Bwrdd Iechyd Lleol a t Local Health Board
Powys

DATA PROTECTION & CONFIDENTIALITY POLICY

Policy	Date	Version Number	Planned Review Date
PtLHB / CP 086	Oct 2006 Jan 2009 Feb 2009 Mar 2009	Initial Issue 2nd Issue - Revised draft 3rd Issue - Further revised draft taking on board internal audit comments 4th Issue - Checks made as to whether addendum of supporting policies and procedures reference Data Protection Policy	Oct 2009 Mar 2012
Document Owner		**Approved by**	**Date**
Director of Finance/Records Manager		Records Management Group Clinical Governance & HCS Committee	Mar 2009 Mar 2009

Contents

1. INTRODUCTION

Powys teaching Local Health Board (PtLHB) is required to collect and use a wealth of personal information about people in order to operate. This includes information about patients, employees, suppliers and others with whom it communicates.

The organisation is required to register under the Data Protection Act 1998 and is subject to the Caldicott Principles, NHS guidance and professional codes of conduct. The tLHB must therefore develop an organisational framework and staff culture that ensures all patients identifiable and person identifiable information is managed sensitively, confidentially, legally and securely.

All information held by public authorities is subject to the Freedom of Information Act; however this does not change the right of patients and staff to confidentiality of their personal data as set out in the Data Protection Act 1998 and common law duty of confidentiality.

2. PURPOSE

The purpose of this policy is to define the requirements of the Data Protection Act 1998 and to inform members of staff how to manage personal and patient information in a confidential and secure manner.

The Data Protection Act 1998 came into force on 1 March 2000 and superseded the Data Protection Act 1984. The purpose of the Act is to protect the rights and privacy of individuals, and to ensure that data about them are not processed without their knowledge and are processed with their consent wherever possible.

The Act covers personal data relating to living individuals, and defines a category of sensitive personal data which are subject to more stringent conditions on their processing than other personal data.
The Act provides conditions for the processing of any personal data. It also makes a distinction between "personal" data and "sensitive" personal data.

Personal data is defined as, data relating to a living individual who can be identified from:

- That data;
- That data and other information which is in the possession of, or is likely to come into the possession of the data

controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

Sensitive personal data is defined as personal data consisting of information as to:

- Racial or ethnic origin;
- Political opinion;
- Religious or other beliefs;
- Trade union membership;
- Physical or mental health or condition;
- Sexual life;
- Criminal proceedings or convictions.

The tLHB is committed to a policy of protecting the rights and freedoms of individuals with respect to the processing of their personal data.

3. SCOPE

This policy applies to all types of personal and patient identifiable data held by Powys tLHB on computer, paper and imaging systems and includes visual and audio records, photographs, CCTV and any other media that records information traceable to an individual.

This policy applies to all staff employed by Powys tLHB, including the Business Services Centre, staff contracted under agency or similar arrangements, persons on placements and students. Staff employed by other organisations working at tLHB premises will be required to respect the policies of the tLHB.

There are areas of overlap between this and other organisational policies and procedures; this policy should therefore be considered in conjunction with other relevant documents and not read in isolation. Related polices and procedures have been highlighted at Appendix A.

4. LEGISLATIVE AND OTHER NHS REQUIREMENTS

For the purpose of this policy the leading legislative and NHS requirements/guidance are defined in:

- Data Protection Act 1998
- WHC (2000) 111 'Data Protection Act 1998'

- The Access to Medical Records Act 1990 (where it still applies)
- The Freedom of Information Act 2000
- WHC (2000) 71 'For the Record'
- Department of Health Code of Practice for Records Management
- Welsh Assembly Government Confidentiality: Code of Practice for Health and Social Care in Wales (August 2005)
- Standard for Information Security Management Systems ISO17799/27001 (formally BS7799)

5. PRINCIPLES

The tLHB will notify the Information Commissioner, as required by the Act of the information being processed by the tLHB in its role as a service provider, commissioner and processor. The notification will be reviewed regularly and amendments made promptly as necessary.

The tLHB fully endorses and will observe the principles of the Data Protection Act 1998 and the Caldicott Report 1997 in respect of confidentiality and the handling of personal information (Appendix B).

Where appropriate the tLHB will put in place an active "fair processing" framework to inform people and patients about how their information will be used and disclosed.

The tLHB undertakes to ensure that data held is adequate, relevant and not excessive in relation to the purpose for which it is held and processed. In addition the data will be, as far as is reasonable, accurate, kept up to date and not kept for longer than necessary.

The tLHB will ensure that appropriate technical and organisational measures are taken to prevent the unauthorised or unlawful processing, accidental loss, destruction or damage to personal data it holds.

The tLHB will not transfer any personal data to any country outside of the EEA, unless they ensure adequate levels of protection.

To comply with additional statutory restrictions, sensitive information will not be passed on in an identifiable format. For example:

- HIV/AIDS

- Other sexually transmitted diseases
- Assisted conception
- GU medicine
- Terminations

All tLHB employees will ensure that all personal data when communicated will only be on a need to know basis. Any personal data corresponded electronically will be sent securely in accordance with the tLHB and BSC Email policies.

6. RESPONSIBILITIES

All staff in the tLHB have a 'duty of confidentiality' and must apply the Data Protection Act 1998 and Caldicott principles to all processes involving the use of personal or patient identifiable information. They are responsible for ensuring that the information is kept securely, and not disclosed orally or in writing, accidentally or otherwise to an unauthorised third party. It is tLHB policy that unauthorised disclosures or misuse of information is a valid reason for disciplinary action.

The Director of Finance takes overall responsibility for compliance with the Data Protection Act in the tLHB. This includes maintaining and reviewing the notification, the Data Protection Policy, and any other related policies. Within the Business Services Centre, the Information Governance Manager is the agreed Data Protection lead.

The Medical Director is the tLHB Caldicott Guardian and takes responsibility for agreeing and monitoring protocols governing the management and movement of patient identifiable information within and outside the tLHB. These responsibilities are undertaken by the Head of Contractor Services in the Business Services Centre.

Clinical directors, directorate managers and all in managerial or supervisory roles have the responsibility of developing and encouraging good information handling practice within their designated areas.

A framework of professional groups is in place to support the requirements of this policy.

- tLHB Information Security and Caldicott Group (ISAGC),
- BSC Information Security Forum (ISF),
- BSC Information Governance Group (IGG),

- tLHB Records Management Group
- BSC Records Management Group
- Executive Ops Meeting

New uses, purposes or sharing of information will be referred to the Information Security and Caldicott Group for approval then passed to the Director of Finance who will be responsible for updating the Data Protection notification.

7. EMPLOYEE INFORMATION

The tLHB holds a great deal of information about staff for the purpose of appointments and removals, pay, discipline, superannuation, work management and other personnel matters. Any member of tLHB staff requesting access to their personnel records will need to be put their request in writing to the Human Resources Department at Bronllys Hospital, or for BSC staff to Human Resources, Pontypool.

8. RIGHTS OF ACCESS

Under the Act individuals have a right to see or be provided with a copy of personal information the organisation holds about them, known as 'Subject Access'.

In all cases requests must be made in writing and include sufficient information to be able to confirm the identity of the person making the request and to locate the information requested. The tLHB must respond to the request within 40 calendar days. A fee for this access may be made and will be advised upon request of the request.

If the request is from a third party, the request should generally contain the written consent of the individual concerned for the release of the information. Where this is not supplied, the tLHB will consider each request on a case by case basis. All records will be reviewed by the Data Protection Officer who will make sure that any individual's rights are respected, and that the release will not be likely to cause harm or distress to any party.

There are a variety of arrangements in place for dealing with Subject Access requests both within the tLHB and BSC which are covered in more detail at Appendix C.

9. TRAINING AND AWARENESS

Data Protection, Caldicott and confidentiality awareness training will be included as part of the tLHB induction programme at department and corporate sessions.

As part of ongoing training the tLHB will ensure its staff are made aware of changes to legislation or other standards and receive a level of training that is appropriate to their role.

No staff should be given or give access to personal or patient identifiable information in any format unless they have received appropriate training.

10. MONITORING AND REVIEW

Regular monitoring reports will be submitted to the Information Security and Caldicott Group (ISACG), BSC Information Security Forum and Powys tLHB Records Management Group, on all matters relating to Data Protection, including registration details.

This policy will be reviewed one year from the date of issue and at three yearly intervals thereafter. The review will be led by the Director of Finance in conjunction with the Information Security and Caldicott Group (ISACG), BSC Information Security Forum and Powys tLHB Records Management Group. An earlier review may take place if circumstances or legislation require it.

APPENDIX A – Related Policies and Procedures

Policy Name	Applies to	Comment
Freedom of Information Act Policy (PLHB CP0031)	tLHB/BSC	Sets out how the LHB will comply with FOIA and the overlap with the Data Protection Act.
Records Management Strategy and Policy	tLHB/BSC	Sets out responsibilities and process for management of records personal and non-personal in content
Information Security Policy (IMT0001)	tLHB	Covers the measures in place to protect the confidentiality, integrity, availability and security of all information including personal.
Information and IT Security Policies (PLHB CO0047 and 0048)	BSC	
Email Policy (PLHB CP0055 IMT0009)	tLHB	Covers security of mailboxes and transmissions and how to manage email records including those containing personal data.
Email Policy (PLHB CP 0050)	BSC	
Internet Policy (PLHB CP0057 IMT0006)	tLHB	Sets out proper/acceptable use that minimises risks to the network and protects personal data
Internet Policy (PLHB CP 0049)	BSC	
Procedure Name	**Applies to**	**Comment**
Access to Health Records Procedure (Requests by patients, relatives, or their legal representatives made under the Data Protection Act 1998 or Access to Health Records Act 1990.	tLHB	Covers process in place within the LHB, excluding the BSC
Access to Health Records Procedure and Supplementary Guidance	BSC	For copies of deceased patients records previously held by GP practices or for records of patients not registered with a GP
Data Protection Act 1998: Procedures and Supplementary Guidance for dealing with requests for information	BSC	For subject access requests excluding access requests for health records
Data Protection Procedure Employee Information	tLHB/BSC	More detailed provisions relating to Employees information
Retention and Destruction of Records	tLHB	
Corporate Records Management Procedures	BSC	
Procedure for the Archiving of Records and File Disposal	BSC	

APPENDIX B - Data Protection and Caldicott Principles

The Data Protection Act 1998 became law in March 2000. It expands on the 1984 Act to include manual as well as electronically held records. It also encompasses the Access to Medical Records Act 1990 where it applies to living individuals. The eight data protection principles underpin all related policies and procedures:-

1. Personal data shall be **processed fairly and lawfully** and, in particular, shall not be processed unless certain conditions (set out in schedules to the Act) are met.
2. Personal data shall be obtained only for one or more **specified and lawful purposes**, and shall not be further processed in a manner incompatible with the purposes.
3. Personal data shall be **adequate, relevant and not excessive** in relation to the stated purpose.
4. Personal data shall be **accurate** and, where necessary, **kept up to date.**
5. Personal data shall **not be kept for any longer than is necessary.**
6. Personal data shall be processed in accordance with the **rights of the individual.**
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing and against accidental loss, damage or destruction to personal data.
8. Personal data shall not transferred to countries outside the EEA without adequate protection being in place.

In 1997 the Caldicott Committee recommended that in order to regulate the use and transfer of patient identifiable information within and outside the NHS every use or flow of patient identifiable information should be regularly justified and routinely tested against six principles. Although tighter controls on the use of patient information were brought about by the introduction of the Data Protection Act 1998, the Caldicott principles and recommendations remain in place and provide a robust framework to ensure that organisations handle patient information in a confidential and secure manner. The Caldicott principles are:-

1. Justify the purpose(s) for using confidential information
2. Only use it when absolutely necessary
3. Use the minimum that is required
4. Access should be on a strict need to know basis
5. Everyone must understand his or her responsibilities
6. Understand and comply with the law

APPENDIX C – Subject Access Rights

Subject access requests will generally fall into the following categories:-

1. Requests for access to medical records of living individuals (under the Data Protection Act 1998)

The Records Manager, Support Services oversees this process for Powys tLHB records. The Procedure 'Access to Health Records – Requests by patients, relatives or their legal representatives' sets out the process and includes a request form and standard letters. It should be followed in all cases.

The BSC deal with requests to access GP records held on behalf of client LHBs. These requests are dealt with in accordance with local procedures within each BSC region.

2. Individuals seeking access to deceased persons medical records (under the Access to Medical Records Act 1990)

For records held by PtLHB the 'Access to Health Records Procedure' as detailed in 1 above includes details of how to deal with this type of request.

The BSC holds the GP deceased person records for all Wales on behalf of client LHBs. Access to these records is dealt with in accordance with local procedures within each BSC region.

3. Members of staff seeking access to their personnel/employee records

Employees may view their personnel record by making a request to the Human Resources Department at Bronllys Hospital. It is the responsibility of the Human Resources Department to make the Records Manager, Support Services aware of any such requests. In the BSC requests will be dealt with by the Information Governance Manager. All requests may be subject to the £10 fee.

4. Other subject access requests

Subject access requests that do not fall into the above categories will be dealt with by the Freedom of Information Team, Support Services Department, Bronllys Hospital and in the BSC the Information Governance Manager.