



Tel: 01392 829989  
Website: [www.epicsolutions.org.uk](http://www.epicsolutions.org.uk)  
Email: [admin@epicsolutions.org.uk](mailto: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)/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)/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.



Tel: 01392 829989

Website: [www.epicsolutions.org.uk](http://www.epicsolutions.org.uk)

Email: [admin@epicsolutions.org.uk](mailto:admin@epicsolutions.org.uk)

### **What is confidential information?**

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

### **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



Tel: 01392 829989  
Website: [www.epicsolutions.org.uk](http://www.epicsolutions.org.uk)  
Email: [admin@epicsolutions.org.uk](mailto:admin@epicsolutions.org.uk)

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.

### **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**

**Dr Vicky Hill and Dr Karen Street**, as Directors of EPIC Solutions, along with EPIC Solutions Managers, 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 should be carried out on a regular basis in line with system procedures/controls. For unstructured information, such as MS Word or hard copy documents, monitoring should be carried out in order to check that controls are in place and irregularities regarding access to confidential information can be identified, reported, and action taken to address



Tel: 01392 829989

Website: [www.epicsolutions.org.uk](http://www.epicsolutions.org.uk)

Email: [admin@epicsolutions.org.uk](mailto:admin@epicsolutions.org.uk)

the situation, either through disciplinary action, the implementation of additional controls or other remedial action as necessary.

### **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
- 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

### **Audit Method**

Audits will be carried out through the annual internal audit programme where EPIC Solutions identifies notes for a confidentiality audit or as part of a records or other Information Governance audit. These audits will be carried out by the EPIC Solutions Managers. Serious, critical incidents and complaints related to confidentiality and information governance will also be reviewed.



Tel: 01392 829989

Website: [www.epicsolutions.org.uk](http://www.epicsolutions.org.uk)

Email: [admin@epicsolutions.org.uk](mailto:admin@epicsolutions.org.uk)

Peer review audits will be invited if there have been any significant or recurrent breaches of confidentiality identified through the annual internal audit procedures.

## Frequency

Internal Audits will take place annually.

## Peer Review Audits

- Pre-Audit Questionnaires

Using this information the auditor will get a feel for the nature of EPIC Solutions work. This will allow the auditor to ask informed questions when conducting the audit. The pre-audit questionnaire should be annotated with a contact name and number and should be returned to the auditor in advance of the scheduled audit date.

- Pre-Audit Meeting

Unless the questionnaire provides all the necessary background information required the auditor should arrange a brief pre-audit meeting with the EPIC Directors/Managers with the aim of discussing the process and what documentation will be required. The required documentation, including local procedures which are in place, should be forwarded to the auditor prior to the audit commencing.

## Audit Checklist

An Audit Checklist (see Appendix 4) should be used to detail the elements to be checked. This will enable the auditor to track progress of the audit.

## Conducting the Audit

Audit check list: Brief notes should be made on the Audit Checklist as follows:

Column B should be used to record evidence put forward to support the responses to questions asked. Where documents form the evidence provided, the reference number of the document or documents should be included for ease of reference.

Column C should be used to record the auditor's assessment as to how the evidence demonstrates compliance with the requirements of the Data Protection Act, the procedures and the Caldicott Principles.

Column D should be used to record the auditor's grading of the response to each question:

- COM – evidence demonstrates fully compliance
- MAJ – evidence demonstrates major non-compliance
- MIN – evidence demonstrates minor non-compliance

## Staff Awareness

In addition to the above the auditor should consider carrying out staff awareness interviews. The following should be considered:

- Roles and responsibilities
- Awareness of general confidentiality issues



Tel: 01392 829989

Website: [www.epicsolutions.org.uk](http://www.epicsolutions.org.uk)

Email: [admin@epicsolutions.org.uk](mailto:admin@epicsolutions.org.uk)

- Understanding of Data Protection Principles directly relating to their job
- Understanding the requirements of policies and procedures relating to confidentiality

The auditor's questions and the interviewee(s) responses should be recorded on the Interview Record Sheet – See Appendix 4.

## Reporting

Where non-compliance is observed, this should be recorded as soon as possible, be sufficiently detailed, including all the facts and referring to any relevant evidence. The non-compliance should be recorded on the Non-compliance Observation Sheet – Appendix 5. The detail recorded should include an outline of what was observed, where it was observed, who was involved, the date of the observation and why it was considered non-compliant. Each non-compliance observed should have an associated recommendation which should be discussed and agreed with the Directors and other associates. Each recommendation should also include a target date for completion and a named individual who will be responsible for ensuring that the recommendation is implemented. Once the follow-up meeting has taken place the auditor will complete the bottom section of the form, indicating implementation of recommendations and effectiveness of those recommendations. When the auditor is satisfied that the non-compliance has been resolved the auditor will sign the Non-compliance Observation Sheet.

Non-compliance can fall into one of two categories:-

**Major Non-compliance:** this would indicate that the non-compliance has occurred on a regular basis and could potentially have serious consequences.

**Minor Non-compliance:** these could include one-off occurrences of non-compliance; there are likely to be only minor consequences.

Where a number of minor instances of non-compliance are observed in the same area of work, this may indicate a more serious problem, these instances of non-compliance should be combined into a Major non-compliance.

Once the audit has been completed a formal report should be produced by the auditor detailing the outcome of the audit. It will include a summary of the findings of the audit, together with observations of non-compliance and recommendations which have been made. A meeting should be held with the Directors/Managers to go through the findings and agree the corrective actions required. Any comments expressing disagreement should be noted on the audit report.

## Quality Assurance

The Directors will sample review reports and their supporting documentation in order to verify consistency of approach. (Audit report template – Appendix 6)

## Audit Follow-Up

Reports on audit outcomes including progress on recommendations made will be considered by the Directors/Managers who will monitor progress on actions identified.



Tel: 01392 829989  
Website: [www.epicsolutions.org.uk](http://www.epicsolutions.org.uk)  
Email: [admin@epicsolutions.org.uk](mailto:admin@epicsolutions.org.uk)

### **Audit Closure**

Once corrective action has been checked and agreed as compliant by the auditor, the audit can be formally closed.

Author	Publication date	Reviewed	Review date
Karen Street	October 2020	March 2023	March 2026



Tel: 01392 829989  
 Website: [www.epicsolutions.org.uk](http://www.epicsolutions.org.uk)  
 Email: [admin@epicsolutions.org.uk](mailto:admin@epicsolutions.org.uk)

**PRE AUDIT QUESTIONNAIRE**

<b>Department:</b>		<b>Audit Ref.</b>
<b>Location:</b>		
<b>Contact Name:</b>	<b>Position:</b>	<b>Telephone No:</b>
<b>Summary of Department Functions:</b>		
<b>Number of Full Time Staff:</b>		<b>Number of Full Time Staff:</b>
<b>Question 1</b>		<i>Enter Question Here:</i>
<i>Response:</i>		
<b>Question 2</b>		<i>Enter Question Here:</i>
<i>Response:</i>		
<b>Question 3</b>		<i>Enter Question Here:</i>
<i>Response:</i>		
<b>Question 4</b>		<i>Enter Question Here:</i>
<i>Response:</i>		
<b>Question 5</b>		<i>Enter Question Here:</i>
<i>Response:</i>		





Tel: 01392 829989  
Website: [www.epicsolutions.org.uk](http://www.epicsolutions.org.uk)  
Email: [admin@epicsolutions.org.uk](mailto:admin@epicsolutions.org.uk)

**INTERVIEW RECORD SHEET**

<b>Department:</b>	<b>Audit Date:</b>	<b>Audit Ref.</b>
<b>Page No:</b>		
<b>ATTENDEES</b>		
<b>Name</b>	<b>Position</b>	
<b>DETAILS OF INTERVIEW</b>		
<b>Question 1</b>	<i>Enter Question Here:</i>	
<i>Response:</i>		
<b>Question 2</b>	<i>Enter Question Here:</i>	
<i>Response:</i>		
<b>Question 3</b>	<i>Enter Question Here:</i>	
<i>Response:</i>		
<b>Question 4</b>	<i>Enter Question Here:</i>	
<i>Response:</i>		
<b>Question 5</b>	<i>Enter Question Here:</i>	
<i>Response:</i>		



Tel: 01392 829989  
 Website: [www.epicsolutions.org.uk](http://www.epicsolutions.org.uk)  
 Email: [admin@epicsolutions.org.uk](mailto:admin@epicsolutions.org.uk)

**NON-COMPLIANCE OBSERVATION SHEET**

<b>Department:</b>	<b>Audit Date:</b>	<b>Audit Ref:</b>
<b>Details of Non-Compliance:</b>		
<b>Extent of non-compliance (tick as appropriate)</b>	<b>Auditor Name:</b>	<b>Date of observation:</b>
Major	Minor	<b>Signature:</b>
<b>Recommendations:</b>		
<b>Follow-up Date:</b>	<b>Additional Comments:</b>	
<b>Follow-up:</b>		
<b>Compliance Assessment:</b>	<b>Auditor Name:</b>	<b>Date Re-assessed:</b>
COM/MIN/MAJ	<b>Signature:</b>	



Tel: 01392 829989  
 Website: [www.epicsolutions.org.uk](http://www.epicsolutions.org.uk)  
 Email: [admin@epicsolutions.org.uk](mailto:admin@epicsolutions.org.uk)

**AUDIT REPORT TEMPLATE**

<b>Department:</b>	<b>Audit Date:</b>	<b>Audit Ref.</b>
<b>Page No. 1</b>		
<b>AUDIT SUMMARY</b>		
<b>Auditor Name:</b>	<b>Signature:</b>	<b>Date Closed:</b>

**AUDIT REPORT TEMPLATE (CONTINUED)**

<b>Department:</b>	<b>Audit Date:</b>	<b>Audit Ref.</b>	
<b>Page No:2</b>			
<b>OBSERVATIONS SUMMARY</b>			
<b>Obs Ref</b>	<b>Details of Observations</b>		
<b>SUMMARY OF AGREED CORRECTIVE ACTIONS</b>			
<b>Non Compliance Ref</b>	<b>Action By</b>	<b>Corrective Action to be Taken</b>	<b>Date</b>



Tel: 01392 829989  
 Website: [www.epicsolutions.org.uk](http://www.epicsolutions.org.uk)  
 Email: [admin@epicsolutions.org.uk](mailto:admin@epicsolutions.org.uk)

<b>AGREED AUDIT FOLLOW UP</b>			
<b>Auditor Name:</b>	<b>Signature:</b>	<b>Date Closed:</b>	
<b>AUDIT CLOSED</b>			
<b>Auditor Name:</b>	<b>Signature:</b>	<b>Date Closed:</b>	
<b>ADDITIONAL COMMENTS:</b>			

Appendix 7

**AUDIT CHECKLIST**

Department: Interviewee: Date:  
 Process: Auditor: Ref No.  
 Question or Check    Documentary Evidence    Findings and Observations    Result  
    Examined