CALDICOTT: PRINCIPLES INTO PRACTICE

OUT-TURN REPORT 2013 &

IMPROVEMENT PLAN 2013/14

February 2013

Prepared by: Dorian Edwards
Information Governance Manager
ABMU LHB

CONTENTS

1.0 EXECUTIVE SUMMARY

1.1 **Background**

Since the Caldicott Report was published in 1997 by Dame Fiona Caldicott, there have been significant changes to both Legislation and Codes of Practice which govern access to and use of patient identifiable information.

Implementation of the Caldicott Report recommendations commenced across NHS Wales in 1999 with the expectation that all health organisations would embark on a programme of continuous improvement of the organisation's status against the Caldicott Principles.

In 2008, Informing Healthcare embarked on a review of the Caldicott Manual and in November launched the Foundation Manual for Caldicott Guardians, Caldicott Leads and Information Governance Leads. This manual provides all involved with protecting and using patient identifiable information with a knowledge framework with what they need to know, why they need to do it and how to do it. It also includes an online Self Assessment tool (C-PIP Assessment) which enables organisations to quickly evaluate where they are with compliance and plan improvement. This is the fourth annual assessment completed by ABMU.

1.2 **Work Programme**

There is a requirement for each organisation to develop work programmes to assess their compliance with the Caldicott Principles on an annual basis. As such this organisation completed the online self assessment tool in February 2013 and has developed an improvement plan. Progress with the improvement plan will be monitored via the Health Care Standards Improvement Plan (HCSIP) on a quarterly basis.

The following out-turn report provides a summary of the completed assessment and the improvement plan for 2013/14.

1.3 **Action Required**

The *Quality & Safety Committee,* on behalf of the Executive Board, is asked to approve this Caldicott Out-Turn report.

2.0 REPORT SUMMARY

2.1 Caldicott: Principles into Practice (C-PIP)

The Caldicott Foundation Manual: Principles into Practice (C-PIP) provides Guardians and their support staff with updated knowledge about the legal background to their duties and aspects of Information Governance. The manual sets out what organisations need to do and the arrangements that need to be in place to ensure patient information is handled appropriately. The C-PIP Assessment consists of 41 Self Assessment standards which have been grouped into 6 sections. Against each question there is a hierarchy of answers that depending on which option is selected will automatically generate a score. Each organisation must then annually assess their compliance with the Caldicott Principles and produce a programme of work and continual improvement.

2.2 Caldicott Standards & Self Assessment

As part of the Caldicott Annual Programme of Improvement, this organisation has self assessed itself against the updated Caldicott standards. The self assessment allows a simple and effective assessment of organisational performance by rating current performance in percentage against the standards to construct an organisational profile. In doing this, the on line assessment was completed with a copy of the standards below, the organisation's response (whether fully or partially compliant), score and any additional comments, differences from last year's score are highlighted:

Number	Assessment Standard	LHB Response	Score	Comments
Section 1 – Governance The organisation must assign Caldicott and Information Governance responsibilities				
G1	Has your organisation appointed a Caldicott Guardian	Full compliance	2/2	The Medical Director is the Caldicott Guardian
G2	Does your organisation have an Information Management Strategy that has been approved by the Board or equivalent?	Full compliance	1/1	IM&T Strategy re-approved by the Exec Board July 2009 and still current.
G3	Do staff responsible for Information Governance provide regular reports to the Board or equivalent?	Full compliance	1/1	The Information Governance Manager provides reports on Caldicott, DPA & Information Sharing Agreements to the Execs and Executive Board via ISGB and Q&S Committee.

G4	Is there an Information Governance work plan, sponsored by the Caldicott Guardian and approved by the Board or equivalent?	Full compliance	1/1	To be developed by May 2013.
G5	Has the Records Management Policy and implementation plan been approved by the Board or its equivalent, communicated to appropriate staff and reviewed on a regular basis?	Full compliance	1/1	The Records Management Policy has been approved by the Exec Board, communicated to all members of staff and is reviewed on a regular basis.
G6	Do mechanisms and guidelines exist to ensure that any decision taken by a patient or service user to restrict the disclosure of their personal information are appropriately respected?	Partial compliance	0.67/2	A process was developed, approved by ISGB and put in place in mid 2011
G7	Is information risk management included in the organisation's wider risk assessment and management framework?	Full compliance	2/2	A formal Risk Management Programme exists with half yearly reviews which are reported to the Audit Committee and High Level Risks are reported directly to the Board.
G8	Does the organisation have documented and accessible information security incident reporting, investigation and resolution procedures in place that are explained to all staff?	Full compliance	2/2	The Incident Reporting Procedures are freely available to all Staff and Contractors. Reports are provided to Risk Management Group.
G9	Does the organisation have formal contractual arrangements with all contractors and support organisations that include their responsibilities in respect of information security and confidentiality?	Partial compliance	1.4/2	Although contracts include responsibilities in respect of information security & confidentiality, further development of systems for monitoring compliance is required. ISMS & Clinical Governance Assessment Tool covers GP Practices.
G10	Does the organisation ensure that all new services, projects, processes, software and hardware comply with information security, confidentiality and data protection	Non compliance	0/2	The organisation needs to develop systems for Privacy Impact Assessing new processes, etc in line with the Information Commissioners recommendations.

	requirements?			
Section 2 – Management The organisation must have core policies in place for Caldicott and Information Governance.				
M1	Where staff have been assigned Information Governance roles, are they appropriately qualified & trained	Full compliance	5/5	The Information Governance Managers and Information Security Managers have been delegated responsibility for Information Security, Data Protection and Information Sharing and have received appropriate training.
M2	Was the organisations last assessment of performance against the Caldicott Standards completed within the last year	Full compliance	1/1	Yes – score is 78% for 2012/13.
M3	Does the organisation have a comprehensive Records Management Policy for corporate and medical records	Full compliance	1/1	The Records Management Policy & Guidelines incorporate storing, creation, record keeping, closure, disposal and retention of all records.
M4	Does the organisation have an accurate and up to date Notification to the Information Commissioner under the Data Protection Act 1998?	Full compliance	1/1	The organisation's Notification is reviewed and updated accordingly each year.
M5	Is Data Protection comprehensively addressed either in a dedicated policy or by its incorporation into another policy	Full compliance	1/1	The Trust Data Protection & Confidentiality Policy was updated and approved in March 2013 and is regularly reviewed.
M6	Is Information Security comprehensively addressed either in a dedicated policy or by its incorporation in a wider security policy	Full compliance	1/1	Information Security policies reviewed and approved in March 2013.
M7	Does the organisation have an up to date Business Continuity and Disaster Recovery Plan?	Partial compliance	1/2	The Business Continuity Plan and Disaster Recovery Plan are both up to date.
M8	Is a comprehensive confidentiality statement included within all established staff and non-staff contracts	Full compliance	1/1	All staff contracts include a confidentiality statement
M9	Are personal responsibilities in respect of	Full	2/2	All Job Descriptions include responsibility clauses

	confidentiality, records management, information security, data protection and freedom of information in all job descriptions?	compliance		for confidentiality, FoI, Records Management.
Section 3 – Information for Patients and Service Users The organisation must have an active information campaign in place to inform patients about the use of their information.				
IP1	Does the organisation have appropriate procedures for recognising and responding to patient requests for access to health records	Full compliance	2/2	Exec Board approved the Health Records Policy in January 2010. Our website is also used to inform patients on the uses of their information, information sharing agreements and policies in respect of patient information.
IP2	Do you tell patients and service users about the ways in which their information will or may be used?	Partial compliance	0.6/2	This standard is similar to the previous standard governing providing patients where possible on how their information might be used. It was agreed nationally that further support is needed to provide material across all organisations in the NHS in Wales in the form of posters and leaflets. These support documents were approved centrally but unfortunately costs for this process were prohibitive and there has not been an all Wales implementation..
Section 4 – Training and Awareness The organisation must assess Information Governance training needs and ensure that role specific information is provided to all staff.				
TA1	Does your organisation effectively address information governance for all staff at induction?	Partial compliance	1.5/2	Staff induction procedures include comprehensive awareness-raising regarding information governance. No formal checks of comprehension are assessed.
TA2	Have you conducted an analysis of information governance training needs?	Full compliance	2/2	Training assessed – all staff require full awareness regarding data protection and confidentiality.
TA3	Do you provide information governance training to staff, other than at induction?	Partial compliance	1.33/2	Mandatory and ad hoc training is provided for staff and attendance spreadsheets are kept.

				These include DPA, Caldicott & IM&T Security, FoI and Records Management. From April 2013 this data is recorded and linked to the ESR.
TA4	What percentage of your staff have undertaken an Information Governance awareness session?	Partial compliance	0.4/1	This highlights the need for mandatory training and electronic enforcement tools.
Section 5 – Information Management The organisation must ensure that information is dealt with legally, securely, efficiently and effectively.				
IM1	Have information flows been comprehensively mapped and has ownership for information assets been established?	Partial compliance	1/2	Some flows are mapped, work will continue.
IM2	Does the organisation have appropriate arrangements in place to support the Information Sharing Agenda?	Full compliance	2/2	WASPI is now led by WG and this HB is compliant with regard to policies and has 4 staff trained as Facilitators.
IM3	Has the organisation made progress in implementing the Wales Accord for the Sharing of Personal Information (WASPI)?	Full compliance	2/2	The Records Management Group agreed to adopt the principles outlined in WASPI and the Chief Executive signed the accord in 2006 and for the ABMULHB in 2009. See above.
IM4	Are sufficient arrangements in place to ensure that the organisation complies with Data Protection requirements in respect of personal data outside of the EEA?	Full compliance	1/1	Currently records are transferred outside EEA only with consent of the data subject. We do not use processors outside EEA so no further policy restrictions are necessary. Transfers are declared in our Notification to the ICO.
IM5	Does the organisation have a strategy to ensure the correct NHS number is recorded for each active patient and that it is used routinely in clinical communications?	Full compliance	2/2	Requirement for using NHS Numbers is included in the Health Records Policy.
IM6	Does the organisation have paper health records of a standard design?	Full compliance	1/1	Health Records Committee has agreed a design for records' folders across the organisation.
IM7	Does the organisation have documented	Full compliance	1/1	Process included as part of the Health Records

	procedures on the identification and resolution of duplicate or confused patient records?			Policy.
IM8	Does the organisation have processes and procedures in place to enable it to regularly monitor, measure and trace paper health records?	Full compliance	1/1	The Key Performance Indicator Report monitors the accessibility of all records internally and reports are submitted to the Health Records Committee.
Section 6 – Controlling Access to Confidential Information The organisation must have arrangements in place to control and monitor access to information.				
CA1	Is there a Confidentiality Code of Conduct which provides staff with clear guidance on the disclosure of patient/service user identifiable information?	Partial compliance	1.5/2	Code of Conduct is included in the Data Protection and Confidentiality Policy. The Confidentiality Code of Practice for Health & Social Care in Wales is available via the website. All staff are aware of the code via staff awareness sessions. The effectiveness of this code is not monitored.
CA2	Are processes in place to ensure that contractors understand their responsibilities regarding confidentiality and information security?	Full compliance	1/1	GP's covered via ISMS & CG Assessment Tool. Opticians will be covered with the pending CG Assessment Tool. All Caldicott Information & Assessment have been disseminated to all contractors for completion of understanding. Awareness training has been provided to Pharmacists & Dentists.
CA3	Are there safe haven procedures in place for sharing information both electronically and manually?	Partial compliance	1.75/2	E mail Policy gives clear direction regarding the transfer of personal data by e mail. Some areas of the organisation have Safe Haven facilities for faxing personal data. There is a Fax Policy, which instructs staff on the way personal data must be sent to ensure confidentiality. Data transfer sticks and portable computers are encrypted.
CA4	What controls are in place to restrict staff access to patient/service user identifiable	Partial compliance	1.33/2	Access to patient information is managed on a "trust" basis.

	information?			Access can be monitored ; audit is undertaken as and when necessary.
CA5	Are there physical access controls in place for relevant buildings?	Full compliance	2/2	Building is securely locked and alarmed. Safe Haven faxes are located within lockable rooms. Locks are located on all PII Storage containers and filing cabinets.
CA6	What password management controls are in place for information systems that hold patient/service user identifiable information systems?	Partial compliance	0.8/1	Password enforcement is in place. Awareness sessions given by IT Security and IG Managers include strong messages regarding security and “not to share” passwords. Strong passwords are used within some systems.
CA7	Has the organisation established appropriate confidentiality audit procedures to monitor access to patient identifiable information?	Partial compliance	0.8/2	Processes have been implemented to investigate and audit where breaches have been identified. Information security audits are planned and carried out by ICT Security and IG departments.
CA8	Does the organisation have appropriate policies in place to cover risks associated with mobile/tele working?	Full compliance	1/1	The organisation has in place an approved authorisation procedure via the Telecoms Manager and guidelines are issued to staff. Mobile working is only possible via secure systems link.

2.3 **C-PIP Score**

Star Rating	C-PIP Score	
*****	91-100%	Your responses to the assessment demonstrate an excellent level of assurance of information governance risks.
****	76-90%	Your responses to the assessment demonstrate a good level of assurance of information governance risks; but there is still work to be done.
***	51-75%	Your responses to the assessment demonstrate a satisfactory level of assurance of information governance risks although there are some significant weaknesses which you should address.
**	21-50%	Your responses to the assessment demonstrate an insufficient level of assurance of information governance risks and a number of significant weaknesses which you need to be addressed.
*		Your responses to the assessment suggest an inadequate level of assurance of information governance risks should be addressed as a matter of urgency.

The organisation has scored 78% *(83% in 2011/12)* and therefore falls within the category highlighted above at a 4 star rating.

2.4 **Yearly Score Comparison**

The organisation is fully compliant with 28 standards, partially compliant with 12 and non compliant with 1 out of 41 standards; these figures remain unchanged from last year. A comparison will be made with these scores after next year's assessment to establish any patterns and improvements.

3.0 IMPROVEMENT PLAN 2010/11

3.1 **Responsibilities**

Implementation and progress of the Improvement Plan [Appendix A] will be the responsibility of the Information Governance Managers, IT Security Managers and the Caldicott Guardian.

Work will be co-ordinated through the *Quality and Safety Committee.* This will provide the appropriate organisational framework to progress work and to provide management with additional reporting and monitoring mechanisms.

3.2 **Timescale**

The organisation will progress the Improvement Plan over the next financial year and regular updates will be monitored via the Health Care Standards Improvement Plan

(HCSIP). A further assessment will be required to be completed by March 2014 for 2013/14.

4.0 SUMMARY

This report will be presented to the *Quality and Safety Committee*. It has been agreed by the Caldicott Guardian and the actions will be monitored by the Information Governance Manager on a quarterly basis as part of the HCSIP. This will help to ensure continual progress with compliance with the Caldicott Principles.

APPENDIX A

Caldicott Improvement Plan 2013/14

Caldicott Standard		Proposed Action	Lead	Timescale
G6	Do mechanisms and guidelines exist to ensure that any decision taken by a patient or service user to restrict the disclosure of their personal information are appropriately respected?	Ensure all staff understand guidelines on restricting access to PII.	Information Governance Manager	September 2013
G9	Does the organisation have formal contractual arrangements with all contractors and support organisations that include their responsibilities in respect of information security and confidentiality?	Service users must ensure that all support organisations are suitably informed of their responsibilities and where possible WASPI agreements are to be put in place.	Information Governance Manager	December 2013
G10	Does the organisation ensure that all new services, projects, processes, software and hardware comply with information security, confidentiality and data protection requirements?	Develop process to ensure all new processes undergo a form of privacy impact assessment to check compliance with confidentiality and Data Protection requirements.	Information Governance Manager	December 2013
M7	Does the organisation have an up to date Business Continuity and Disaster Recovery Plan?	No single plan, there is a strategy.	IT Security Manager	Ongoing
IP2	Do you tell patients and service users about the way in which their information will or may be used	Staff need to actively promote the ways in which information is used other than for direct patient care	IG Manager	September 2013
TA1	Does your	Competence	IG/ICT Security	When all

	organisation effectively address information governance for all staff at induction?	testing will be used at e learning stage	staff	Wales e learning implemented
TA3	Do you provide information governance training to staff other than at induction?	Targeted training to be identified	Information Governance Manager	October 2013
TA4	What percentage of staff have undertaken an IG training session?	Continue with training/awareness sessions.	Information Governance Manager	Ongoing
IM1	Have information flows been comprehensively mapped and has ownership for information assets been established?	Consider re-establish mapping information flow project in organisation.	Information Governance Manager	December 2013
IM4	Are sufficient arrangements in place to ensure that the organisation complies with the DP requirements in respect to transfer of personal data outside of the EEA?	Reinforce section in DP Policy.	Information Governance Manager / IT Security Manager	June 2013
CA1	Is there a Confidentiality Code of Conduct which provides staff with clear guidance on the disclosure of patient/service user identifiable information?	This is included in the DP Policy but effectiveness of the Code is not checked with staff.	Information Governance Manager / IT Security Manager	March 2014
CA3	Are there safe haven procedures in place for sharing information both electronically and manually?	Some Safe Havens in place and fax policy for non Safe Havens.	No action necessary	
CA4	What controls are in place to restrict staff access to patient/service user identifiable information?	Controls are in place to allow relevant levels of access.	No action necessary	
CA6	What password	Working towards	ABMU	March 2014

	management controls are in place for information systems that hold patient/service user identifiable information systems?	integrating all system to use Cymru user accounts. Some legacy system are unable to do this but work on going.		
CA7	Has the organisation established appropriate confidentiality audit procedures to monitor access to patient identifiable information?	NHS Wales is considering the procurement of a software package that enables the interrogation of system logs. This system will then be rolled out to key information systems across the Health Board.	NWIS	2013-14