



## **Caldicott visits**

A Caldicott visit establishes a process for observational review to monitor access to confidential person-identifiable in both a paper and electronic format across services within the Trust.

This process forms part of the Trusts overall assurance framework to meet requirements within: -

- the Data Security and Protection Toolkit
- the NHS Confidentiality Code of Conduct
- Registration Authority Governance Arrangements for the NHS

## **Scope of the visits**

For the purposes of this procedure, confidential person-identifiable information is defined as any information about a person which would allow that person to be identified.

All work areas within the Trust which process (handle) confidential person-identifiable information will be subject to the Caldicott visit process.

Access to both electronic and manual confidential person-identifiable information will be reviewed. Audits across all the Trusts sites including integrated areas will be undertaken as this will help to capture any inconsistencies in working practices and policy.

## **Caldicott visit approach**

What the Caldicott visit will look for: -

- Staff awareness of Trust policies and guidelines concerning confidentiality
- Guidance for patients,
- Appropriate use of smartcards
- Appropriate allocation of access rights to systems
- Appropriate staff access to physical areas
- Storage of and access to filed hard copy person-identifiable notes and information
- Security of post handling areas
- Security of recorded telecommunications and message books
- Appropriate use and security of the telephone in open areas
- Storage of person-identifiable information in public areas

The DSPTeam will provide the following deliverables: -

- Planned and implemented audit programme
- Audit reports and recommendations for the Service Manager, SIAO, IAO Data Security and Protection Committee (DSPC) as required
- Support with action plans to address any areas requiring review
- Reports to the Caldicott Guardian concerning any identified breaches.

Audit methods and facilities to be utilised: -

- Spot checks to random work areas
- Interviews with staff using structured questionnaires



- Registration Authority (smartcard usage) enhanced reporting facilities
- Regular staff knowledge and understanding surveys

### **Audit findings**

Results from the audits will be collected in a standard template. The draft report including recommendations and action plan to address any noted issues will be sent to the service manager / IAO and SIAO for review and comment. Copy also to be sent to the Caldicott Guardian. Service manager / IAO and SIAO will also agree timescales for completion and implementation of actions.

An update report of all actions will be submitted to the monthly DSPC for information.

In the event of serious breaches found, the SIAO must be informed immediately, incidents should be logged on Safeguard and a report should be submitted to the DSPC highlighting any areas or risk that requires further corporate development, making recommendations concerning any corrective actions as required.

A follow up visit by a member of the DSP team will take place once actions are complete as a final sign off and close down of the visit outcomes.