ECCH Confidentiality Policy

Version 10: November 2021

First Issued: July 2012
Review date: November 2023

DOCUMENT CONTROL SHEET

Name of Document:	ECCH Confidentiality Policy
Version:	10
File Location / Document Name:	Policy repository/Confidentiality policy
Date Of This Version:	November 2021
Produced By (Designation):	Information Governance Lead
Reviewed By:	Data Protection Officer
Synopsis And Outcomes Of Consultation Undertaken:	Amendments from recommendations made by Information Governance Group
Synopsis And Outcomes Of Equality and Diversity Impact Assessment:	No adaptations required as document has no direct impact on specific groups listed in the Impact Assessment.
Ratified By (Committee):-	IG & Caldicott Group Virtually
Date Ratified:	29/11/2021
Distribute To:	ECCHO Intranet
Date Due For Review:	November 2023
Enquiries To:	Data Protection Officer

Version Control

Version Date	Version No.	Author/ Reviewer	Comments
10 July 2012	3	J. George	Amend company details
20 November 2012	4	J Holt	Amend some role designations and key documents
01 September 2016	5	C Coleman	General review and update of document
24 October 2016	6	A Thornton	Review and update
11 November 2016	7	IG Group	Updated section 3.5 to include looking at own records
18 December 2017	7.1	A Thornton	Review and update
2 October 2019	8		Remove instructions regarding faxing on page 14, section 4.2
April 2021	9	H Lewis -DPO	Updated Caldicott Principles (8th), removed reference to 1998 DPA
November 2021	10	H Lewis -DPO	Full review and update of contents including and not limited to transfer to new template, references to emailing updated and addition of definitions and references. Updated appendices.

EQUALITY AND DIVERSITY IMPACT ASSESSMENT

Impact Assessments must be conducted for:

- ❑ **All ECCH policies, procedures, protocols and guidelines (clinical and non-clinical)**
- ❑ **Service developments**
- ❑ **Estates and facilities developments**

Name of Policy / Procedure / Service	**Confidentiality Policy**
Manager Leading the Assessment	**Information Governance Lead**
Date of Assessment	**17/11/2021**

STAGE ONE – INITIAL ASSESSMENT

Q1. Is this a new or existing policy / procedure / service?

☐ New

x Existing

Q2. Who is the policy / procedure / service aimed at?

☐ Patients

x Staff

☐ Visitors

Q3. Could the policy/procedure/service affect different groups (age, disability, sex, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sexual orientation) adversely?

☐ Yes

x No

If the answer to this question is NO please sign the form as the assessment is complete, if YES, proceed to Stage Two.

Analysis and Decision-Making

Using all of the information recorded above, please show below those groups for whom an adverse impact has been identified.

	Adverse Impact Identified?
Age	No
Disability	No
Gender reassignment	No
Marriage and civil partnership,	No
Pregnancy and maternity	No
Race	No
Religion or Belief	No
Sex	No
Sexual Orientation	No

- Can this adverse impact be justified?
- Can the policy/procedure be changed to remove the adverse impact?

If your assessment is likely to have an adverse impact, is there an alternative way of achieving the organisation's aim, objective or outcome N/A
What changes, if any, need to be made in order to minimise unjustifiable adverse impact? N/A

Contents

*(For quick access to a specific heading - **press CTRL and click your mouse** to follow the link for the below options)*

1. INTRODUCTION

1.1. The policies, procedures, protocols, and guidance notes produced by East Coast Community Healthcare (ECCH) provide the means by which the organisation conveys its intentions and the manner in which things should be done. Such documents also have a particular significance in terms of their legality, which have a bearing on the need to ensure that they are accessible, relevant, timely, and, where appropriate, are evidence-based.

1.2. This policy and procedure sets out the minimum standards that documentation should meet as a means of maintaining the organisation's governance, image and integrity whilst upholding the aims of its integrated governance strategy.

1.3. The control of policies and procedures is essential as a key means of ensuring standardisation in the provision of safe care across the organisation and the successful minimisation of risk.

2. PURPOSE

2.1. It is the policy of East Coast Community Healthcare CIC (ECCH) to ensure the security and confidentiality of information relating to or held by the organisation. It is also policy to comply with all relevant legislation and regulation relating to the collection, storage, sharing and disposal of information including, but not restricted to that detailed in paragraph 2.7 below.

2.2. This document details required practice for maintaining confidentiality for all person identifiable and/or business sensitive information: understanding of and compliance with these practices is required of all ECCH employees. For the purposes of this document the term "employee" is used as a convenience to refer to all those to whom this policy should apply. Whilst directed at ECCH staff it is also relevant to anyone working in and around ECCH and its premises to include contractors, agency & temporary staff, student, honorary and volunteer staff.

2.3. An Information Governance and Confidentiality clause exists in ECCH employment contracts. Managers should explain the statement attached at Appendix 2 to individuals working for ECCH who do not have a formal contract of employment and ask them to sign the declaration at Appendix 3.

2.4. All employees working for ECCH are bound by a statutory duty of confidence to protect personal information. This is a requirement established within The Data Protection Act 2018, General Data Protection Regulation (GDPR), Common Law, Article 8 of the Human Rights Act 1998 and the Confidentiality: NHS Code of Practice November 2003. In addition, for clinical and other professional staff it is contained within their own professional Code/s of Conduct (please see appendix 1), as well as all staff being required to undertake annual mandatory information governance training.

2.5. This means that employees are obliged to keep any person identifiable information strictly confidential e.g., patient and staff records. It should be noted that employees also come into contact with non-person identifiable information which should also be treated with the same degree of care e.g., business sensitive information such as waiting list data, consultant's workloads, and clinic lists etc.

2.6. The principle behind this policy is that no employee shall breach their legal duty of confidentiality, allow others to do so, or attempt to breach any of ECCHs systems or controls in order to do so.

2.7. This policy has been written to meet the requirements of the:

- The General Data Protection Regulation (GDPR) /UK GDPR
- Data Protection Act 2018
- Humans Rights Act 1998
- Computer Misuse Act 1990
- Copyright Designs and Patents Act 1988

2.8 This policy has been produced to protect employees by making them aware of the correct procedures so that they do not inadvertently breach any of these requirements. Unless an employee has taken all appropriate steps to safeguard confidential information and has followed the requirements of the codes of practice or conduct/legislation referred to in this policy they may be held to have acted negligently which may lead to disciplinary action being taken against them.

3. DEFINITIONS

3.1. The following definitions are intended to provide a brief explanation of the various terms used within this policy.

Duty of Confidentiality	A duty of confidentiality arises when information is obtained in circumstances where it is reasonable for a person confiding personal information to expect that it will be held in confidence by the recipient of the information.
Data Protection Act (DPA)	The Data Protection Act 2018 controls how your personal information is used by organisations, businesses or the government. The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).
General Data Protection Regulation (GDPR)	The General Data Protection Regulation 2016/679 is a regulation in EU law on data protection and privacy in the European Union and the European Economic Area.
UK GDPR	The GDPR is retained in domestic law as the UK GDPR, but the UK has the independence to keep the framework under review. The 'UK GDPR' sits alongside an amended version of the DPA 2018. The key principles, rights and obligations remain the same. However, there are implications for the rules on transfers of personal data between the UK and the EEA.
Caldicott Guardian	The Caldicott Guardian is senior person responsible for protecting the confidentiality of personal confidential data and information. The Caldicott Guardian plays a key role in ensuring that ECCH and partner organisations abide by the highest level of standards for handling personal information and personal identifiable information
Senior Information Risk Owner (SIRO)	The Senior Information Risk Owner (SIRO) acts on behalf of the Board. The SIRO owns the information risk and incident management framework, overall information risk approach and risk assessment processes, and is responsible for ensuring they are implemented consistently.
Data Protection Officer (DPO)	The Data Protection Officer is a legal role required by the GDPR. This person is responsible for overseeing the Information Governance (IG) Policy and Framework and the implementation of data protection and security

	measures to ensure compliance with the GDPR requirements; these measures should ultimately minimise the risk of breaches and uphold the protection of PII and special categories of data.
Person identifiable information	Person identifiable information relates to information about a person which would enable that person's identity to be established by one means or another.
Disclosure	This is the divulging or provision of access to data.

4. RESPONSIBILITIES

4.1. All employees are responsible for maintaining the confidentiality of information.

5. CONFIDENTIALITY OF INFORMATION

5.1. Confidential information can be anything that relates to patients and employees, their family or friends, however stored. For example, information may be held on paper, laptops, USB memory sticks, smart devices, digital cameras, tapes including film microfiche, audio cassettes, video etc., removable hard disks and drives, DVDs and CD ROMs, photographs or even heard by word of mouth.

5.2. It can take many different forms including medical notes, audits, employee records, occupational health records etc. It also includes any company e.g. ECCH and/or its subsidiaries – confidential information.

5.3. Person identifiable information relates to information about a person which would identify the individual. This could be explicit such as an unusual surname or isolated postcode or items of different information which if taken together could allow a person to be identified, All information that relates to an attribute of an individual should be considered as potentially capable of identifying them to a greater or lesser extent. Please note that even a visual image (e.g. photograph) is sufficient to identify an individual.

5.4. Certain categories of information are legally defined as particularly sensitive. Sensitive information can be broadly defined as that which if lost, misdirected or compromised could affect an individual or individuals. In the context of health: as well as containing person identifiable information such as name, date of birth, private address and home telephone number it is probable that appointments, illnesses, conditions, courses of treatment and lifestyle issues etc. will also be contained in information of this nature. In addition, members of Senior Management and Human Resources will hold sensitive information about staff for example payroll details and sickness notifications. For this type of information stringent security measures must be taken to ensure that a breach of confidentiality does not occur.

5.5. Financial and security information about an organisation is likely to be deemed "sensitive" if, when compromised or misdirected, it will affect the day to- day running of ECCH and/or discredit the services that it provides.

5.6. During duties of work employees should consider all information to be sensitive, even something as simple as a name and address. The same standards should be applied to all information employees come into contact with.

5.7. Employees and service users must understand how ECCH will use information about them. Achieving this understanding will therefore depend on giving the service user relevant information about the purposes of processing information and any disclosures.

5.8. The confidentiality statement in Appendix 4 should be provided to all service users where possible. Service users should be asked to confirm that they understand and agree the statement. The clinician responsible for giving care to the service user must discuss the uses of their information with them. Leaflets are useful for reinforcing information given to a person but are not in themselves sufficient. Any explanation should include as a minimum:

- That the main use of information will be to manage the service user's care and treatment, and that it is very important that ECCH has full and accurate information so that it can provide the best possible care within its available resources.

- That ECCH also uses service user information to check the quality of the care that they and other service users receive, to ensure that this is of the right standard. Everyone involved in the auditing process must follow the same strict rules on confidentiality.

- That employees work as part of a team and will share information about the service user with the team if it is necessary to provide the best possible care for them. If employees work with another agency then they should explain that information may be passed to that agency if it is necessary to provide their care, but that the agency has also signed up to the same standards of confidentiality.

- That service users have the right to access their health records which can be explained on request.

- That ECCH sends anonymised information to the Department of Health (DoH) to allow it to manage services and monitor effectiveness

5.9. It may also be appropriate or necessary to discuss the use of service user's information at other times during their care for example when transferring their care to someone or somewhere else, if a person potentially lacks the capacity to make decisions surrounding their healthcare. The Mental Capacity Act 2005 will generally only affect people aged 16 or over and provides a statutory framework to empower and protect people who may lack capacity to make some decisions for themselves, for example, people with dementia, learning disabilities, mental health problems, stroke or head injuries who may lack capacity to make certain decisions. The Act makes it clear who can take decisions in which situations and how they should go about this. It enables people to ahead for a time when they may lack capacity. The whole Act is underpinned by a set of five key principles set out in Section 1 of the Act:

- A presumption of capacity – every adult has the right to make his or her own decisions and must be assumed to have capacity to do so unless it is proved otherwise.

- Individuals being supported to make their own decisions – a person must be given all practicable help before anyone treats them as not being able to make their own decisions.

- Unwise decisions – just because an individual makes what might be seen as an unwise decision, they should not be treated as lacking in capacity to make that decision.

- Best interests – an act done or decision made under the Act must be done in the best interests of the patient; and

- Least restrictive option – anything done for or on behalf of a person who lacks capacity should be the least restrictive of their basic rights and freedoms.

5.10. The service user must consent to ECCH's proposed uses of their personal information. They therefore need sufficient information about the potential uses of their personal information to make informed choices. Staff must check that patients are aware that they have the right to choose whether to agree to information that they have provided in confidence being shared.

5.11. Staff should communicate effectively with patients to ensure they understand what the implications may be if they choose to agree to, or restrict, the disclosure of information.

5.12. Staff must check with patients that they have no concerns or queries about how their information is disclosed and used. In addition, staff must recognise the different communication needs of patients when seeking consent to use information (Please see appendix 5 for guidance about translation and signing facilities). It is not usual practice to obtain written consent for the use of information for care and treatment, although this is required for some other uses (such as research). Please seek advice from ECCH's Caldicott Guardian if in doubt.

5.13. If service users do not consent to ECCH's proposed use of their personal information, then it cannot be used in this way. It is important that service users fully understand the implications of such a decision and in serious situations, where the well-being of the patient or others may be compromised, if in doubt advice should be sought from ECCH's Caldicott Guardian.

5.14. Employees should explain to service users the limits of confidentiality and that, in certain circumstances, they will be obliged to pass on or act upon information even if the service user objects. This will apply if a failure to pass on information may lead to harm to the service user or someone else. There are also certain legal requirements to pass on information that can be explained to the service user if required.

5.15. Employees should only collect as much personal information as is necessary for the purpose, and no more. The information collected must be adequate but not excessive.

5.16. Clearly, most medical and employee records are by necessity very detailed, but they must nevertheless be accurate and relevant. Where information is extracted for other agreed purposes (e.g., audit) there should be a sound rationale for every piece of information that is used. Personal identifiers must be removed from the data if they are not strictly necessary for the intended use.

5.17. Employees have a legal obligation to ensure that any personal information recorded and held is accurate. Data is regarded as inaccurate if it is incorrect or misleading as to any matter of fact. Services users have a legal right to have inaccuracies of fact corrected or removed from their records, and to have any entry made in their record if they disagree with a statement of opinion.

6. REQUESTS FOR INFORMATION ON SERVICE USERS & STAFF

6.1. Never give out information on patients and staff to persons who do not need to know in order to provide healthcare, treatment and staff support.

6.2. All requests for person identifiable information should be based on a justified need and, in relation to patient identifiable information; some may also need to be agreed by ECCH's Caldicott Guardian.

6.3. If you have any concerns about disclosing/sharing person identifiable information you must discuss this with your line manager and if they are not available, someone with the same or similar responsibilities. If you cannot find anyone to discuss the issue with, you must wait until someone is available and only disclose when you have discussed with a manager and decided it is the appropriate thing to do.

6.4. If a request for information is made by telephone always check the identity of the caller and whether they are entitled to the information they request. In addition, verify a caller's identity independently by calling back, preferably via directory enquiries and/or a main switchboard number. Remember even the fact that a patient is in hospital, a patient of the hospital/practice or a member of staff is confidential. If in doubt you must consult your line manager.

6.5. Information requests made by the police must always be referred to the DPO, Caldicott Guardian, or the SIRO.

6.6. If a request for information is made by the media do not give out any information unless authorised to do so either by the Chief Executive or by a Director. If a request for information is received in person or by phone from a representative of the media, please refer them to the PA to the Chief Executive.

6.7. When disclosing information about patients and employees to other employees it must only be released on a "need to know" basis. Always check the member of staff is who they say they are. This can be achieved by checking face to face the employee's ID badge or Smartcard and/or calling the employee back via a main switchboard number if they do not reside in the same building. If possible, check whether they are entitled to the information. Do not be bullied into disclosing information. If in doubt always consult a manager.

6.8. It is strictly forbidden for employees to look at any information relating to their own records or those of family, friends, or acquaintances unless they are directly involved in a patient's clinical care or administration of another employee's records on behalf of ECCH. Any action of this kind is an abuse of privilege and will be viewed as a breach of confidentiality and may result in disciplinary action and potentially legal action by the Information Commissioners Office (ICO). Please consult your line manager if you have any concerns.

6.9. Employees must not treat confidential information with carelessness:

- Do not talk about patients in public places or where you can be Overheard
- Do not talk about confidential staff information in public places, communal staff areas or where you can be overheard
- Do not leave any confidential information e.g., medical notes/records

and staff records etc. lying around unattended

- Make sure that any computer screens, or other displays of information cannot be seen by staff members to whom the information is not relevant i.e., they do not have a “need to know” and members of the public.

- When leaving a desktop computer or laptop unattended you must lock your computer screen to ensure that nobody else can attempt to access and view confidential information in your absence.

- Staff are not permitted to post sensitive or confidential information e.g., any personal information about patients or staff, or any confidential corporate information to any social media platforms. Staff should refer to the ECCH Social Media and use of Websites Policy for full guidance.

7. TRANSFER OF INFORMATION

(See also the Information Governance Staff Handbook and the Information Security Policy)

7.1. 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 or 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 manager.

7.2. Internal mail containing confidential information must only be sent in a securely sealed envelope, and marked accordingly i.e. ‘Private and Confidential’. Where possible, internal mail should be used as a viable alternative to external mail.

7.3. External mail must also observe these rules. Confidential information must not be sent in bulk using external mail, either by standard or recorded delivery. Where it is necessary to send confidential information in bulk a viable alternative such as emailing using secure / password protected WinZip file/s or a portable media device such as a USB memory stick should be explored.

7.4. Confidential information sent via external mail must be sent using recorded delivery or approved courier to safeguard that the information is only seen by the authorised recipient/s. In some circumstances it is also advisable to obtain a receipt as proof of delivery e.g., patient records to a solicitor.

7.5. All Portable Media used by ECCH employees must be owned or approved by ECCH and must be encrypted. For advice on encryption please call IT on 01502 448615 or email ICT@ecchcic.nhs.uk.

7.6. **Faxing -** It is ECCH policy that no information should be sent by FAX.

7.7. **Email -** The email transmission of person identifiable and/or business sensitive information using anything other than secure email poses significant risks to confidentiality and should always be avoided unless essential to the delivery of care or management of resource. In these cases, strict principles should always be followed.

Person identifiers should be removed wherever possible, and only the minimum necessary information sent; this may be NHS or Payroll number but not a name and address. Special care should be taken to ensure the information is sent only to the recipients who have a "need to know"; always double check recipient details so that you are sure that the information is being sent to the correct recipient/s.

7.8. External transfers of person identifiable and/or business sensitive information should ideally take place to persons with access to a secure email address. A list of accredited NHS organisations can be found here https://digital.nhs.uk/services/nhsmail/the-secure-email-standard alternatively if you are unsure please contact the ICT helpdesk who will be able to advise. If required, encrypted messages can be sent to recipients using the encryption service. Contact the ICT department for further guidance if required.

8. STORAGE OF CONFIDENTIAL INFORMATION

8.1. Paper-based confidential information must always be kept locked away in a filing cabinet and/or a dedicated room, and the buildings in which the information is stored must be alarmed and every effort made to conceal confidential information so that when unattended, particularly at nights and weekends or when the building/office will be un-occupied for a long period of time, the information is not subject to theft.

8.2. Electronic confidential information should not be saved onto local hard drives; instead, it should be saved onto ECCH's network. Encrypted portable media can be used with prior agreement of the ICT department to store confidential information but must never act as a primary source of data. ECCH's network should act as the primary source of confidential information produced by the activity of its employees. This is to ensure that in times of loss or theft, information is sufficiently backed-up and available.

9. DISPOSAL OF CONFIDENTIAL INFORMATION

9.1. When disposing of paper-based person identifiable information or confidential information, always use a shredder or a 'Confidential Waste for Shredding' blue bin. Efforts should be made to keep waste in a secure place until it can be collected for disposal. The same applies for computer printouts of confidential information.

9.2. Electronic portable media including laptops, USB memory sticks, smart devices, DVD Hard disks and drives and CD ROMs containing person identifiable information or confidential information must be 'cleaned down' before they can be re-used. For this and permanent destruction of any of the above devices please consult IT support by calling 01502 448615 or email ICT@ecchcic.nhs.uk . The same applies to desktop computer hard drives.

10. CONFIDENTIALITY OF PASSWORDS –

10.1. Personal passwords issued to or created by employees should be regarded as confidential and those passwords must not be communicated to anyone else.

- Passwords should not be written down.
- Passwords should not be obvious in nature e.g., relate to the employee or system which they are accessing.

10.2. Passwords should generally be complex in nature i.e. letter, number and symbol based, and case sensitive. No employee should attempt to bypass or defeat the security systems or attempt to obtain or use passwords or privileges issued to other employees. Any attempts to breach security

must be immediately reported to the relevant director or senior manager and may result in disciplinary action and also a breach of the Data Protection Act 2018 and/ or the Computer Misuse Act 1990 which could lead to criminal action being taken.

11. WORKING AT HOME WHEN THERE IS A RECOGNISED NEED TO DO SO

11.1 It is sometimes necessary for employees to work at home. If you need to work at home you must first gain approval from your line manager. If they agree you will need to ensure the following are considered and remember that there is personal liability under the Data Protection Act 2018 and your contract of employment/DPA or confidentiality agreement for breach of these requirements:

- Ensure that you have authority to take the confidential information home.
- If you are taking paper-based information you must ensure that there is a record that you have these, where you are taking them and when they will be returned. This is particularly important for clinical information, patient records and sensitive staff information.
- Before transporting paper-based confidential information including person identifiable and business sensitive information from ECCH to your home you must ensure that it is sealed in a lockable case which will be supplied to you by ECCH if there is a recognised need for you to use one.
- You must make sure that the information is stored in the boot of the car or carried on your person whilst being transported from your workplace to your home and vice versa.
- If you are using public transport, where possible an alternative method of transfer other than carrying the information in paper format should be investigated e.g. An ECCH laptop with access to the U: & G: Drives.
- Portable media devices containing confidential information including person identifiable and business sensitive information must be encrypted, concealed, locked away and powered down before they can be transported. Again, they should be stored in the boot of the car or carried on your person whilst being transported from your workplace to your home and vice versa.
- Where possible electronic data should be accessed and saved to the ECCH network from home using ECCH's remote working solution. This ensures that data is 'in flight' securely using electronic means rather than being carried in public.
- You must not let anyone have any access to the information.
- Other family members must not be able to access the information.

11.2. When taking the information back to work you must, where appropriate ensure that the necessary assurance that the information has been returned is recorded e.g. your line manager is aware that the information has been returned or the record has been logged as returned in the record management system.

12. COMPUTER SOFTWARE

12.1. All computer software authorised for use within ECCH is regulated by license agreements. A breach of the agreement could lead to legal action against the organisation and/or the employee.

12.2. It is important that software on ECCH's desktop computers and systems is not copied and used for personal use. This would constitute a breach in the license agreement.

12.3. All Software installed on ECCH devices must only be done so by the ICT department. It is forbidden for any staff outside of the ICT department to download, copy, install or uninstall software from ECCH owned electronic devices.

13. GENERAL PROVISION

13.1. If any person requires an explanation concerning the interpretation or the relevance of this policy then they should discuss the matter with their line manager or the Data Protection Officer.

13.2. As a consequence of your employment by ECCH, you may acquire or have access to confidential person identifiable and/or business sensitive information which must not be disclosed to any other person unless in pursuit of your duties or with specific permission given by a person on behalf of ECCH. This condition applies during your relationship with ECCH and after the relationship ceases.

13.3. Non-compliance with this policy by any person working for ECCH may result in disciplinary action being taken, in accordance with ECCH's Disciplinary Policy. A copy of this and all other ECCH policies and documents mentioned in this policy are available on ECCHO. Alternatively, please ask your line manager.

12. LOSS OR COMPROMISE OF PERSONAL IDENTIFIABLE DATA

12.1. Any loss or compromise of data/person identifiable information in any format (electronic and paper) is regarded as an incident and will require reporting via Datix immediately as detailed in the Incident Reporting Procedure.

12.2. Near misses should also be reported via Datix. In the first instance any queries regarding reporting should be addressed to your line manager there after the Data Protection Officer.

12.3. Loss or theft of portable media must be reported to the IT Department via ICT@ecchcic.nhs.uk and to the DPO. In addition, a Datix Incident must be submitted. Any queries regarding reporting should be directed to the DPO.

14. CONFIDENTIALITY STATEMENT

14.1. All ECCH emails must contain the following disclaimer:

"The information contained in this e-mail is STRICTLY CONFIDENTIAL. If you are not the intended recipient please accept our apologies; please do not disclose, copy, or distribute information in this e-mail or take any action in reliance on its contents: to do so is strictly prohibited and may be unlawful. If you have received this e-mail in error, please notify the sender immediately. Thank you."

15. MONITORING AND REVIEW

15.1. The Information Governance and Caldicott Group will undertake the monitoring and review of this policy and procedure. This policy and procedure will be reviewed every two years (or earlier in light of new legislation/guidance).

16. REFERENCES

- Professional Codes of Conduct (e.g. GMC, HCPC, NMC) –
  - https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/good-medical-practice
  - https://www.hcpc-uk.org/standards/standards-of-conduct-performance-and-ethics/
  - https://www.nmc.org.uk/standards/code/
- Data Protection Act
  - https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
- Confidentiality: NHS Code of Practice
  - https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf
- Caldicott information governance review
  - https://www.gov.uk/government/publications/caldicott-information-governance-review-department-of-health-response
- ICO UK GDPR Guide
  - https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/
- Human Rights Act
  - https://www.legislation.gov.uk/ukpga/1998/42/contents
- Copyright, Designs and Patents Act
  - https://www.gov.uk/government/publications/copyright-acts-and-related-laws
- The Computer Misuse Act
  - https://www.legislation.gov.uk/ukpga/1990/18/contents
- Mental Capacity Act 2005
  - https://www.legislation.gov.uk/ukpga/2005/9/contents

17. ASSOCIATED POLICIES (To include but not limited to)

- Information Governance Handbook
- Information Governance Policy
- Data Protection and Personal Information Handling Policy
- Confidentiality and Data Protection Policy
- Record Keeping Policy
- Records Management Policy
- Communications and Media Policy
- Incident Policy
- Serious Incident Policy
- Disciplinary Policy
- IT Security Policy
- Access to Health Records / Subject Access Request (SAR) Policy and Procedure Guidance
- Social Media and use of Websites Policy

18. APPENDIX

- Appendix 1 - Professional Codes of Conduct
- Appendix 2 - Ensuring Confidentiality in ECCH
- Appendix 3 - Declaration of Confidentiality
- Appendix 4 - HEALTHCARE CONFIDENTIALITY STATEMENT
- Appendix 5 - INTRAN
- Appendix 6 - CALDICOTT & CONFIDENTIALITY

Appendix 1
Professional Codes of Conduct

1. Doctors

6. Confidentiality is central to trust between doctors and patients. Without assurances about confidentiality, patients may be reluctant to seek medical attention or to give doctors the information they need in order to provide good care. But appropriate information sharing is essential to the efficient provision of safe, effective care, both for the individual patient and for the wider community of patients.

7. You should make sure that information is readily available to patients explaining that, unless they object, their personal information may be disclosed for the sake of their own care and for local clinical audit. Patients usually understand that information about them has to be shared within the healthcare team to provide their care. But it is not always clear to patients that others who support the provision of care might also need to have access to their personal information. And patients may not be aware of disclosures to others for purposes other than their care, such as service planning or medical research. You must inform patients about disclosures for purposes they would not reasonably expect or check that they have already received information about such disclosures.

8. Confidentiality is an important duty, but it is not absolute. You can disclose personal information if:

(a) It is required by law (see paragraphs 17 to 23)

(b) The patient consents – either implicitly for the sake of their own care (see paragraphs 25 to 31) or expressly for other purposes (see paragraphs 32 to 35)

(c) It is justified in the public interest (see paragraphs 36 to 56).

9. When disclosing information about a patient, you must:

(a) Use anonymised or coded information if practicable and if it will serve the purpose

(b) Be satisfied that the patient:

(i) Has ready access to information that explains that their personal information might be disclosed for the sake of their own care, or for local clinical audit, and that they can object, and

(ii) Has not objected

(c) Get the patient's express consent if identifiable information is to be disclosed for purposes other than their care or local clinical audit, unless the disclosure is required by law or can be justified in the public interest

(d) Keep disclosures to the minimum necessary

(e) Keep up to date with, and observe, all relevant legal requirements, including the common law and data protection legislation.

10. When you are satisfied that information should be disclosed, you should act promptly to disclose all relevant information.

11. You should respect, and help patients to exercise, their legal rights to:

    (a) Be informed about how their information will be used, and

    (b) Have access to, or copies of, their health records.

2. Nurses and Midwives

Extract from Nursing and Midwifery Council "The Code: Professional standards of practice and behaviour for nurses and midwives"

5 Respect people's right to privacy and confidentiality
As a nurse or midwife, you owe a duty of confidentiality to all those who are receiving care. This includes making sure that they are informed about their care and that information about them is shared appropriately.

To achieve this, you must:

5.1 respect a person's right to privacy in all aspects of their care

5.2 make sure that people are informed about how and why information is used and shared by those who will be providing care

5.3 respect that a person's right to privacy and confidentiality continues after they have died

5.4 share necessary information with other healthcare professionals and agencies only when the interests of patient safety and public protection override the need for confidentiality, and

5.5 share with people, their families, and their carers, as far as the law allows, the information they want or need to know about their health, care, and ongoing treatment sensitively and in a way they can understand.

3. Health & Care Professionals

Extract from UK Council for health and care professionals *'Standards of conduct, performance and ethics.'*

5 Respect Confidentiality

Using information
5.1 You must treat information about service users as confidential.

Disclosing information
5.2 You must only disclose confidential information if:

- you have permission;
- the law allows this;
- it is in the service user's best interests; or
- it is in the public interest, such as if it is necessary to protect public safety or prevent harm to other people.

4. Social Workers

Extract from British Association of Social Workers “The Code of Ethics for Social Work: Statement of Principles”

> 10 Maintaining confidentiality
>
> Social workers should respect the principles of confidentiality that apply to their relationships and ensure that confidential information is only divulged with the consent of the person using social work services or the informant.
>
> Exceptions to this may only be justified on the basis of a greater ethical requirement such as evidence of serious risk or the preservation of life. Social workers need to explain the nature of that confidentiality to people with whom they work and any circumstances where confidentiality must be waived should be made explicit. Social workers should identify dilemmas about confidentiality and seek support to address these issues.

5. Health Informatics Professionals

Extract from UK Council for Health Informatics Professionals “Code of conduct: Protect and act in the interests of patients and the public”

All health informatics professionals shall, to the best of their ability, protect and promote the interests of patients and the public by:

- Ensuring that information systems and equipment for which they are responsible are procured, installed, maintained and operated professionally, efficiently and safely, and provide good value for the public money invested in them.

- Ensuring the security, confidentiality, accuracy and integrity of information, and protecting the safety of patients and the public, both directly through their personal actions and indirectly through the design and operation of any information systems for which they are responsible.

- Reporting to the proper authorities any improper or misleading use of information, whether accidental or deliberate, or misconduct by any person in connection with the procurement, operation or use of information systems and equipment.

- Promoting the appropriate use of information to enhance patient and public involvement and to support patient empowerment, dignity and choice.

Appendix 2

Ensuring Confidentiality in ECCH

Everyone working in ECCH has a legal duty to keep information about patients confidential and to ensure that the information accessed by those contracted to work on its behalf is processed lawfully, for a specific purpose, is relevant and not excessive, and is in accordance with the rights of the data subject. This legal duty also applies to individuals who are not employed by ECCH but have been contracted to work on NHS premises. It is important that you understand what is required of you so do please ask if there is any aspect of what is contained in this document that is unclear. Breaches of information security may be subject to investigation by the Information Commissioner.

The prime focus on confidentiality in ECCH is patient information but data protection laws also apply to many other forms of information. The legal duty means that you must not discuss with anybody - including your family, friends, patients themselves, and indeed, your work colleagues if your work is unconnected to their work or you are working in ECCH premises carrying out maintenance tasks – anything that you may see during the course of carrying out your contracted work for ECCH. If you are working in a clinical area and see somebody that you know, clearly you may greet them and pass the time of day with them in the usual way. You must not, however, enquire after the purpose of their visit, nor must you enquire later as to how they got on at the clinic/surgery.

You must not attempt to access any information that is deemed irrelevant to the task/s that you have been contracted to complete - to do so would constitute a breach in data protection laws and would be subject to local, and possibly national, investigation. For further guidance please consult the manager who has brought you into contract.

If you are concerned that ECCH is not protecting information sufficiently, please discuss this with the manager who has brought you into contract in the first instance so that steps may be taken to rectify matters. Should practices remain unchanged, please contact the Information Governance Lead at East Coast Community Healthcare CIC.

Appendix 3

Declaration of Confidentiality

I have read the statements above and understand that I must not discuss with anyone any information that I may see during the course of my work for ECCH, nor must I attempt to access information that is not relevant to the task/s for which I have been contracted.

Should I have reason to believe that ECCH is not keeping information securely, I will discuss it with the manager who has contracted me to carry out work in the first instance or with the Information Governance Lead for East Coast Community Healthcare CIC at the address below.

Name: ……..

Employer/Agent's Name: ……..

Signature: …….

Manager's Name: …….

Signature: …….

Date: ……..

This document must be held on file by the local ECCH manager, and a copy sent to the Information Governance Lead at East Coast Community Healthcare CIC at the address below:

East Coast Community Healthcare CIC,
Hamilton House
Battery Green Road
Lowestoft
Suffolk,
NR32 1DE

Appendix 4

East Coast Community Healthcare

HEALTHCARE CONFIDENTIALITY STATEMENT

During your contact with East Coast Community Healthcare, you will be asked to provide personal information to help us to deliver the best possible service to you. The information you provide, along with any other information we hold about you, will be kept together and form a healthcare record. ECCH staff and everyone else working for ECCH have a legal duty to maintain the highest level of confidentiality about all service user information and will endeavour to take every reasonable precaution to safeguard the personal information you have entrusted to us. You have a right to see and comment on any information we hold about you: this is called Subject Access. If you do have any concerns or queries about the information ECCH holds about you, we suggest, that in the first instance you discuss this with the member of staff you are in contact with.

Except in very exceptional circumstances, we will only provide information about you to your relatives and carers if you want us to. In certain circumstances we are required by law to disclose information. This information is only provided by ECCH where we have a statutory duty to do so, in accordance with our obligations under the Data Protection Act 2018.

In some instances, you may be receiving care from other people as well as ECCH and we may need to share some of the information about you with them, so that we can all work together for your benefit. Anyone who receives confidential information about you from us is also under a legal duty of confidence. Unless there are exceptional circumstances, for example, when the health and safety of others is at risk, we will not disclose your information to a third party without your permission.

east coast
community healthcare

Appendix 5

IN
TRAN
communication for all

How to book an INTRAN Interpreter?
Verbal Communication

Language Line

Telephone Interpreting

Tel: 0800 169 2694

CINTRA

Face-to-face Interpreting in a foreign language Tel: 01223 348870
You can email requests to; booking@cintra.org.uk
or fax requests to: 01223 309923

Deaf ConneXions

British Sign Language
Lip-speaking

Tel: 01603 660889
Min: 01603 661113

- **Your I.D. Code?**
- **Your Name?**
- **The name of your organisation?**
- **The language/dialect you require?**
- **What is it about? (context)**

Brief the Interpreter

- Who?
- Where?
- What?

- When?
- Where?
- With Whom?

Text-To-Speech

- If you were to receive a written document, letter, message, in a foreign language.
- If you were to write a note and you would like an interpreter to inform your client/ patient about the content of these notes. An interpreter will ring back and explain the content of the written 'document'.

What to do?

- Fax the document to Language Line together with the booking form and an interpreter will ring you or your client, explaining the meaning of the faxed document
- Fax Language Line on: 020 7520 1490

TRANSLATION

Please contact your INTRAN Internal rep first if you would like to have a written document translated into another language or into English.
Contact: Pearl Linguistics
Telephone: 020 7253 7700

Specify the format in which you would like to receive the document, and when you need it for.

MY INTRAN INTERNAL REP IS:

For further information or questions
Name: Jennifer Downie
Job Title: Equality and Diversity Manager
Telphone: 01603 257252

Please remember to give your INTRAN ID code when you use any of the above services

Appendix 6

CALDICOTT & CONFIDENTIALITY

Caldicott is a report from the committee chaired by Dame Fiona Caldicott in 1997, which looked at uses of patient identifiable information in healthcare and made recommendations to safeguard the confidentiality of personal medical information for everyone. There is still a requirement for every NHS organisation to have a Caldicott Guardian to monitor patient information flows and control of access to patient information.

Caldicott Principles:

1. **Principle 1:** ***Justify the purpose(s) for using confidential information***

2. **Principle 2:** ***Use confidential information only when it is necessary***

3. **Principle 3:** ***Use the minimum necessary confidential information***

4. **Principle 4:** ***Access to confidential information should be on a strict need-to-know basis***

5. **Principle 5:** ***Everyone with access to confidential information should be aware of their responsibilities***

6. **Principle 6:** ***Comply with the law***

7. **Principle 7:** ***The duty to share information for individual care is as important as the duty to protect patient confidentiality***

8. **Principle 8:** ***Inform patients and service users about how their confidential information is used***