Health Service Circular
Local Authority Circular

Series Number:	**HSC 2002/003 : LAC(2002)2**
Issue Date:	**31 January 2002**
Review Date:	**31 January 2003**
Category:	**Information Management**
Status:	**Action**
	sets out a specific action on the part of the recipient with a deadline where appropriate

IMPLEMENTING THE CALDICOTT STANDARD INTO SOCIAL CARE

Appointment of "Caldicott Guardians"

For action by:	Councils - Common Council of the City of London, Chief Executive Councils - Council of the Isles of Scilly, Chief Executive Councils - County Council Chief Executives Councils - London Borough Council Chief Executives Councils - Metropolitan District Council Chief Executives Councils - Shire Unitary Council Chief Executives Social Services Directors - England
For information to:	Health Authorities (England) - Chief Executive NHS Trusts - Chief Executives NHS PCGs and PCTs - Chief Executives

Further details from: Confidentiality Issues Section
Department of Health
1N35 A
Quarry House
Quarry Hill
Leeds LS2 7UE
0113 254 6267
matthew.birkenshaw@doh.gsi.gov.uk

Additional copies of this document can be obtained from:
Department of Health
PO Box 777
London
SE1 6XH
Fax 01623 724524
It is also available on the Department of Health web site at
http://www.doh.gov.uk/publications/coinh.html

IMPLEMENTING THE CALDICOTT STANDARD INTO SOCIAL CARE

Appointment of "Caldicott Guardians"

Summary

The Caldicott review of personally identifiable information in 1997 recommended that "Guardians" of personal information be created to safeguard and govern the uses made of confidential information within NHS organisations.

The Caldicott principles and processes provide a framework of quality standards for the management of confidentiality and access to personal information under the leadership of a Caldicott Guardian. The Caldicott standard is being extended into Councils with Social Services Responsibilities (CSSRs) in order to provide a good foundation for joint working between health and social services, and to help support the fulfilment of the many joint strategies across children's and adult services.

This requirement follows a consultation process with Directors of Social Services, Chief Executives of Local Authorities, stakeholder organisations, and the Information Commissioner. A report of the feedback has been compiled and will shortly be disseminated.

The Data Protection Act 1998 is the key legislation covering all aspects of information processing, including security and confidentiality of personally identifiable information. The Caldicott requirements provide a framework to operationalise the Data Protection Act and underpin appropriate information sharing.

Action

As part of the implementation strategy, all CSSRs are expected to have appointed a Caldicott Guardian by **1st April 2002.** This is a later date than proposed in the consultation paper to enable CSSRs to adequately prepare for the appointment/nomination and to provide some flexibility to this process. We are keen to ensure that appropriate Guardians are appointed and understand that some CSSRs will require time to make the right appointment.

We recommend that the first task CSSRs undertake is an audit of existing systems, procedures and organisational capabilities relating to confidentiality and security in the organisation. This will assist in the development of stock-take reports and an improvement plan for internal use, both of which will be necessary to comply with Caldicott requirements effectively.

Councils should confirm in their Position Statements to SSI that they have completed the necessary processes, and have action in hand for the implementation of the next steps.

We recognise that in some CSSRs a Caldicott Guardian has already been appointed. Where this is the case, the audit of systems will form their first task. However, for those CSSRs who choose to appoint at a later date, then an appropriate person will need to be identified to carry out the initial audit tasks.

The Caldicott work programme for the next 18 months and the Management Audit are shown at Attachments A and B. To assist with conducting audits, CSSRs should have received an electronic Caldicott 'Toolkit' developed by the NHS as a training and education pack. This provides 'signposting' to relevant examples of good practice, appropriate guidance material and related legislation. The intention is for these products to be tailored

over time to include 'social services specific' scenarios and guidance. More information about the toolkit is shown at Attachment C.

The details of your social services Caldicott Guardian should be added, by the 1st April 2002 to the national Register. The appropriate registration form can be obtained by contacting Matthew Birkenshaw at the Department of Health in Leeds via matthew.birkenshaw@doh.gsi.gov.uk or 0113 254 6267. Alternatively an electronic copy can be downloaded from www.doh.gov.uk/ipu/confiden.

The Caldicott standards apply to social services functions within the council, however the Department of Health is currently giving consideration to how it might be possible to extend implementation of the standards across other local authority functions in due course. In the meantime, as several of the Caldicott requirements cannot be met fully by social services alone, Local Authority Chief Executives are encouraged to support the delivery of this programme of work especially where joint work extends beyond social services.

Further information

Information about Caldicott into Social Care will continue to be posted on the following websites:

ADSS: www.adss.org.uk (under latest)
ADSS IMG: www.ssimg.freeserve.co.uk
NHS (confidentiality website): www.doh.gov.uk/ipu/confiden.

This Circular has been issued by:

David Gilroy
Deputy Chief Inspector
Social Services Inspectorate

Attachments:

- A – Timetable of work for 2001/02 and 2002/03
- B – Management Audit
- C – Overview of the Caldicott Toolkit

ATTACHMENT A

Timetable of work for the implementation of Caldicott into Social Care

Timetable of work 2001/2002	
JANUARY– APRIL	Conduct an initial management audit and produce first stock-take report. This will include the identification and registration of the Caldicott Guardian by 1st April 02
MAY	Develop proposed improvement plan.
JUNE	Present stock-take report and improvement plan to the organisation's Management Board.
JULY	Agree and initiate work programme to implement the improvement plan.
AUGUST– NOVEMBER	Review current information flows of personally identifiable data.
AUGUST-NOVEMBER	Develop and agree protocols to govern information sharing with partner organisations and other local authority functions.
DECEMBER	Update the organisation's Management Board on progress against the improvement plan.
DECEMBER-FEBRUARY	Conduct management audit and prepare first annual out-turn report for the organisation's Management Board. Also prepare the improvement plan for 2003/2004.
FEBRUARY-APRIL	Agree and initiate work programme to implement the improvement plan. Submit out-turn report and improvement plan to the SSI

ATTACHMENT B

Management Audit

In relation to their social services functions, it is essential that CSSRs take stock of their current performance across a wide range of confidentiality and security measures. This should serve to highlight areas where improvement is needed and provide a benchmark for evaluating progress over time.

Working with the Data Protection Officer and information security or other support staff, an audit should be carried out of existing systems, procedures and organisational capabilities relating to confidentiality and security in the organisation. Using this audit as a measure of the organisational baseline, i.e. current performance, an improvement plan should be developed to begin the process of year on year improvement. At the end of the year an out-turn report should be prepared to measure whether planned improvements have been achieved. This out-turn report is effectively the Management Audit that will underpin the following year's improvement plan.

A straightforward audit tool follows which provides a simple and effective assessment of organisational performance and capacity, by rating current performance from 0-2 against 18 broad headings to construct an organisational profile. Additional headings can be added to the audit tool at local discretion and, if there is a logical or practical need to do so, existing headings can be sub-divided to facilitate achievable target setting.

During the recent consultation process, amendments to the audit tool were proposed, some of which have been incorporated. However, some of the suggestions would have resulted in changes to the order of the audit areas, the addition of some new ones and the deletion of others. Had these changes been made at this time, the audit content would not have been reflected by the electronic Caldicott 'Toolkit' that is available, and this would have resulted in the toolkit being of less assistance to them. (Details to obtain a copy of the electronic toolkit are attached in annex C.) As a result, the audit has remained largely unchanged at this time, but suggestions have been recorded and will be a valuable source of information to assist with the modifications that will be required to Caldicott for its convergence with Information Governance.

It should also be noted that for the first stock-take report compiled, audit areas 8, 10 and 11 will not be measured. It is acknowledged that more clarity and central guidance is required before CSSRs can be expected to have made sufficient progress in the areas of mapping information flows, safe haven procedures and the structure and content of information sharing protocols. Further information will be made available in support of these audit areas – all of which will be measured in subsequent audits.

THE MANAGEMENT AUDIT ORGANISATIONAL PROFILE

A portfolio of evidence should be created and may be required during performance monitoring.

	AUDIT AREA	LEVEL 0	LEVEL 1	LEVEL 2
1	Information for clients on the proposed uses of information about them	No information provided, or limited to simple posters and leaflets in common areas	An active information campaign is in place to promote client understanding of information requirements	An active information campaign is supported by comprehensive arrangements for clients with special/different needs
2	Staff code of conduct in respect of confidentiality	No code exists, or staff not generally aware of it	Code of conduct exists and all staff aware of it (including switchboard and post room staff)	Code regularly reviewed and updated as required
3	Staff induction procedures	No mention of confidentiality & security requirements in induction for most staff	Basic requirements outlined as part of induction process	Comprehensive awareness raising exercise undertaken and comprehension checked
4	Confidentiality & Security training needs assessment	Training needs not assessed systematically for most staff	Training needs only considered as a consequence of organisational or systems changes	Systematic assessment of staff training needs and evaluation of training that has occurred undertaken as part of supervision and appraisal process
5	Training provision – confidentiality & security, including appropriate and lawful information sharing	No training available to the majority of staff	Training opportunities broadcast with take-up left to line management discretion	In-house training provided for staff e.g. comparable to Health & Safety provision
6	Staff Contracts	No reference to confidentiality requirements in staff contracts	Confidentiality requirements included in contracts for some staff	Confidentiality requirements included in all staff contracts

	AUDIT AREA	LEVEL 0	LEVEL 1	LEVEL 2
7	Contracts placed with other organisations	No confidentiality requirements included	Basic agreements of undertaking are signed by relevant support organisations and contractors for service provision, and by other agencies and individuals with access to personal data (including cleaners, photocopy repairers, site security guards, etc.)	Formal contractual arrangements exist with all contractors and support organisations and are regularly monitored and enforced
8	Reviewing information flows containing personally-identifiable information	Information flows have not been comprehensively mapped	Information flows have been mapped and are available to inform and support business processes, and the development of workable protocols and agreements	Procedures are in place to regularly review information flows and justify purposes
9	"Ownership" established for each logically discrete set of information (includes electronic databases and manual records)	Ownership has not been established for any information or data sets	Ownership established for some information or data sets and register established	Ownership established for all information or data sets and owners justifying purposes and agreeing staff access restrictions with the Guardian
10	"Safe Haven" procedures for personally-identifiable information flows	No Safe Haven procedures used	Safe Haven procedures used for some information flows	Safe Haven procedures in place for all relevant information flows

	AUDIT AREA	LEVEL 0	LEVEL 1	LEVEL 2
11	Protocols governing the sharing of personally-identifiable information with other directorates and organisations locally agreed	No locally agreed protocols in place	Partner directorates and organisations clearly identified and information requirements understood	Agreed protocols in place to govern the sharing and use of confidential information
12	Security Policy document (see BS7799 for guidance on content)	No Security Policy available	Security Policy but not reviewed within last 12 months	Security Policy reviewed annually and reissued as appropriate. Regular checks conducted of staff awareness and comprehension.
13	Security responsibilities	No awareness of information security responsibilities at personal or organisational levels	Responsibilities clarified and an information security training and awareness programme is underway	Responsibility for information security identified in various staff roles, co-ordinated at a high level by one or more individuals in the organisation
14	Information risk management programme	No programme of information risk management exists	A risk management programme is underway and reports are available	A formal programme exists with regular reviews, outcome reports and recommendations provided for senior management
15	Security incidents	No incident control or investigation procedures exist	The security incidents are handled as they arise	Procedures are documented and accessible to staff to ensure incidents are reported and investigated promptly

	AUDIT AREA	LEVEL 0	LEVEL 1	LEVEL 2
16	Security monitoring	No monitoring or reporting of security effectiveness or incidents takes place	Basic reporting of major incidents or problem areas only	There are processes in place to ensure security is monitored and lessons are learnt from security incidents, and there are regular reports to senior management on the effectiveness of information security
17	Systems user responsibilities for password management	No guidance issued to systems users for password management	Systems users encouraged to change passwords regularly but this is at their discretion	Password changes are enforced on a regular basis and effective password management by systems users can be evidenced (including notifying of leavers so passwords can be disabled)
18	Controlling access to manual and systems based confidential information	Staff vigilance, and/or an “honour” system, controls access. Some physical controls, lockable rooms, etc. may exist	Access for many staff controlled by ‘all or nothing’ systems. Staff groups requiring access identified and agreed with the Guardian	All staff have defined and documented access rights agreed by the Guardian. Access is controlled, monitored and audited

ATTACHMENT C

Overview of the electronic Caldicott Toolkit

The electronic Caldicott toolkit has been developed by the NHS as part of a training and education pack to provide 'signposting' to relevant examples of good practice, appropriate guidance material and related legislation.

The toolkit comes as a ‘pack’, which contains a video with 16 scenarios, each showing security and confidentiality breaches, along with an accompanying booklet and a very comprehensive CD.

The CD is web-enabled and is designed in such a way as to take the user through each performance measure in the Management Audit, with the opportunity at each measure to investigate four routes to further relevant resources. The four routes for further information are:

- law and guidance
- organisation
- people
- education, training and awareness

This pack was released to the NHS in September 2001 and has been distributed to Caldicott Guardians in social care. The pack will be an invaluable resource to all Caldicott Guardians

The pack was accompanied by a covering letter to social services explaining that the content has been designed for the NHS, but that the intention is for the products to be tailored over time to include 'social services specific' scenarios, information and links to appropriate legislation and guidance.

If you have not received a copy of this pack, please contact helpdesk3@nhsia.nhs.uk or telephone 0121 333 0420.