | SIRO | 22.06.23 | 27.06.23 |

Contents

[1 Introduction 4](#_Toc130985141)

[2 Purpose 4](#_Toc130985142)

[3 Definition/ Explanation of Terms 4](#_Toc130985143)

[4 Scope of the Policy 5](#_Toc130985144)

[5 Duties/ Accountabilities and Responsibilities 5](#_Toc130985145)

[6 Policy Document Requirements 6](#_Toc130985146)

[7 Consultation 10](#_Toc130985147)

[8 Training 10](#_Toc130985148)

[9 Monitoring Compliance 10](#_Toc130985149)

[10 Arrangements for Review 10](#_Toc130985150)

[11 Dissemination 10](#_Toc130985151)

[12 Associated Documentation 10](#_Toc130985152)

[13 References 11](#_Toc130985153)

[14 Appendices 11](#_Toc130985154)

[15 Impact Assessments 11](#_Toc130985155)

[Appendix 1 - Anti-Fraud, Bribery and Corruption 11](#_Toc130985156)

[Appendix 2 - Mechanisms for Auditing Information Security Control 13](#_Toc130985157)

[Appendix 3 – Safe Haven Checklist 14](#_Toc130985158)

# Introduction

The Humber and North Yorkshire Integrated Care Board (from this point on known as the HNY ICB), has a statutory duty to safeguard the information it holds. The HNY ICB has a legal obligation to comply with appropriate legislation in respect of data, information, and information security. All employees or anyone working for or on behalf of the HNY ICB are bound by a legal duty of confidence to protect personal confidential information they may encounter during their work. The principle of this policy is that no individual, including Third Party Contractors, volunteers and seconders working for or on behalf of the HNY ICB shall misuse any information it processes or comes into contact with or allow others to do so.

All health and care organisations have a legal duty to share information about a patient or service user to facilitate their individual care. The duty to share information for individual care is as important as the duty to protect confidentiality. This policy is intended to provide guidance to help support you so that you can share information correctly, safely, and securely.

The [Caldicott Principles](https://www.gov.uk/government/publications/the-caldicott-principles) help to ensure that health and care information is used and shared appropriately to support care. Please follow the guidance set out in the principles when sharing information for care and other purposes.

# Purpose

The purpose of this policy is to set out the HNY ICB’s commitment to the confidentiality and safe appropriate sharing of information and its responsibilities and compliance with the Data Protection legislation regarding the disclosure of such information.

# Definition/ Explanation of Terms

**Data Controller** – the person or organisation that determines the purpose and means of personal data processing.

**Data Processor** – the person or organisation (other than an employee of the Data Controller) that processes data on behalf of and/or under the instruction of the Data Controller.

**Data Subject** - a living individual who is the subject of the personal data.

**Personal Confidential Data** – Data that relates to a living individual that can identify the individual from the data or other information in the possession of the data controller or data processor (e.g.name, address, NHS number)

**Sensitive Personal Data** - also known as ‘Special Category Data’- Data that relates to a living individual that includes racial or ethnic origin; political opinions; religious or other beliefs; trade union membership; Health data (physical or mental health conditions); genetics; sex life and sexual orientation; criminal proceedings, convictions or biometric data (where used for identification purposes).

**Third Party** - any person other than; The data subject; The data controller or any data processor or other person authorised to process data on behalf of the data controller.

**Processing** - in relation to information or data means; obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, which may include adaptation or alteration of the information; retrieval, or use of the information or data; disclosure of the information or data by transmission, dissemination or otherwise making available, or alignment, combination, blocking, erasure or destruction

of the information or data. In summary anything you do with data is “processing”.

# Scope of the Policy

The policy applies to HNYICB, its employees and must be followed by all those who work for the organisation, including the Health, and Care Partnership, those on temporary or honorary contracts, secondments, pool staff, contractors, and students.

This policy applies to all information, held in manual or electronic format by or on behalf of the HNY ICB and includes, but is not limited to, photographs, images, electronic media, and CCTV.

# Duties/ Accountabilities and Responsibilities

**Chief Executive**

## Overall accountability for procedural documents across the organisation lies with the Chief Executive, for meeting all statutory requirements and adhering to guidance issued in respect of procedural documents.

## Executive Director of Corporate Affairs

The Executive Director of Corporate Affairs has delegated responsibility for the operational management of Data Protection and Confidentiality and will be supported by Senior Information Governance Manager

**Information Governance Specialist**

The ICB’s Caldicott Guardian(CG), Senior Information Risk Owner (SIRO), and Data Protection Officer(DPO) are responsible for overseeing and advising on disclosure of individual’s information held by the ICB.

**Senior Information Governance Manager**

The Senior Information Governance Manager is responsible for ensuring effective management, accountability, compliance, and assurance for all aspects of information governance within the organisation.

**Line Managers**

Line managers are responsible for ensuring that all staff, (including, temporary staff, contractors, and volunteers, know what is expected of them and are aware of their responsibilities towards the protection and confidentiality of information and ensure that it is held and processed in a confidential secure manner.

All staff should be aware of:

• their responsibilities for data protection and confidentiality

• the key principles for safeguarding confidentiality

• preserving information security

• complying with all information governance policies and completing their statutory and mandatory Data Security & Awareness training

## Responsibilities for approval

The ICB Board is responsible for the review and approval of this policy.

# Policy Document Requirements

**6.1 Data Protection & Confidentiality**

The HNY ICB is committed to the delivery of a first-class confidential service. This means ensuring that all personal service user and staff information is processed fairly, lawfully, and as transparently as possible so that the public can:

• understand the reasons for processing personal information.

• give their consent for the disclosure and use of their personal information where relevant and necessary.

• gain trust in the way the HNY ICB handles information; and

• understand their rights to access information held about them

**6.2 Protecting Personal Confidential and Corporately Sensitive Information**

• The HNY ICB is responsible for protecting all the information it holds at all times and must always be able to justify any decision to share information.

• Personal confidential information, wherever possible, must be anonymised by removing as many identifiers as possible whilst not unduly compromising the utility of data.

• Appropriate data processing agreements need to be in place with the relevant organisations.

• Access to rooms and offices where terminals are present or personal confidential information or corporately confidential information is stored must be controlled. Doors must be locked with keys, keypads or accessed by swipe card. In mixed office environments measures should be in place to prevent oversight of personal confidential information or corporately confidential information by unauthorised parties.

• Working from home creates a new dynamic with the use of different IT solutions presenting other risks than in an office environment, particularly when it comes to data protection. Staff should treat the data collected and handled in the same way as if they were in the workplace and should not prioritise convenience over security. The HNY ICB have updated their policies and procedures accordingly.

• All staff should follow a clear desk and screen policy when left unattended and at the end of each day. They must keep all records containing personal confidential information or corporately confidential information in recognised filing and storage places that are locked.

• Staff should ensure that they cannot be overheard when discussing confidential matters.

• Print options should only be used if necessary or relevant, any unwanted printouts containing personal confidential information or corporately confidential information must be put into a confidential waste bin provided. Discs, tapes, printouts, must not be left lying around but be filed and locked away when not in use.

• At home staff will not have the facility of confidential waste bins. Therefore, printed material should be safely stored e.g., in a locked drawer or safe, until they can be taken into the office and disposed of securely.

• Staff should be extra vigilant about opening web links and attachments in emails or other messages and should not click on unfamiliar web links or attachments.

• Data Security Awareness training is mandatory, and all staff should ensure IT equipment has been updated when prompted to do so.

• The Contract of Employment includes a commitment to confidentiality. Breaches of confidentiality could be regarded as gross misconduct and may result in serious disciplinary action up to and including dismissal.

**6.3 Data Protection Principles**

The Data Protection Act applies GDPR Data Protection principles to support good practice and fairness in processing personal information. Compliance with these key principles is therefore a fundamental for good data protection practice.

Employees must be aware of these requirements and ensure that any use of personal data satisfies the requirements of the principles.

Where applicable the Caldicott Principles as well as the Data Protection Principles will be complied with. Further details on these principles can be found at [data protection principles](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/) and [Caldicott Principles](https://www.gov.uk/government/publications/the-caldicott-principles)

## Disclosing Information

Whether personal information can be disclosed to others is dependent on a number of factors, including, whether the individual has consented to the information being shared, to whom the information is being disclosed and the reason for its disclosure. The approach may vary according to the individual circumstances surrounding the disclosure.

HNY ICB will inform the data subject why, how and for what purpose personal information is collected, recorded, and processed by means of a privacy notice published on the HNY ICB [website](https://humberandnorthyorkshire.icb.nhs.uk/privacy-policy/) and where necessary information leaflets.

To process personal data, Health and Social care organisations must comply with one of the lawful bases for processing data. There are number of lawful bases for processing personal or special category data as set out in the GDPR articles 6 & 9. The most appropriate basis for lawful processing available to health and social care organisations in the delivery of their functions are:

* 6(1)(e) ‘…for the performance of a task carried out in the public interest or in the exercise of official authority…’
* 9(2)(h) ‘…for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services

To note consent is not a lawful basis for processing where the disclosure is necessary for healthcare purposes.

All individuals must:

* exercise all due care and diligence to prevent unauthorised disclosure of confidential information.
* ensure the physical security of all confidential documents, including storage of files on corporate devices.
* exercise care in transferring information to ensure that the method used is as secure as it can be. In most instances a Data Sharing, Data Re-Use or Data Transfer Agreement will have been completed before any information is transferred. The Agreement will set out any conditions for use and identify the mode of transfer.

Transferring any personal data by email to anyone outside the HNY ICB network may only be undertaken through the NHS Mail system (i.e., from one NHSnet account to another NHSnet account or to a secure government domain e.g., gsi.gov.uk), since this ensures that mandatory government standards on encryption are met, as set out in NHS mail good practice guidance.

The NHS Mail secure facility must always be used when corresponding with non-NHS Mail account holders where confidential information needs to be sent. This allows personal confidential information to be sent securely to non-NHS Mail addresses and allows the recipient to respond in a secure manner. <https://digital.nhs.uk/services/nhsmail/guidance-for-sending-secure-email>

If staff have any concerns about disclosing information, they must discuss this with their Line Manager or the HNY ICB’s Data Protection Officer.

## Disclosure of Personal Data and Transfers outside the UK

Personal data will not be transferred (including hosting) outside of the UK without the consent of the data subject, unless the following circumstances apply:

* It supports the HNY ICB’s statutory functions and provides significant benefit to the HNY ICB or patients.
* Adequate safeguards, such as contractual clauses, have been included within any agreement with the third party receiving the personal data.
* Appropriate assessment of the security standards of the recipient of the data.
* The transfer has been approved by the Data Protection Officer.

## National Data Opt-Out

The National Data Opt-Out Programme allows patients to opt-out of uses of their data, for purposes other than direct care. The HNY ICB will notify patients of this right via the privacy notice.

The National Data Opt-Out is applied by NHS Digital at source and will therefore be applied prior to receipt of data processed for the HNY ICB’s functions. The ICB’s National Data Opt-Out Policy is available on our [website](http://humberandnorthyorkshire.icb.nhs.uk/documents-and-publications/).

## Abuse of Privilege

It is strictly forbidden for employees to knowingly browse, search for or look at any information relating to themselves, their own family, friends, or other persons, without a legitimate purpose. Action of this kind will be viewed as a breach of confidentiality and of the current Data Protection Act and the United Kingdom General Data Protection Regulation.

When dealing with personal confidential information or corporately confidential information of any nature, staff must be aware of their personal responsibility, contractual obligations and undertake to abide by the policies and procedures of the HNY ICB.

If staff have concerns about this issue, they should discuss it with their Line Manager.

## Data Protection Breaches

Where it is identified that personal data is disclosed to, or accessed by, any person or organisation not entitled to see it, this must be reported on the HNY ICB incident app and to their Line Manager. The breach will be managed in accordance with the HNY ICB’s incident policy.

## Termination or expiry of a contract with the HNY ICB

On leaving or termination of a contract with the HNY ICB any copies of software, documents or correspondence, diaries, documents, plans, specifications, or any other information relevant to the HNY ICB (whether or not prepared or produced by the individual) must be returned to the HNY ICB’s possession and under no circumstances must the leaver take this information with them. All individuals that have left the HNY ICB are bound by this policy that was in publication at the time of their departure.

## Confidentiality Audit

Appropriate systems must be implemented to ensure that personal confidential information and commercially sensitive information is held and processed in a confidential and secure manner. To ensure that appropriate controls are maintained the HNY ICB have implemented a regular system of reviews and audits to assess controls in place and compliance to these controls. Mechanisms to achieve this are detailed at Appendix A.

## Secure Handling of Information (Safe Haven)

Secure and appropriate handling of information is essential to maintain confidentiality of both personal identifiable information and commercially sensitive information. Appropriate controls must be in place to ensure the secure transfer, receipt, storage, and disposal of personal confidential information, to protect it from loss, damage, or unauthorised access.

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.

A checklist for appropriate methods of handling, processing, and transferring information has been developed to guide staff. See Appendix B

# Consultation

All stakeholders such as ICB SIRO/DPO and Executive lead and IG leads involved in developing, implementing, managing, and monitoring Data Protection and Confidentiality have been engaged in the development of this policy.

# Training

All ICB employees and Board Members (including temporary or contractors) are required to undertake Data Security Awareness training on an annual basis.

Where relevant further specialist training is required, staff will be informed by the Training Needs Analysis.

# Monitoring Compliance

Adherence to this policy will be monitored through staff awareness and supporting evidence as part of the Data Security Protection Toolkit compliance.

# Arrangements for Review

This policy will be formally approved by the ICB Board and will be reviewed every 3 years. Earlier review may be required in response to exceptional circumstances, organisational change, or relevant changes in legislation/guidance, as instructed by the Executive Director responsible for this policy.

# Dissemination

The policy will be disseminated by being made available on the ICB website and highlighted to staff through staff communications, and by managers.

**Breaches of this policy may be investigated and may result in the matter being treated as a disciplinary offence under the HNY ICB’s disciplinary procedure.**

# Associated Documentation

* Information Governance Framework & Strategy
* IT & Information Security Policies
* Privacy by Design
* Subject Access Request
* Information Governance Staff Handbook
* Incident Policy

This list is not exhaustive.

# References

This policy is designed to reflect the following legislation and mandatory NHS standards.

* UK General Data Protection Regulation
* Data Protection Act 2018
* The Common Law Duty of Confidentiality
* Privacy and Electronic Communications Regulations
* Confidentiality: NHS Code of Practice (Department of Health)
* Health and Social Care (Safety and Quality) Act 2015
* Caldicott Principles
* The Public Interest Disclosure Act 1998
* Human Rights Act 2000
* Public Records Act 1958

# Appendices

Appendix 1 – Anti fraud, bribery, and corruption

Appendix 2 - Mechanisms for Auditing Information Security Control

Appendix 3 – Safe Haven checklist

# Impact Assessments

## Equality

In developing this policy an Equality Impact Analysis (EIA) has been undertaken. As a result of performing the analysis, the policy does not appear to have any adverse effects on people who share Protected Characteristics, and no further actions are recommended at this stage.

## Bribery Act 2010

Due consideration has been given to the Bribery Act 2010 in the development (or review, as appropriate) of this policy document, further details can be found in appendix 1.

## General Data Protection Regulations (GDPR)

The General Data Protection Regulation (GDPR)/ Data Protection Act 2018 includes the requirement to complete a Data Protection Impact Assessment for any processing that is likely to result in a high risk to individuals.

Consideration should be given to any impact the policy may have on individual privacy; please consult NHS Humber and North Yorkshire ICB Data Protection Impact Assessment Policy

The ICB is committed to ensuring that all personal information is managed in accordance with current data protection legislation, professional codes of practice and records management and confidentiality guidance as detailed within this policy and related policies and procedures.

If you are commissioning a project or undertaking work that requires the processing of personal data, you must complete a Data Protection Impact Assessment

# Appendix 1 - Anti-Fraud, Bribery and Corruption

The ICB has a responsibility to ensure that all staff are made aware of their duties and responsibilities arising from the Bribery Act 2010.  Under the Bribery Act 2010 there are four criminal offences:

•           Bribing or offering to bribe another person (Section 1)

•           Requesting, agreeing to receive or accepting a bribe (Section 2);

•           Bribing, or offering to bribe, a foreign public official (Section 6);

•           Failing to prevent bribery (Section 7).

These offences can be committed directly or by and through a third person and, in many cases, it does not matter whether the person knows or believes that the performance of the function or activity is improper.

It should be noted that there need not be any actual giving and receiving for financial or other advantage to be gained, to commit an offence.

All individuals should be aware that in committing an act of bribery they may be subject to a penalty of up to 10 years imprisonment, an unlimited fine, or both.  They may also expose the organisation to a conviction punishable with an unlimited fine because the organisation may be liable where a person associated with it commits an act of bribery.

Individuals should also be aware that a breach of this Act renders them liable to disciplinary action by the ICB, whether or not the breach leads to prosecution.  Where a material breach is found to have occurred, the likely sanction will be loss of employment and pension rights.

To raise any suspicions of bribery and/or corruption please contact the Executive Director of Finance and Investment.  Staff may also contact the Local Counter Fraud Specialist (LCFS) at – Audit Yorkshire, email:  [nikki.cooper1@nhs.net](mailto:nikki.cooper1@nhs.net)  or mobile 07872 988939.

The LCFS or Executive Director of Finance and Investment should be the contact for any suspicions of fraud. The LCFS will inform the Executive Director of Finance and Investment if the suspicion seems well founded and will conduct a thorough investigation.  Concerns may also be discussed with the Executive Director of Finance and Investment or the Audit Committee Chair.

If staff prefer, they may call the NHS Counter Fraud reporting line on 0800 028 40 60 between 8am-6pm Monday-Friday or report online at [www.reportnhsfraud.nhs.uk](http://www.reportnhsfraud.nhs.uk).  This would be the suggested contact if there is a concern that the LCFS or the Executive Director of Finance and Investment themselves may be implicated in suspected fraud, bribery, or corruption.

# Appendix 2 - Mechanisms for Auditing Information Security Control

The Data Security Protection Toolkit (DSPT) requires the ICB to undertake regular audits as appropriate to ensure the following reviewed as necessary.

1. General Information Security/ Safe Haven Procedures (Appendix 3)

It is essential that all departments have appropriate information security controls in place to always protect personal/sensitive confidential data. The security and transmission of confidential information/safe haven standard includes an audit checklist to enable IAOs and senior leadership to record the assessment of controls in place.

1. Review of Information Asset Register and associated Data Flow Maps

Information asset owners must on a regular basis review their information asset register to ensure that all information assets are recorded, and the associated information flow maps have been documented and risk assessed.

1. Review of Network Folders and individual systems access

Access of staff to network folders should be reviewed on a regular basis, to ensure that leavers have been removed and access allocated is appropriate to the job role. This will require reports of access levels to be produced via the IT department and senior leadership/team levels to review access levels set.

This process also needs to be undertaken for specific systems, to ensure that access is allocated to staff on a need-to-know basis and that all live users are current employees.

1. Failed Logins

Periodically and upon the suspicion of attempted unauthorised access to network folders or an individual system, checks should be made to assess whether unauthorised access has been attempted or obtained. The IT Department would need to assist in the production of reports enable these assessments to be undertaken.

1. Monitoring Incidents

All Information Security and Confidentiality incidents reported must be monitored and investigated and reported to the Information Governance Steering Groups this includes potential and actual incidents identified as a result of any audit work undertaken.

**Audit Reporting and Follow-up**

A formal report will be produced detailing the outcome of the audit, recommendations, corrective action, and completion timescales agreed. These reports will be provided to the SIRO for approval and reported as part of the Data Security Protection Toolkit.

Arrangements should be made to follow-up corrective action agreed to ensure appropriate implementation and that where necessary system documentation and procedures are amended accordingly.

All risks identified must be reported as appropriate on the corporate risk register until such a time as appropriate corrective action is complete. All residual risks must remain on the corporate risk register for management consideration.

**Audit Closure**

Once the corrective action has been implemented and checked the audit can be formally closed.

# Appendix 3 – Safe Haven Checklist

| **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 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. |  |  |  |  |
| **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 overlooked, 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 IT 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** | | | | | |
| **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, and 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 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 in line with the documented information sharing agreement for that service  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 controls of the data at all times.  An Information sharing agreement should be documented and agreed by all parties to the information sharing |  |  |  |  |
| **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. |  |  |  |  |
| **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. |  |  |  |  |
| **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. |  |  |  |  |
| **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.  Use of Tamper proof envelopes  **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. |  |  |  |  |
| **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. |  |  |  |  |
| ***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 overheard 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. |  |  |  |  |
| **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** | | | | | |
| **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 area, 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 requests received and appropriate staff identified 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** | | | | | |
| **1** | Staff should be aware that all breaches of confidentiality and information security must be reported, 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.  Data Awareness Statutory and Mandatory Training must be completed annually and any additional specialist 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. |  |  |  |  |
| **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. |  |  |  |  |