Tel: 01392 829989
Website: www.epicsolutions.org.uk
Email: admin@epicsolutions.org.uk

Confidentiality Policy and Audit Process

This policy is consistent with the guidance from NHSE, GMC and CQC

Introduction

Confidentiality is the client's right for information shared with anyone who works in association with EPIC Solutions to not be shared with another party unless they consent to do so. This must be respected by all who work in association with EPIC Solutions. Consent must be obtained from clients for any disclosure of confidential information. The client can give consent orally or in writing. This should always be recorded.

This policy should be read in conjunction with EPIC Solutions:

Consent Policy
Safeguarding Policy
Data Protection Policy

To give consent to information sharing the client needs to understand:

- who the information will be disclosed to
- precisely what information will be disclosed
- why the information is to be disclosed
- the significant foreseeable consequences

When a client gives consent, you must only disclose information the client has agreed you may disclose, and only to the third party that requested it. No other use can be made of the information without seeking further consent from the client.

Children and Young People

For young people under 18 parents/guardians generally need to be provided with information about their child's problems and treatment in order to adequately support and care for them. From the outset there should be a discussion with the child/young person, and where appropriate their parent(s)/carer(s)/guardian(s), about information sharing and confidentiality. The extent and nature of the discussion will vary according to the age of the child and the nature of treatment. Where information is shared with parents about a competent child, the child's agreement to share the information should be obtained and evidence recorded in the notes.

Where a competent child refuses to allow information to be shared with their parent(s)/carer(s)/guardian(s), there should be evidence that the risks of not sharing the information have been considered. Where it is thought to be in the child's best interests to share information, there should be evidence of attempts to seek a compromise. Where there are safeguarding concerns, information may need to be shared with parents/guardians and/or other professionals in the absence of agreement.

What is confidential information?

Tel: 01392 829989
Website: www.epicsolutions.org.uk
Email: admin@epicsolutions.org.uk

All information about a patient is confidential. This includes any information that could identify an individual, for example:

- medical records
- current illness or condition and its ongoing treatment
- personal details – name, address, age, marital status, sexuality, race, etc.
- record of appointments
- audio or audio/visual recordings
- the fact that a person is or was a client

Maintaining Confidentiality (see also Data Protection Policy)

It is the responsibility of all who work in association with EPIC Solutions to:

- Safeguard the confidentiality of all person-identifiable or confidential information
- Keep all non-digital records containing person-identifiable or confidential information in locked filing and storage places
- Securely dispose of any non- digital records once transferred to the electronic notes system (Cliniko)
- Password protect computers with access to person-identifiable or business confidential information
- Ensure that you cannot be overheard when discussing confidential matters
- Challenge and verify where necessary the identity of any person who is making a request for person-identifiable or confidential information and ensure they have a need to know.
- Share only the minimum information necessary.
- Use secure e mail accounts to send confidential information (nhs.net or gov.uk) or password protect access
- Seek advice from the Directors of EPIC Solutions if you need to share patient/person-identifiable information without their consent
- Report any actual or suspected breaches of confidentiality.
- Not share passwords or leave them around for others to see
- Not share confidential information without clients consent unless there are statutory grounds to do so
- Don't use person-identifiable information unless necessary, anonymize where possible
- Don't collect, hold or process more information than you need, and don't keep it for any longer than necessary

Authorised Access to Clinical Records

Policy Amendment: Access to Clinical Records

Effective immediately, all staff are reminded that access to clinical records is strictly limited to instances where there is both a right and a legitimate need to do so in the course of their professional duties.

Tel: 01392 829989
Website: www.epicsolutions.org.uk
Email: admin@epicsolutions.org.uk

Staff must only access patient records when:

- They are directly involved in the care, treatment, or support of the individual, or
- They require access to fulfil a specific, authorised function related to their role (e.g. administration, audit, safeguarding, or clinical governance), and
- Access is proportionate and justifiable for the purpose intended.

Accessing records out of curiosity, for personal interest, or without authorisation is strictly prohibited and constitutes a breach of confidentiality, which may result in disciplinary action, up to and including dismissal, and potential referral to relevant professional bodies.

Additional Restrictions: Family Members Accessing Services

Employees must not access the clinical records of their own child, family member, or anyone with whom they have a personal relationship, unless:

- There is a clear, documented professional need to do so, and
- Explicit written consent has been obtained from the individual (or their parent/guardian, where appropriate), and
- This access has been authorised in advance by a director

Accessing the records of someone you know personally — including your own child — without appropriate consent and authorisation is a serious breach of confidentiality, regardless of role, and may lead to disciplinary action up to and including dismissal.
All staff are required to complete mandatory training on Information Governance annually and must report any concerns or breaches immediately to a Director.

Handling of confidential information

With advances in the electronic management of information the requirement to monitor access to confidential information has become increasingly important. Furthermore, with the increased use of electronic communications, the movement of confidential information via these methods poses an increasing threat of information falling into the hands of individuals who do not have a legitimate right of access to it. Good practice requires that all organisations put in place control mechanisms to manage and safeguard confidentiality, particularly client and other personal information.

It is recognised that those working in association with EPIC Solutions would not willingly abuse the information to which they have access, but EPIC Solutions has a responsibility to ensure that confidential information is protected. Access needs to be carefully monitored and controlled as failure to ensure that adequate controls are implemented and fulfil their intended purpose may result in a breach of confidentiality, therefore contravening the requirements of Caldicott, GDPR, the Data Protection Act 2018, the Human Rights Act 1998 and the Common Law Duty of Confidentiality.

The audit procedures described below will provide an assurance mechanism by which the controls implemented within EPIC Solutions and the effectiveness of these controls are audited, areas for improvement and concern highlighted, and recommendations for improved control and management of confidentiality within made.

Tel: 01392 829989
Website: www.epicsolutions.org.uk
Email: admin@epicsolutions.org.uk

Scope of audit

All work areas within EPIC Solutions which process (handle) confidential information will be subject to this confidentiality audit procedure. Confidentiality audits will focus primarily on controls within electronic systems but access to both electronic and hard copy confidential information will be audited.

Objectives

- To establish an approach to monitor access to confidential information throughout EPIC Solutions
- To provide assurance that the necessary controls are in place to manage access to confidential information
- To discover whether confidentiality has been breached, or put at risk, through misuse of systems, or as a result of poorly applied controls

Responsibilities

The Epic Directors have overall responsibility for ensuring that Information Governance is managed responsibly. They are responsible for ensuring that a confidentiality audit procedure is developed and communicated to all associates with the potential to access confidential information.

Controls and Monitoring Access to Confidential Information

In order to provide assurance that access to confidential information is gained only by those individuals that have a legitimate right of access, it is necessary to have appropriate controls in place and undertake monitoring as required. Monitoring will be carried out on a regular basis in line with system procedures/controls.

Reporting and Investigating Confidentiality Incidents

Actual or potential breaches of confidentiality should be reported in line with EPIC Solutions Significant, Critical Event Policy in order that action can be taken to prevent further breaches taking place. The Directors/Managers will be responsible for ensuring that the whole EPIC Solutions organisation is informed of any concerns highlighted as a result of monitoring access to confidential information.

Investigation and management of confidentiality incidents will be in line with the EPIC Solutions Significant, Critical Event Policy.

Unauthorised access to confidential information by any individual is not tolerated. Any breaches of confidentiality or security made outside the proper course of duty may be considered by the Directors and lead to termination of the association with EPIC Solutions.

Auditing Access to Confidential Information

Audits will check:

- Failed/repeated attempts to access confidential information

Tel: 01392 829989
Website: www.epicsolutions.org.uk
Email: admin@epicsolutions.org.uk

- Access of confidential information by unauthorized persons
- Evidence of shared login sessions/passwords
- Previous confidentiality incidents and actions taken
- Associates awareness of policies and guidelines concerning confidentiality and understanding of their responsibilities with regard to confidentiality
- Appropriate communications with clients
- Appropriate recording and/or use of consent forms
- Appropriate allocation of access rights to systems which contain confidential information
- Appropriate use of mobile telephones in open areas
- Extent of using and handling protectively marked documents
- Confidential information sent or received via e-mail, security applied and e-mail system used
- Information removed from the workplace
- Security applied to laptops and portable electronic media
- Evidence of secure waste disposal
- Appropriate transfer and sharing arrangements are in place

Author	Publication date	Reviewed	Review date
Karen Street	October 2020	July 2025	July 2028