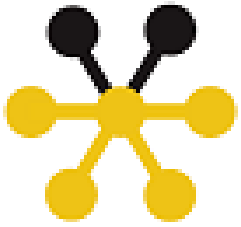
Confidentiality Policy



Kernow Health

Version: 5.0
Date: July 2024

Policy Name	Confidentiality Policy
Version	5.0
Name of responsible (ratifying) committee	Executives
Date Agreed & Ratified by Executive:	27/08/2024
Responsible Policy Lead	Director of Integrated Community Care Services
Document Manager (job title)	Business & Quality Assurance Manager
Date issued	September 2024
Review date	June 2027
Electronic location	Sharepoint
Related Policy/Procedure Documents	Complaints Policy Information Governance and Data Protection Policy Subject Access Requests Guidance Data Quality Policy I.T. Security Policy Mobile I.T. Security Policy Patient Safety and Incident Reporting Policy Duty of Candour Policy Safeguarding Policy
In the case of hard copies of this policy the content can only be assured to be accurate on the date of issue marked on the document. For assurance that the most up to date policy is being used, staff should refer to the version held on the intranet.	

Amendment History

Version	Status	Date	Reason for Change	Authorised
1.0	Final	November 2015	New	
2.0	Final	April 2017	Review	L Manolchev
2.1	Final	March 2018	Update to include GDPR	L Manolchev
3.0	Final	May 2019	Amalgamate Cwll111 and KHCIC policy	L Manolchev
4.0	Final	May 2020	Review	L Manolchev

CONFIDENTIALITY POLICY

Contents

1. INTRODUCTION 2
2. PURPOSE 2
3. SCOPE 2
4. DEFINITIONS 2
5. ROLES & RESPONSIBILITIES 2
6. STANDARDS AND PRACTICE 3
7. MONITORING & COMPLIANCE 7
8. DISSEMINATION & IMPLEMENTATION 7
9. EQUALITY IMPACT ASSESSMENT 7

Appendix 1 - Initial Equality Impact Assessment Form 8

1. INTRODUCTION

1.1. Kernow Health CIC (KHCIC) is committed to ensuring all information it holds is kept safe, secure and confidential. This includes all information relating to patients, the organisation's financial and business records, and any staff information.

1.2. KHCIC commits itself to working within the Data Protection Act 2018 which encompasses the General Data Protection Regulations (GDPR), Caldicott Principles and adheres to the Confidentiality: NHS Codes of Practice 2003.

1.3. All staff are obliged to keep any personal identifiable information strictly confidential e.g. patient and employee records. It should be noted that staff also come into contact with non-person identifiable information which should also be treated with the same degree of care e.g. business "in confidence" information.

2. PURPOSE

2.1. The purpose of this policy is to ensure that staff are aware of their responsibilities in relation to keeping information confidential. This policy will set out the framework for which staff will need to work within to ensure that information is kept safe, that there are appropriate access levels applied and where information needs to be shared, how this can be achieved safely and securely.

3. SCOPE

3.1. This policy applies to all staff whether permanent or temporary, and contractors working on behalf of KHCIC.

3.2. Any information held by the organisation, whether patient, staff or business related is included in this policy.

4. DEFINITIONS

4.1. **Confidential Information**

Confidential Information can be anything that relates to patients, staff, their family or friends, in whatever format it is stored, such as paper, electronic files and photographs. This includes any confidential corporate information.

4.2. **Personal Identifiable Data (PID)**

Personal Identifiable Data (PID) is anything that contains the means to identify a person, for example, name, address, postcode, date of birth, NHS number, National Insurance Number. This can also include visual images, such as a photograph, which is sufficient to identify individuals.

4.3. **Sensitive Information**

Certain categories of information are legally defined as particularly sensitive and should be most carefully protected by additional requirements as stated in legislation e.g. health information. All information should be considered sensitive e.g. name and address.

5. ROLES & RESPONSIBILITIES

5.1. **KHCIC Board**

It is the responsibility of the Board to have a strategic overview of all work and policies undertaken to ensure that it meets all legal, statutory and good practice guidance requirements.

5.2. **Caldicott Guardian**

The Caldicott Guardian is responsible for ensuring implementation of the Caldicott Principles with respect to patient-identifiable information.

5.3. **Information Governance Lead**
The Information Governance Lead is responsible for ensuring that there are policies and procedures in place for the collection and sharing of information.

5.4. **Data Protection Officer**
The Data Protection Officer is responsible for monitoring compliance with legislation, taking any actions to mitigate against breaches of confidentiality and to act as lead investigator where required on data breaches. The Data Protection Officer will provide advice and guidance to ensure that the organisation continues to meet it duties and responsibilities within legislative requirements.

5.5. **Information Governance Steering Group**
The Information Governance Steering Group (IGSG) is responsible for overseeing, developing and implementing information governance policies. The IGSG will continue to complete and submit the Data Security and Protection (DSP) Toolkit on an annual basis.

5.6. **Managers**
All managers have a responsibility to ensure that their staff have read policies relating to information governance and data protection and to make staff aware of their responsibilities in keeping information safe and secure.

5.7. **All Staff**
All staff have a responsibility to keep confidential information safe and secure, and to not disclose information where it is not appropriate to do so. If staff are asked to disclose information, advice should be sought from the appropriate manager. All staff are expected to complete their Information Governance Training on an annual basis. Staff contracts of employment include a commitment to confidentiality. Any breaches of confidentiality could be regarded as gross misconduct and may result in disciplinary action.

6. STANDARDS AND PRACTICE

6.1. All information held by KHCIC will be treated as confidential information and will not be shared outside of the organisation, unless it has been consented to or there is a requirement within a contract that requires us to. This includes patient information, HR records, and financial/business records. However, there may be occasions where information may need to be shared without consent in order to protect an individual. Such occasions may be where there are safeguarding concerns.

6.2. **Principles of Patient Confidentiality**
All staff must ensure that the following principles are adhered to:

- Person-identifiable or confidential information must be effectively protected against improper disclosure when it is received, stored, transmitted or disposed of
- Access to person-identifiable or confidential information must be on a need- to- know basis
- Disclosure of person-identifiable or confidential information must be limited to that purpose for which it is required
- Recipients of disclosed information must respect that it is given to them in confidence
- If the decision is taken to disclose information, that decision must be justified and documented
- Any concerns about disclosure of information must be discussed with either the staff member's Line Manager or the Information Governance Lead

Kernow Health CIC is responsible for protecting all the information it holds and must always be able to justify any decision to share information.

Person-identifiable information, wherever possible, must be anonymised by removing as many identifiers as possible whilst not unduly compromising the utility of the data.

Access to rooms and offices where person-identifiable or confidential information is stored must be controlled; filing cabinets/cupboards must be locked, with the key(s) kept in a secure place e.g. key safe.

All staff must clear their desks at the end of each day, particularly any person- identifiable or confidential information which must be put away in lockable filing cabinets.

Unwanted printouts containing person-identifiable or confidential information must be shredded.

6.3. **Requests for Information & Disclosure**

If disclosure of information has been requested, which may have personal consequences for the patient or staff involved, consent must be obtained. If the person withholds consent, or is unable to give consent disclosure may only happen where:

- It can be justified in the public interest (usually where disclosure is essential to protect the patient or someone else from the risk of significant harm)
- It is required by law or by order of a court
- There is an issue of child protection. You must act at all times in accordance with national and local policies.

Everyone has the right to expect that their information will be held in confidence. Confidentiality is central to trust between health providers and patients. The following must be applied:

- Never give out information on patients or staff to persons who do not need to know
- All requests for identifiable information should be based on a justified need. Some requests may also need to be agreed by the Caldicott Guardian or Information Governance Lead
- The transfer of information may be agreed under an Information Sharing Protocol or Agreement.

If it is uncertain whether the information can be disclosed, staff must seek advice from the relevant Line Manager or from the Information Governance.

If a request for information is made by telephone, staff must:

- Always check the identity of the caller and whether they are entitled to the information they are requesting
- Take a number, verify it independently and call back if necessary
- Consult the relevant manager, it is safer not to disclose than to disclose inappropriately.

Information requests from the police should always be referred to the appropriate manager to ensure national guidance is checked prior to disclosing information.

Under no circumstances should any information be given to the media. Media may not always make their status apparent, and if there are any concerns about the validity of a caller or visitor a more senior member of staff must be notified.

6.4. **Sharing Information**

6.4.1. Use of Internal and External Post

Best practice with regard to confidentiality requires that all correspondence containing personal information should always be addressed to a named recipient. This means personal information/data should be addressed to a person, a post

holder, but not to a department, a unit or an organisation. In cases where the mail is for a team it should be addressed to an agreed post holder or team leader.

Where possible, window envelopes should always be used. Care should be taken to ensure only the recipient and address is displayed in the window. If it is not possible to use a window envelope, for example where the recipient has been copied into the letter, specific attention must be paid to ensure that the envelope is correctly addressed and only the intended letter inserted.

The envelope must be labelled above the addressee details, with “Private and Confidential“.

Electronic media should always be protected. No electronic media, such as CDs, should be sent unencrypted. Before electronic media is sent, permission must be sought from the Information Governance Lead and the IT Team.

6.4.2. Emailing confidential information

Special care should be taken to ensure that where information is to be sent via email, this is sent only to recipients who have a “need to know “. Staff must always double check they are sending the mail to the correct person/s. All staff have a personal responsibility to ensure that all personal or sensitive information is sent and received in a secure and confidential manner. It is the sender’s responsibility to ensure that all the information being sent is accurate and that the recipient’s details are correct. Any incidents regarding a breach of this should be reported immediately as an incident via the Incident Reporting Form (https://forms.office.com/e/2BH3k80RXu).

Staff must include the phrase “Patient Information” in the subject field; this ensures that the message is clearly identifiable to the authorised addressee.

If sending an email containing sensitive information outside of KHCIC staff must first establish if it is legal to do so. Sharing information without consent could be a breach of the Data Protection Act 2018. If in doubt, staff should seek advice.

Person identifiers should be removed wherever possible, and only the minimum necessary information sent, this may be considered to be the NHS number. This in itself can pose problems as the wrong number may be typed.

External transfers should only take place to persons with access to a secure email address. Under no circumstances whatsoever should any type of patient identifiable information, sensitive or confidential information about any person be emailed to persons who only have private email addresses, such as hotmail.com or gmail.com accounts without staff first speaking to their line manager. Due to its insecure nature any information transmitted over the Internet should be considered to be in the public domain.

6.5. Working Remotely

There may be occasions where KHCIC staff will need to work remotely. This includes staff who are working from home, working outside of Cornwall or are working from another location delivering services where access to the KHCIC domain is required. In these circumstances:

- Staff can only use equipment that has been provided by KHCIC due to the security and encryption already set up on these devices. Where staff work in other bases to deliver KHCIC, such as community hospitals, staff are only allowed to use the I.T. equipment available to them for that purpose in that base.

- Staff are not to email any of their work to their personal email addresses to work on from home or save any work on their personal computers.
- There may be occasions when staff need to take patient information home. If this is required, staff should seek approval from their Line Manager in the first instance. If it is deemed appropriate, no patient information is to be left in the staff member's car but to be taken into the staff member's home and kept securely.
- All passwords are to be kept confidential and not to be shared with wider members of the organisation.

Please refer to the Mobile I.T. Security Policy for more information.

6.6. **Carelessness**

All staff have a legal duty of confidentiality to keep person-identifiable or confidential information private and not to divulge information accidentally.

Staff may be held personally liable for a breach of confidence. The following steps will help staff to keep personal and confidential information safe. Staff must:

- Not talk about patients or the organisation's business in public places or where conversations may be overheard
- Not talk about patients or the organisation's business on social media
- Not leave any confidential information out unattended
- Ensure that the public cannot see computer screens, or other displays of information
- Ensure the computer is locked (Ctrl + Alt + Delete, or Windows key + L) when leaving the desk
- Ensure any portable forms of data are locked in a drawer/filing cabinet
- Not disclose passwords to anyone.

6.7. **Abuse of Privilege**

It is strictly forbidden for employees to knowingly browse, search for or look at any personal or confidential 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 Data Protection Act 2018.

When dealing with person-identifiable or 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 KHCIC.

If staff have concerns about this issue they should discuss it with their Line Manager in the first instance or Governance Team.

6.8. **Storage and Disposal of Confidential Information**

Paper-based confidential information should always be kept locked away and preferably in a room that is locked when unattended, particularly if the room is to be un-occupied for a long period of time.

Disposal of confidential information should always be put in the shredder. Prior to destroying confidential information, KHCIC's Record Retention & Destruction Policy should be checked where guidance is provided on retention period for certain categories of information, particularly patient identifiable information. This does not apply to voided prescriptions which must be returned to Cudmore House to be recorded and then destroyed.

6.9. **Confidentiality of Passwords**

Login details and passwords provided to employees must be regarded as confidential and they must not be communicated to anyone. All staff must have regard to the following principles:

- Never write passwords down
- Password should not relate to the employee or system being accessed

No employee should attempt to bypass or defeat the security systems or attempt to obtain to use passwords issued to other employees. Any breach of security should be immediately reported to the Governance Team, which could lead to disciplinary action.

7. MONITORING & COMPLIANCE

7.1. This policy will be monitored through:

- Monitoring of breaches in confidentiality
- Regular review of training compliance relating to information governance and confidentiality
- Use of communications to remind staff of the importance of keeping information confidential and safe

8. DISSEMINATION & IMPLEMENTATION

8.1. A copy of the policy will be stored electronically on the shared drive and on the staff pages on the KHCIC website.

8.2. Staff will be made aware of this policy through emails, newsletters, employee forums and bulletins

9. EQUALITY IMPACT ASSESSMENT

9.1. An initial equality impact assessment has been carried out and there have been no differential impacts identified on any of the protected characteristics. Therefore, a full equality impact assessment is not required.

Appendix 1 - Initial Equality Impact Assessment Form

Name of strategy/ policy/ proposal/ service function to be assessed:	Confidentiality Policy
Service Area:	Corporate
Is this a new or existing strategy/ policy/ proposal/ service?	Existing
Name of individual(s) completing assessment:	Laura Manolchev
Date:	29/07/2024

1) Policy aim *Who is the strategy/ policy/ proposal/ service function aimed at?*	The aim of the policy is to ensure that all staff understand their responsibilities in keeping personal and sensitive information confidential. This will also provide assurance to the public and to patients that their information is being kept safe and secure.				
2) Policy objectives	• To ensure information is kept confidential • To provide guidance as to when information can be divulged • To ensure staff are aware that only approved I.T. equipment can be used				
3) Policy – Intended Outcomes	• Ensure confidentiality of information and have process in place where it is appropriate to divulge information e.g. safeguarding				
4) How will you measure the outcome?	• Monitoring number of data breaches • Use of staff bulletins to inform staff • Training compliance				
5) Who is intended to benefit from the strategy/ policy/ proposal/ service function?	• Patients will benefit as they will know that any information about them is being kept confidential • Staff will benefit as they will have guidance as to how to keep information secure • The organisation will benefit as it will meet its responsibilities in protecting information as per legislation and regulations.				
6a) Who did you consult with?	Workforce	Patients	Local Groups	Ext. Organisations	Other
6b) Please identify the groups who have been consulted about this strategy/ policy/ proposal/ service function? *Please records specific names of groups*	This is a review of an existing policy. There have been no fundamental changes to the policy.				
7) What was the outcome of the consultation?	Not applicable.				

8) The Impact				
Are there any concerns that the function being assessed **could** have differential impact on:				
Equality Strands:	Yes	No	Unsure	Rationale for Assessment/ Existing Evidence
Age		✓		
Sex (male, female, trans-gender/ gender reassignment)		✓		
Race/ Ethnic Communities/ Groups		✓		
Disability – Learning disability, physical impairment, sensory impairment, mental health conditions and some long term health conditions		✓		
Religion/ Other Beliefs		✓		
Marriage and Civil Partnerships		✓		
Pregnancy & Maternity		✓		
Sexual Orientation – Bisexual, Gay, Heterosexual, Lesbian		✓		

You will need to continue to a full Equality Impact Assessment if the following have been highlighted:

- You have ticked "Yes" in any column above and
- No consultation or evidence of there being consultation- this excludes any *policies* which have been identified as not requiring consultation**. or**
- Major this relates to service redesign or development

9) Please indicate if a full equality analysis is recommended	**Yes**		**No**	✓

10) If you are not recommending a Full Impact Assessment please explain why.
There have been no differential impacts on any of the protected characteristics and therefore a full equality impact assessment is not required.

Sign Off	
Group/ Committee sign off:	Quality Assurance & Audit Committee
Date signed off:	27th August 2024