NHS
Coventry and Warwickshire
Integrated Care Board

Safe Haven Policy

Reference Number:	IG/08
Version:	Version 1.1
Name of responsible Committee and date approved or recommended to Integrated Care Board Board:	Audit Committee 12 November 2027
Date approved by the Integrated Care Board (if applicable):	N/A
Next Review Date:	12 May 2027
Expiry Date:	12 November 2027
Name of author and title:	Kelly Huckvale, Senior Information Governance Manager, AGEM CSU
Name of reviewer and title:	Laura Whiteley, Governance and Corporate Affairs Manager, ICB
Department:	Governance (Information Governance)

VERSION HISTORY

Date	Version	Changes made to previous version	Consulting and Endorsing Stakeholders, Committees / Meetings / Forums etc.
03/10/2024	V1.1	Updated job titles and general update and review	Information Governance Steering Group

Contents

1. Introduction

1.1 The purpose of this policy is to ensure that patient confidentiality is maintained within all areas of NHS Coventry and Warwickshire Integrated Care Board ('the ICB'). Where there is a need to transfer, transport, distribute or access information remotely staff must ensure that patient of staff confidentiality is not breached.

1.2 According to the Department of Health, the key Safe Haven principles are:

- Each organisation should establish Safe Haven administrative arrangements to safeguard confidential person identifiable information. This includes having one designated contact point per department. Ideally all information exchanged between NHS organisations should pass between Safe Haven contact points.
- All members of staff should be made aware, at least in general terms of the policies and procedures surrounding Safe Haven access.
- Safe Haven procedures should be fully documented and approved by the Caldicott Guardian and agreed by Senior Management.

2. Principles

2.1 In practical terms it may be impossible to have a single Safe Haven contact point in each department within the ICB. This is pertinent when considering e-mail. The solution is to consider Safe Haven in the wider context of confidentiality and includes the concept of restricting access to personal confidential data to authorised staff sufficient to perform the functions and provide cover and back-up to ensure continuity of service ensuring that good practice is followed throughout the whole organisation.

2.2 All actual and potential risks to patient and staff confidentiality should be reported as an information security breach and serious incidents will be included in the ICB's Incident log.

3. Definitions

3.1 Safe Haven

This is a location or in some cases a piece of equipment where arrangements and procedures are in place to ensure confidentiality of all personal confidential data commercially sensitive information based on access controls and data management.

3.2 Removable Media

This is any type of media that can be plugged/inserted into your computer and information can be saved to that media and then removed from your computer for transport or storage. Removable media may be in the form of floppy disks, CD's, DVD's, memory cards, USB memory sticks, external hard drives, etc.

3.3 Portable Devices

This is any device that can be plugged into or synchronised to your computer which contains internal memory that can be saved to. Portable devices may be in the form of digital cameras, mobile phones, iPods/MP3 players, PDAs, etc.

3.4 Secure Locations

The organisation has in place security and Information Governance policies to ensure protection of personal confidential data/commercially sensitive information. Secure areas have been identified across the ICB.

3.5 Insecure Locations

These are locations and equipment that are not protected by the security or Information Governance policies to guarantee the safety of personal confidential data /commercially sensitive information, for example, home computers, personal laptops, internet cafés, local libraries.

3.6 Personal Confidential Data (PCD)

Personal Confidential Data relates to information about any living individual, which would enable that person's identity to be established. This could be a patient /client as well as a member of staff.

It could be an individual piece of data such as an unusual surname or isolated postcode, or it could be a collection of different information, e.g. name and address, which if taken together could allow the person to be identified. All information that relates to an individual should be considered as potentially capable of identifying them.

Full postcodes can identify up to approximately 15 properties (in remote areas a postcode may relate to only one house or even one person), therefore, only use the first half of the postcode, e.g. CV6.

3.7 Special Category/Sensitive Information

Special Category/Sensitive Information, as defined in the Data Protection Act 2018, is usually treated as confidential and the loss or misdirection of such information could impact adversely on the individual(s), the organisation or the wider community.

Information becomes sensitive if it includes any of the following types of information about an identifiable, living individual:

- Personal data revealing racial or ethnic origin.
- Personal data revealing political opinions.
- Personal data revealing religious or philosophical beliefs.
- Personal data revealing trade union membership.
- Genetic data.
- Biometric data (where used for identification purposes).
- Data concerning health.

- Data concerning a person's sex life.
- This does not include personal data about criminal allegations, proceedings or convictions, as separate rules apply.

3.8 Routine Information Flows

This describes departments that have routine information flows of personal confidential data/commercially sensitive information both internally and externally, for example, monthly reports to Commissioners containing patient details or clinical services that regularly receive and send information to other services, such as referral information or patient record details. These information flows are reviewed and updated on an annual basis to ensure that information is accurate, and any associated risks identified and where reasonably practical, appropriately mitigated.

3.9 Data Breaches

However, in reviewing all data breaches, the content of the record, whether staff or patient data, must be considered in terms of the effect that this would have on the individual. In some cases, the loss of one person's details could be highly damaging to the individual and to the reputation of the ICB.

3.10 User

Authorised system users that are identified within each organisation.

3.11 IT Service Provider

The contracted IT service provider will support the ICB in terms of technical and other specialist information technology and security issues.

3.12 Information Governance

This is the framework through which NHS organisations ensure that they are meeting the statutory, mandatory and other best practice requirements for the way data / information is handled, specifically personal and sensitive.

4. Scope

4.1 Safe Havens are designated areas where information can be transported and distributed safely and securely. Safe Haven areas include (but are not restricted to) electronic communication, fax, telephone, transportation of bulk data and post. This is to protect both patient and staff confidentiality and ensure compliance with the Data Protection Act 2018 and the Department of Health requirements within the Data Security Protection Toolkit.

4.2 Each department within the ICB should have designated Safe Haven areas. This is a location or in some cases a piece of equipment where arrangements and procedures are in place to ensure confidentiality of all personal confidential data/commercially sensitive information. Safe Haven includes all methods of transferring personal confidential data/ commercially sensitive information, for example, faxes, telephones, answer phones, message books and post rooms for paper-based information.

This policy applies to all areas within the ICB. The aim of the policy is to:

- Ensure the transfers of information adhere to Caldicott Principles and the Data Protection Act 2018.
- Provide staff with definitive guidance on the use of Safe Haven for distribution information;
- Protect patient confidentiality.
- Ensure that information accessed remotely is done so securely.

5. Statement of Intent

5.1 This policy applies to full-time and part-time employees of the ICB, Non-Executive directors, contracted third party organisations and individuals (including contractors, agency and Bank staff), students/trainees, secondees and other staff on placement with the ICB, and staff or partner organisations with approved access (hereafter referred to as staff).

6. Process - Requirements for Safe Havens - Location/Security Arrangements

6.1 Physical Sites

All physical sites/areas within the ICB must undertake a review the flow of personal confidential data (PCD) / commercially sensitive information both within and external to the ICB.

6.2 Access to Office / Work Area

The office or workspace should be sited in such a way that only authorised staff can enter that location i.e., it should be an area that is not readily accessible to any unauthorised members of staff who work in the same building / office or any visitors to the office.

6.3 Network Folders

Network folders should be reviewed, and access restricted to approved members of staff.

6.4 Paper Records

Manual paper records containing personal confidential data must be stored in locked cabinets or in a facility specifically designed to store records and only accessible by authorised staff.

6.5 Fax Machines

The Department of Health and Social Care (DHSC) announced in December 2018 that NHS organisations and GP practices should have fax machines phased-out by April 2020. It is part of the Health and Social Care Secretary's tech vision, to modernise the health service and make it easier for organisations to use innovative technologies.

The ICB is currently working towards this with primary and secondary providers across their footprint.

But until the project is complete safe haven rules still apply. So, the area where confidential information is received via a fax machine and the paperwork from that transmission must be in a room that is locked or only accessible via a coded keypad or swipe card for authorised staff. Particular attention should be paid to fax machines that are on 24 hours a day when there is not 24-hour supervision. Fax printer ribbons/films should be disposed of securely.

6.6 Computers / Laptops

Computers must not be accessible to unauthorised users. Computers must be password protected by members of staff when left unattended. This can be done by using the Ctrl + Alt + Del or Windows + L keys. Computer usernames and passwords must not be shared with or made easily visible to others.

6.7 Information Asset Register

The ICBs must maintain an Information Asset Register which includes and documents all the confidential data flows internal and external for all departments across the ICB's sites.

6.8 Post Rooms

Post rooms must only be accessible by authorised staff and should be adequately secured from unauthorised access, i.e. situated in a secure area behind access-controlled security doors.

6.9 Reception Areas

Reception areas with post trays must ensure that when the reception area is not staffed all post is secured by either locking it away or where possible locked in a room not accessible to the general public or visitors.

6.10 Answer Machines/ Voicemail

Where staff have telephones that receive and store messages containing personal confidential data/commercially sensitive information, access to those messages should only be possible by use of an individual password or the position of the answer machine should be within a haven/secure area. Where answer phones are attached to telephones, steps must be taken to ensure that only authorised members of staff have access to the answer phone. Staff should review the volume of answer phones where messages can be overheard by others to ensure that confidential information is protected. The use of answer phones in reception areas is discouraged for this reason. It should be noted that when staff phone back to pick up answer phone messages, these will be audible to anyone in the vicinity of the answer phone.

6.11 Message Books

Where message books are used as an alternative to answer phones and contain names, addresses and other personal / sensitive details, these must be locked away when the office or area is not staffed.

6.12 Bring Forward Systems

Paper based information such as bring forward systems or other notes / messages left in work trays must be locked away when the office or area is not staffed.

6.13 Clear Desk

All staff should ensure they keep their desk clear of personal confidential data/ commercially sensitive information when it is unattended.

7. Duties/ Responsibilities

7.1 Individual Staff Responsibilities

The ICB, Directors, Managers and staff are responsible for establishing, maintaining and supporting an approach to Safe Haven management, in all areas of their responsibility. They should comply with the ICB's Safe Haven Policy and Procedures and ensure effective Safe Haven management mechanisms are implemented in accordance with these. Some members of staff and Committees have specialist functions in relation to Safe Havens as described below:

7.2 Chief Executive Officer

The Chief Executive Officer has overall responsibility for the ICBs' security and confidentiality management and ensuring that this operates effectively. The operational responsibility for Safe Havens is then delegated to the Caldicott Guardian and Senior Information Risk Officer.

7.3 Caldicott Guardian

The Caldicott Guardians have a particular role in overseeing the provision of internal advice in relation to Safe Havens, especially in relation to legislation and confidentiality.

7.4 Arden & GEM Commissioning Support Information Governance Team

The Arden & GEM CSU Information Governance team are the designated management advisors for the ICB and have day to day responsibility for the management of all aspects of Safe Havens. They are responsible for advising all staff throughout the organisation on issues relating to Safe Haven activities. They will oversee the investigation of adverse incidents in relation to Safe Havens. They must report all significant risks to the SIRO.

7.5 SIRO

The ICB's Senior Information Risk Owner (SIRO) provides regular reports to the ICB's Board in this regard. The Arden GEM CSU Information Governance team assists him/her with the performance of his/her duties. The SIRO has responsibility for reporting all significant risks to senior management where appropriate and ensuring that they are placed on the ICB's Risk Register.

7.6 All Staff

All staff have a responsibility to ensure they comply with the ICB's Safe Haven Policy and procedures. Failure to do so may lead to disciplinary and/or legal action. Advice can be sought by contacting the Arden GEM CSU Information Governance Team in relation to all Safe Haven issues such as consent, use and disclosure of patient information etc.

8. Training

8.1 Awareness Reviews

Awareness reviews will be carried out to ensure that staff maintain the appropriate level of skills to ensure that safe haven arrangements are used and maintained.

8.2 Induction Training

Induction training will be provided for new staff on Safe Haven arrangements within the ICB.

9. Monitoring Compliance and Effectiveness

9.1 The ICB will monitor the activity of individuals in relation to the use of personal confidential data/ commercially sensitive information on all ICB equipment both static and mobile.

The Arden GEM CSU Information Governance Team will carry out regular confidentiality audits to ensure compliance with this policy and report the outcomes of these audits to the Information Governance Steering Group.

The ICB's equipment will also be checked by the IT Shared Services Department as part of normal support operations.

10. Staff Compliance Statement

10.1 All staff are required to ensure they do not act in a way that places personal confidential data/commercially sensitive information at risk. A number of technical solutions are available to encrypt this type of information, and staff will be given training to use these where required. Where staff are regularly handling this type of information, they must ensure they are aware of and comply with the ICB's policies and procedures.

10.2 Where concern that local procedures are not consistent with this policy, staff must inform their line manager. Similarly, if staff become aware of potential breaches of this policy, they must report it to their line manager and complete an incident report form.

11. Legislation and NHS Guidance

Data Protection Act 2018

12. Associated Policies

- Confidentiality and Information Sharing Policy.
- Data Protection Policy.
- Email Usage Policy.
- Information Governance Policy.
- Information Security Policy.
- Removable Media Policy
- Mobile Device Policy.

Appendix A - Fax Cover Sheet

PRIVATE AND CONFIDENTIAL

This FAX is confidential and is intended only for the person to whom it is addressed. If you have received this FAX in error, please immediately notify the sender by telephone and return the message by post. If the reader of this FAX is not the intended recipient, you are hereby notified that any distribution or copying of this message is strictly prohibited.

To .....

From .....

Contact Number .....

Date .....

Fax Number .....

Number of Pages (including front sheet) .....

Message:

Appendix B - Safe Haven Fax Procedures

Guidance for sharing personal information by FAX

This is an agreed set of administrative and physical security procedures that have been designed to minimise the risks of breach of confidentiality or loss of information when sending or receiving faxing personal information via Fax

Do not fax personal or confidential information unless it is absolutely necessary. Where possible chose a safer method of sending information.

If it is absolutely necessary e.g. urgent clinical purposes, confidential information can be sent and received by fax if the following procedures are followed to reduce the information security risks.

Part 1 - Sending Information by Fax

1. Telephone the recipient of the fax (or their representative) to let them know that you are going to send the confidential information and confirm the number.

2. Verify the correct number by sending a cover sheet first and asking the recipient to acknowledge receipt of the fax by sending it back.

3. Always use a fax cover sheet which states who the information is for, who the information is from and your contact number. Mark it "**Private and Confidential"**

4. Include the following statement on the sheet:

Confidentiality notice
This message is private and confidential. If you have received this message in error, please notify us and destroy this facsimile.

1. Anonymise information wherever possible. If information cannot be anonymised, use only the minimum amount of patient/personal details necessary for the purpose. Where possible use only an identification number e.g. an NHS number

2. Double check to make sure you have dialled the correct the fax number before sending the cover sheet and information.

3. Request confirmation of receipt or request a report sheet to confirm that the transmission was successful.

4. If you send information to a fax number on a regular basis, complete this process by programming the number into the fax directory. This establishes the link as a "Safe Haven".

5. If you are faxing to a known Safe-Haven, you do not need to complete these procedures if (a) you have already verified the number and programmed into your directory and, (b) you use a fax cover sheet.

6. Pre-programmed numbers should be checked periodically to ensure they remain valid or following office relocations, departmental moves or any other reorganisation.

7. Information faxed in error to the wrong person must be reported as an incident

Part 2 - Receiving Confidential faxes

1. Each department should have a least one designated safe haven contact point on which to receive confidential information.

2. Make use of the security features on the fax machine, e.g. passwords, programmed directories etc.

3. A safe haven fax machine should be situated in a secure environment away from the public.

4. Staff responsible for the fax machine should participate with other departments or organisations in verifying a safe haven link by responding to requests from the sender to confirm receipt etc.

5. Confidential faxes should be removed upon receipt. The documentation should be placed inside an envelope to await collection by the addressee.

6. Where possible, safe haven fax machines should be turned off out of office hours.

Appendix C - Safe Haven Post
Guidance for sharing personal information by POST

9.1 Confidential information should be transferred in a sealed envelope and addressed to a named individual, including within a department or organisation. They should be clearly. marked “Personal and Confidential - to be opened by the recipient only”.

9.2 Confidential information contained in written transfers should be limited to those details necessary in order for the recipient to carry out their role.

9.3 Written transfers containing personal or sensitive personal information beyond a standard letter, report or summary (e.g. copies of health records, bulk transfers) must be sent by a recorded / registered postal method or courier.

9.4 Original health records must only be sent by courier – never by mail.

Appendix D – Safe Haven Phone

Guidance for sharing personal information by PHONE.

If the use of a telephone is essential to convey sensitive information, then the following security protocols must be adhered to:

- Ensure that the enquirer has a legitimate right to have access to the information before information is given out and provide information only to the person who has requested it.
- Confirm the name, job title, department and organisation of the person requesting the information, ensuring that you are speaking to the correct person.
- Take a contact telephone number e.g. main switchboard number *(never a direct line or mobile telephone number if possible).*
- Ring back to confirm that person's identity.
- Confirm the reason for the request.

Appendix E - Safe Haven Transporting Personal Information

Guidance for TRANSPORTING personal information.

- Personal Confidential Data (PCD) should only be taken off site when necessary, or in accordance with local policy.
- Keep a log of what you are taking off site and why, and if applicable where and to whom you are taking it.
- Information must be transported in a sealed container.
- Never leave PCD unattended.
- Ensure the information is returned on site as soon as possible
- Record on the log that it has been returned.

Appendix F - Email Procedures

Procedure for using safe email for sharing personal confidential data.

1. Personal confidential data/commercially sensitive Information should only be shared using e-mail when necessary via secure e-mail methods.

2. The ICB support the use of generic nhs.net mailboxes. A generic nhs.net mailbox is not associated with one particular user. It is usually accessed by multiple staff members from the same team. All staff who have access to the generic mailbox are required to log into their own individual nhs.net mailbox before accessing the generic mailbox to be able to send emails 'on behalf' of the mailbox.

3. Secure email link within the ICB.

   An encrypted and secure email link has been created for the ICB. This means that:

3.1. Any exchange of emails, where the sender and all recipient email addresses end in ardengemcsu.nhs.uk or ICB.nhs.uk will be encrypted and secure and therefore suitable for the exchange of personal confidential data or corporate sensitive information.

3.2. A secondary benefit is that any email exchange between the following will also be encrypted and secure:

   ICB.nhs.uk and South Warwickshire NHS Foundation Trust

   or

   ICB.nhs.uk and Coventry and Warwickshire Partnership NHS Trust

4. If it is absolutely necessary to e-mail personal confidential data/commercially sensitive information via an unsecured e-mail method, the following must be applied:

   - The information must be put into a separate document and attached to the e-mail – do not put this type of information into the main body of the e-mail.

   - Before attaching the document to the e-mail, you must ensure it is encrypted to NHS.
   - approved standards.

   - The IT service desk can be contacted for advice on how to encrypt a document;

   - The password, which should consist of a combination of alphanumeric and special
   - characters, should be sent by separate means – preferably by telephone or text
   - message.

   - A delivery and read receipt for the e-mail should be requested.

Appendix G - Removable Media Procedures

Procedure for ensuring the safe transfer of Personal Confidential / Sensitive Data by removable media.

1. Removable media includes USB memory sticks, CD's, DVD's etc.,

2. Removable media poses two problems:
    - They are easily lost or stolen and as the information is not backed- up anywhere else, it will be permanently lost which may result in a breach of confidentiality.
    - Without the appropriate encryption software and password protection on the device, the information contained on it is easily accessible by anyone who may find it.

2. Memory sticks are very small, portable, mass storage devices which can extract huge amounts of data from the ICB's computer network and must be regarded as a potential threat to our information security. Only ICB issued encrypted memory sticks (with Safestick logos) will be allowed to be connected to the ICB's computer equipment. These devices will only be issued where there is a proven need for their use. The use of any other type of memory stick is not permitted.

Personal Confidential Data/commercially sensitive data should only be put on these devices in exceptional circumstances and should be securely deleted as soon as possible. Memory sticks must not be used as a permanent storage solution for this type of data. If there are locations where this type of data is needed but not accessible on the ICB's network, IT Shared Services should be contacted to seek an alternative solution.

Please ensure that any non-ICB staff who use our computer systems (e.g. temporary workers, contractors, etc.) are made aware of this policy.

3. Never leave removable media unattended.

Appendix H - Portable Devices Procedures

Procedure to ensure the secure use of portable devices for storing Personal Confidential / Sensitive Data

1. Portable devices include laptops, blackberries, PDA's (personal digital assistants), mobile phones etc.,

2. All NHS ICB issued laptops must be encrypted to NHS approved standards.

3. Portable media poses two problems:
    - They are easily lost or stolen and as the information is not backed-up anywhere else, it will be permanently lost which may result in a breach of confidentiality;
    - Without the appropriate encryption software and password protection on the device, the information contained on it is easily accessible by anyone who may find it;

4. 'Write' access to USB ports is restricted to devices on an approved 'white list'.

5. Please be aware that Personal Confidential Data (PCD) / commercially sensitive information must not be held on any devices you are currently using.

6. Never leave removable media unattended.

Appendix I - Computer Procedures Safe Haven

Guidance for Computers

1. Computers must have password protected screensavers activated or on shared computers, must be logged off, when unattended to prevent unauthorised access of the computer and prevent others viewing information visible on the screen. This is achieved by selecting Ctrl+Alt+Del or Windows + L keys on the keyboard.

2. Never share your password or make it visible to anyone else. All ICB computer systems have monitoring software installed and any actions taken whilst you are logged in will be your responsibility.

3. All ICB information should be saved on your department's shared drive as this is backed up daily.

4. **NEVER** save information to the C: drive. The C: drive is not backed up and information can be accessed by anyone using that computer.

5. Consideration must be taken about the position of your computer screen, it could allow members of the public/unauthorised people to see information they should not.

Appendix J - Paper Procedures

Procedure for ensuring confidentiality of paper-based information

Incoming Mail/Post Rooms
All incoming mail to your department must be received into a secure area/ locked post room.

Post Trays/Pigeonholes
Departments with post trays for incoming mail must be placed in a secure area.

Work in-trays
If work in-trays are used for personal/sensitive information, they must be located in a secure area or locked away when the area is not staffed.

Message Books
If messages containing names, contact details and more detailed information are written in a message book, this must be locked away when that area is not staffed / out of working hours.

Clear Desk
All desks should be kept clear of personal confidential data/commercially sensitive information, particularly in shared/open plan offices. All personal confidential data/commercially sensitive information must be locked away when away from your desk.

Bring Forward Systems
If you operate a paper-based bring forward system, which contains personal confidential data/commercially sensitive information, you must secure it when the area is not staffed.

Appendix K - Systems Management Procedures

Procedure for ensuring confidentiality of Data and Data System Management

Data
Applies to data for 1 or more persons received, stored and used in any electronic format.

Default Access
In order to minimise the risk of breaches of legislation and mandatory codes of practice; the default access for all individuals will be as follows:

- No access to Personal Confidential Data unless approved by the Information Asset Owner (IAO);

Databases/Repositories
Each database or repository holding data must be held in a location and in a format, which supports secure managed access which includes:

- secure, password protected access to Personal Confidential Data on a need to know basis to individual users with IAO approval.
- prevention of individual users without IAO approval from having access to Personal Confidential Data
- logging of all access to Personal Confidential Data including:
    - data and time of access;
    - name of user;
    - summary of data accessed;

Raw Data
Raw data containing Personal Confidential Data as defined above which is received from providers or other sources and:

- uploaded to a database or repository following receipt; and/or
- retained following upload to a database or repository;

must be held securely and for the purpose which it is intended to be uploaded.

Raw data containing Personal Confidential Data which is received or generated electronically must be received and handled by authorised individual users with IAO approval.

Appendix L – Staff Details and Data Source Details

1. Staff Details	**2. Staff Line Manager Details**
Name: Job Title: Directorate: Department: Tel: Email:	Name: Job Title: Directorate: Department: Tel: Email:
3. Continuous	**4. Occasional**
Start Date: dd/mm/yyyy End Date: dd/mm/yyyy	Start Date: dd/mm/yyyy End Date: dd/mm/yyyy *End date must be no later than 12 months from the start date*
4. Name of Source Information Systems, Databases or Data Repositories	
5. Identifiable/Sensitive Data Field Required	
Name Y/N Address Y/N Postcode Y/N Date of Birth Y/N NHS Number Y/N Ethnic Category Y/N Local Patient ID Y/N Hospital Spell Number Y/N Patient Pathway Identifier Y/N	Patient Pathway Identifier Y/N SUS spell ID Y/N Unique Booking Ref Y/N Social Services Client ID Y/N Date of Death Y/N National Insurance Number Y/N Bank Details Y/N Driving Licence Number Y/N Employment Record Y/N

6. Information Asset Owner (IAO) (responsible for giving access)

Name:

Job Title:

Directorate:

Tel:

Email:

7. Who else will have access to the data?

I will ensure that where **Personal Confidential Data (PCD)** *or information is made available or transmitted onwards through reports and analysis to other users, the appropriate IAO approval is secured for each data disclosure. (I will not give other users access to personal confidential data).*

8. How will the service users be contacted?

This is a secondary use of data and service users will not be contacted – consent is assumed.

9. Where will the Personal Confidential Data (PCD) be stored?

Unless approved by the IAO, I will ensure that Personal Confidential Data (PCD) is stored only on workstations, laptops, servers, portable devices which are the property of or directly managed by the NHS ICB and which are password protected and/or encrypted and which comply with ICB data security policies. Files holding PCD and their locations will be fully password protected to prevent non- approved users from accessing the data without intervention or knowledge.

Appendix M – Quality and Equality Impact Assessment

Quality and Equality Impact Assessment

The following assessment screening tool will require judgement against all listed areas of risk in relation to quality. Each proposal will need to be assessed whether it will impact adversely on patients / staff / organisations.

Insert your assessment as positive (P), negative (N) or neutral (N/A) for each area.

Record your reasons for arriving at that conclusion in the comment's column. If the assessment is negative, you must also calculate the score for the impact and likelihood and multiply the two to provide the overall risk score. Insert the total in the appropriate box.

Quality Impact Assessment

Scheme Title:	Data Protection and Confidentiality Policy		
Project Lead:	Laura Whiteley, Governance and Corporate Affairs Manager	**Senior Responsible Officer:**	Andy Wilkins, Director of Corporate Governance
		Quality Sign Off:	n/a – policy does not require quality review
Intended impact of scheme:	This policy outlines and ensures that patient confidentiality is maintained within all areas of NHS Coventry and Warwickshire Integrated Care Board ('the ICB'). Where there is a need to transfer, transport, distribute or access information remotely staff must ensure that patient of staff confidentiality is not breached.		
How will it be achieved:	Through the process detailed in this document.		

Name of person completing assessment:	Laura Whiteley
Position:	Governance and Corporate Affairs Manager
Date of Assessment:	28/10/2024

Quality Review by:	Matt Hopkins
Position:	**Governance and Corporate Affairs Officer**

Date of Review:	29/10/2024

High level Quality and Equality Questions

The risk rating is only to be done for the potential negative outcomes. We are looking to assess the likelihood of the negative outcome occurring and the level of negative impact. We are also seeking detail of mitigation actions that may help reduce this likelihood and potential impact.

AREA OF ASSESSMENT		OUTCOME ASSESSMENT (Please tick one)			Evidence/Comments for answers	Risk rating (For negative outcomes)			Mitigating actions
		Positive	Negative	Neutral		Risk impact (I)	Risk likelihood (L)	Risk Score (IxL)	
Duty of Quality Could the scheme impact positively or negatively on any of the following:	Effectiveness – clinical outcome			**N/A**	Effective process ensures the organisation is sighted on and can address issues as a result of complaints and improve the quality of care and patient experience				
	Patient experience			**N/A**	"				
	Patient safety			**N/A**	"				
	Parity of esteem			**N/A**	"				
	Safeguarding children or adults			**N/A**	"				
NHS Outcomes Framework Could the scheme impact positively or negatively on the delivery of the five domains:	Enhancing quality of life			**N/A**	"				
	Ensuring people have a positive experience of care			**N/A**	"				
	Preventing people from dying prematurely			**N/A**	"				
	Helping people recover from episodes of ill health or following injury			**N/A**					
	Treating and caring for people in a safe environment and protecting them from avoidable harm			**N/A**					
Patient services Could the proposal impact positively or negatively on any of the following:	A modern model of integrated care, with key focus on multiple long-term conditions and clinical risk factors			**N/A**					

	Access to the highest quality urgent and emergency care			**N/A**					
	Convenient access for everyone			**N/A**					
	Ensuring that citizens are fully included in all aspects of service design and change			**N/A**					
	Patient Choice			**N/A**					
	Patients are fully empowered in their own care			**N/A**					
	Wider primary care, provided at scale			**N/A**					
Access Could the proposal impact positively or negatively on any of the following:	Patient choice			**N/A**					
	Access			**N/A**					
	Integration			**N/A**					
Compliance with NHS Constitution	Quality of care and environment			**N/A**					
	Nationally approved treatment/drugs			**N/A**					
	Respect, consent and confidentiality			**N/A**					
	Informed choice and involvement			**N/A**					
	Complain and redress			**N/A**					

Equality Impact Assessment

Project / Policy Details

What is the aim of the project / policy?
This policy is to ensure that patient confidentiality is maintained within all areas of NHS Coventry and Warwickshire Integrated Care Board ('the ICB'). Where there is a need to transfer, transport, distribute or access information remotely staff must ensure that patient of staff confidentiality is not breached.

Who will be affected by this work? e.g staff, patients, service users, partner organisations etc.
All staff and data subjects

Is a full Equality Analysis Required for this project?			
Yes	Proceed to complete this form.	No	Explain why further equality analysis is not required.
If no, explain below why further equality analysis is not required. For example, the decision concerned may not have been made by the ICB or it is very clear that it will not have any impact on patients or staff.			
N/A			

Equality Analysis Form

1. Evidence used
What evidence have you identified and considered? This can include national research, surveys, reports, NICE guidelines, focus groups, pilot activity evaluations, clinical experts or working groups, JSNA or other equality analyses.
N/A

2. Impact and Evidence:
In the following boxes detail the findings and impact identified (positive or negative) within the research detailed above; this should also include any identified health inequalities which exist in relation to this work.
Age: A person belonging to a particular age (e.g., 32-year old's) or a range of ages (e.g., 18-30 year old's)
This policy applies to ICB staff of all ages. There is no evidence or informal intelligence to suggest that differing ages would cause anyone to be disadvantaged more than another in applying this policy
Disability: A person has a disability if he/she has a physical, hearing, visual or mental impairment, which has a substantial and long-term adverse effect on that person's ability to carry out normal day-to-day activities
Describe disability related impact and evidence. This can include attitudinal, physical, communication and social barriers as well as mental health/ learning disabilities, cognitive impairments:

This policy applies to all staff and there is no evidence or informal intelligence to suggest that anyone with a disability would be disadvantaged more than someone who didn't have a disability.
Gender reassignment (including transgender): Where a person has proposed, started or completed a process to change his or her sex.
Describe any impact and evidence on transgender people. This can include issues such as privacy of data and harassment. N/A
Marriage and civil partnership: A person who is married or in a civil partnership.
Describe any impact and evidence in relation to marriage and civil partnership. This can include working arrangements, part-time working, and caring responsibilities: N/A
Pregnancy and maternity: A person is protected against discrimination on the grounds of pregnancy and maternity. With regard to employment, the person is protected during the period of her pregnancy and any statutory maternity leave to which she is entitled. Also, it is unlawful to discriminate against women breastfeeding in a public place.
Describe any impact and evidence on pregnancy and maternity. This can include working arrangements, part-time working, and caring responsibilities: N/A
Race: A group of people defined by their race, colour, and nationality (including citizenship) ethnic or national origins.
This policy applies to all races and there is no evidence or informal intelligence to suggest that any race will be disadvantaged more than the other in applying this policy.
Religion or belief: A group of people defined by their religious and philosophical beliefs including lack of belief (e.g., atheism). Generally, a belief should affect an individual's life choices or the way in which they live.
This policy applies to all staff irrespective of their religion/religious beliefs and there is no evidence or informal intelligence to suggest that people holding differing religious beliefs would be disadvantaged more than another in applying this policy.
Gender:

This policy applies to both genders and there is no evidence or informal intelligence to suggest that either will be disadvantaged more than the other in applying this policy.

Sexual orientation: Whether a person feels generally attracted to people of the same gender, people of a different gender, or to more than one gender (whether someone is heterosexual, lesbian, gay or bisexual).

There is no evidence or informal intelligence to suggest that people of differing sexual orientation will be disadvantaged more than another in applying this policy

Carers: A person who cares, unpaid, for a friend or family member who due to illness, disability, a mental health problem or an addiction cannot cope without their support

This policy applies to ICB staff irrespective of carer responsibilities. There is no evidence or informal intelligence to suggest that people with carer responsibilities would be disadvantaged more than someone who didn't

Other disadvantaged groups:

Describe any impact and evidence on groups experiencing disadvantage and barriers to access and outcomes. This can include lower socio-economic status, resident status (migrants, asylum seekers), homeless, looked after children, single parent households, victims of domestic abuse, victims of drugs / alcohol abuse: (This list is not exhaustive)

N/A

3. Human Rights

FREDA Principles / Human Rights	Question	Response
Fairness – Fair and equal access to services	How will this respect a person's entitlement to access this service?	N/A
Respect – right to have private and family life respected	How will the person's right to respect for private and family life, confidentiality and consent be upheld?	N/A
Equality – right not to be discriminated against based on your protected characteristics	How will this process ensure that people are not discriminated against	N/A

	and have their needs met and identified?	
Dignity – the right not to be treated in a degrading way	How will you ensure that individuals are not being treated in an inhuman or degrading way?	N/A
Autonomy – right to respect for private & family life; being able to make informed decisions and choices	How will individuals have the opportunity to be involved in discussions and decisions about their own healthcare?	N/A
Right to **Life**	Will or could it affect someone's right to life? How?	N/A
Right to **Liberty**	Will or could someone be deprived of their liberty? How?	N/A

4. Engagement, Involvement and Consultation		
If relevant, please state what engagement activity has been undertaken and the date and with which protected groups:		
Engagement Activity	**Protected Characteristic/ Group/ Community**	**Date**
N/A		
For each engagement activity, please state the key feedback and how this will shape policy / service decisions (E.g., patient told us …. So we will ….):		
N/A		

5. Mitigations and Changes
Please give an outline of what you are going to do, based on the gaps, challenges and opportunities you have identified in the summary of analysis section. This might include action(s) to mitigate against any actual or potential adverse impacts, reduce health inequalities, or promote social value. Identify the **recommendations** and any **changes** to the proposal arising from the equality analysis.
N/A

6. How will you measure how the proposal impacts health inequalities?
e.g. Patients with a learning disability were accessing cancer screening in substantially lower numbers than other patients. By revising the pathway, the ICB is able to show increased take up from this group, this is a positive impact on health inequalities. You can also detail how and when the service will be monitored and what key equality performance indicators or reporting requirements will be included within the contract.
N/A

7. Is further work required to complete this assessment?			
Please state what work is required and to what section. e.g., additional consultation or engagement is required to fully understand the impact on a particular protected group (e.g., disability).			
Work needed	**Section**	**When**	**Date completed**
N/A			

8. Sign off		
The Equality Analysis will need to go through a process of **quality assurance** by a Senior Manager within the department responsible for the service concerned before being submitted to the Policy, Procedure and Strategy Assurance Group for approval. Committee approval of the policy / project can only be sought once approval has been received from the Policy, Procedure and Strategy Assurance Group.		
Requirement	**Name**	**Date**
Senior Manager Sign off	Laura Whiteley	24/10/2024
Which committee will be considering the findings and signing off the EA?	Audit Committee	12/11/2024
Approved by the Policy Procedure and Strategy Assurance Group.	PAG	29/10/2024