

Reference Number: UHB 350 Version Number: 1	Date of Next Review: 20 Sep 2019 Previous Trust/LHB Reference Number: UHB 002 v2 T/57
DATA PROTECTION ACT PROCEDURE	
Introduction and Aim This procedure supports the Data Protection Act Policy and will ensure that Cardiff and Vale University Health Board (the UHB) fully meets all the legislative requirements placed upon it under the Data Protection Act 1998. It will ensure that all staff understand the obligations placed upon them and that they are able to comply with the requirements of the Act.	
Objectives To ensure there is a structure for staff to follow in respect of the legislation and thereby the UHB can be fully compliant with the legislative requirements of the Data Protection Act 1998.	
Scope This procedure applies to: <ul style="list-style-type: none"> • All types of personal and patient identifiable data held by the UHB on computer, paper, imaging systems, visual and audio records, photographs, CCTV and any other media that records information traceable to an individual. • All staff in all locations employed by the UHB including contractors, students, volunteers, honorary contract holders and anyone who provides a service on behalf of the UHB. 	
Equality Impact Assessment	An Equality Impact Assessment has not been completed as this procedure forms part of the overarching Information Governance Policy and Framework and is covered in that document.
Health Impact Assessment	A Health Impact Assessment (HIA) has not been completed as this procedure forms part of the overarching Information Governance Policy and Framework .
Documents to read alongside this Procedure	<ul style="list-style-type: none"> • Data Protection Act Policy • Information Governance Policy • Information Governance Operational Management and Responsibilities Procedures • Freedom of Information Act Policy and Procedure • IT Security Policy and Procedure • Dealing with Subject Access Requests Procedure • Records Management Policy and Procedures

Document Title: Data Protection Procedure	2 of 34	Approval Date: 20 Sep 2016
Reference Number: UHB 350		Next Review Date: 20 Sep 2019
Version Number: 1		Date of Publication: 08 Mar 2017
Approved By: Information Governance Sub Committee		

	<ul style="list-style-type: none"> • Records Retention and Destruction Protocol • Confidentiality Code of Conduct • Personal Information Use and Disclosure of and Duty to Share Guidance • Transportation of Casenotes and Personal Identifiable Information Procedure
Approved by	Information Governance Sub Committee

Accountable Executive or Clinical Board Director	Medical Director/Director of Corporate Governance
Author(s)	Corporate Governance Senior Information and Communication Manager
<p><u>Disclaimer</u></p> <p>If the review date of this document has passed please ensure that the version you are using is the most up to date either by contacting the document author or the Governance Directorate.</p>	

Summary of reviews/amendments			
Version Number	Date of Review Approved	Date Published	Summary of Amendments
1	20/9/17(IGSC)	08/03/2017	Previous Policy re-structured into new UHB format. These procedures have been developed to underpin and support the policy and are based on the information provided within the previous policy. Addition of appendices.

Document Title: Data Protection Procedure	3 of 34	Approval Date: 20 Sep 2016
Reference Number: UHB 350		Next Review Date: 20 Sep 2019
Version Number: 1		Date of Publication: 08 Mar 2017
Approved By: Information Governance Sub Committee		

Contents page

1	Introduction	4
2	Scope	4
3	Aims and Objectives	5
4	Management and Employee Responsibilities	6
5	Disclosing Personal Data	9
6	Processing Personal Data	10
7	Use of Documentation and Forms used for Obtaining Personal Data	10
8	Ensuring Accuracy of Data	11
9	Retention of Data	11
10	Complying with the Requirements of Subject Rights	12
11	Security of Personal Data	12
12	Safe Use of Faxes	14
13	Safe Use of E-Mail	14
14	Data Protection Act Breaches	16
15	Transfers of Personal Information Outside the European Economic Area (EEA)	16
16	Training	16
17	Audit	17
18	Distribution and Review	17

Appendices

Appendix 1	Patient Data Security Guidance
Appendix 2	Relevant Legislation and Information
Appendix 3	Data Protection Act Useful Information and Definitions

Document Title: Data Protection Procedure	4 of 34	Approval Date: 20 Sep 2016
Reference Number: UHB 350		Next Review Date: 20 Sep 2019
Version Number: 1		Date of Publication: 08 Mar 2017
Approved By: Information Governance Sub Committee		

Appendix 4	Ten Rules for Data Protection Compliance
Appendix 5	Caldicott Guidance

Document Title: Data Protection Procedure	5 of 34	Approval Date: 20 Sep 2016
Reference Number: UHB 350		Next Review Date: 20 Sep 2019
Version Number: 1		Date of Publication: 08 Mar 2017
Approved By: Information Governance Sub Committee		

1. INTRODUCTION

The Data Protection Act 1998 (the Act) implements the European Union (EU) Data Protection Directive 95/46/EC on the protection of individuals with regard to the processing of personal data. The Act came into force on 1 March 2000 and regulates the processing of personal information, it sets out eight Principles for the processing of personal data.

The Data Protection Principles – Personal information:

- 1 Must be fairly and lawfully processed.
- 2 Must be processed for limited purposes.
- 3 Must be adequate, relevant and not excessive
- 4 Must be accurate and up to date
- 5 Must not be kept for longer than is necessary
- 6 Must be processed in line with the rights of the data subject
- 7 Must be secure
- 8 Must not be transferred to other countries without adequate protection.

Full details of the Principles can be accessed [here](#)

Cardiff and Vale University Health Board (the UHB) has a vast quantity of manual files holding personal data, predominantly for staff administration and medical purposes. Increasingly, automated systems are being used to store personal data and to share (disclose) this data for clinical, research, audit, training, employment and business purposes.

To ensure compliance with the Data Protection Act (DPA) employees need to be aware of their duties and obligations under the DPA, in order to reduce the risk that personal data may be processed inappropriately and/or unlawfully, and to ensure that neither staff nor the UHB commit any offences under the Act.

2. SCOPE

This procedure applies to all types of personal and patient identifiable data held by the UHB in every format including electronic data as held on computer, paper, imaging systems, visual and audio records, photographs, CCTV and any other media that records information traceable to an individual.

This procedure applies to all staff employed by the UHB including contractors, students, volunteers, honorary contract holders and anyone providing a service on behalf of the UHB.

Document Title: Data Protection Procedure	6 of 34	Approval Date: 20 Sep 2016
Reference Number: UHB 350		Next Review Date: 20 Sep 2019
Version Number: 1		Date of Publication: 08 Mar 2017
Approved By: Information Governance Sub Committee		

The Data Protection Act Policy and this supporting procedure underpin the Codes of Practice produced by the Information Commissioner's Office (ICO), the Caldicott Report and principles, NHS/Welsh Government guidance, professional body guidance (e.g. GMC, NMC) and Acts of Parliament.

All UHB employees have a common law duty of confidentiality towards all of the personal data in their possession.

3 AIMS AND OBJECTIVES

The UHB will, through appropriate management, and strict application of criteria and controls:-

- Ensure that its registration as a data controller with the ICO is completed on an annual basis, as required, and regularly review the notification to ensure amendments are made promptly as necessary.
- Fully observe the conditions regarding the fair and lawful collection and use of personal information by putting in place an active "fair processing" framework to inform people and patients how their information will be used and disclosed;
- Meet its legal obligations by specifying the purposes for which information is used;
- Collect and process appropriate information only to the extent that it is needed to fulfil the operational needs of the UHB and to comply with any legal requirements;
- Ensure the quality of the information used;
- Apply strict checks to determine the length of time information is held;
- Ensure the rights of people about whom information is held can be fully exercised under the Act. This will include; the individual rights of access to a subject's personal information; the right to prevent processing in certain circumstances; the right to rectify, block or erase information which is regarded as incorrect;
- Take appropriate technical and organisational security measures to safeguard personal information;
- Ensure that personal information is only transferred abroad within the UHB's policies and procedures.

Document Title: Data Protection Procedure	7 of 34	Approval Date: 20 Sep 2016
Reference Number: UHB 350		Next Review Date: 20 Sep 2019
Version Number: 1		Date of Publication: 08 Mar 2017
Approved By: Information Governance Sub Committee		

- Ensure everyone processing personal information understands that they are contractually responsible for following good data protection practice. This includes only viewing personal information where there is a legitimate clinical or administration reason to do so;
- Ensure everyone processing personal information is appropriately trained to do so;
- Ensure there is a procedure for handling subject access requests and queries are managed within the prescribed time period;
- Ensure there is a procedure for undertaking Privacy Impact Assessments to identify and minimise the privacy risks associated with new projects, services or systems;
- Ensure methods of handling personal data are clearly described;
- Ensure the processing and management of personal data is reviewed annually;
- Ensure the UHB is signed up to the Wales Accord for Sharing Personal Information (WASPI) and all Information Sharing Protocols / Data Disclosure Agreements are developed within the WASPI Framework;
- Ensure an annual assessment is carried out on compliance against the Caldicott Principles and standards;
- Ensure that employees and patients are provided with information regarding the purposes for which their personal data is processed;
- Ensure that all forms (automated and manual) used to obtain personal data are not misleading as to the purpose(s) for which the data are to be processed, that they identify the purpose for data being processed and ensure that the specifics of personal data disclosures can be reasonably envisaged by the data subject.

4 MANAGEMENT/EMPLOYEE RESPONSIBILITIES

Chief Executive

Overall responsibility for the UHB's compliance with the DPA rests with the Chief Executive (CE). The CE has delegated responsibility for medical records to the Medical Director (as Caldicott Guardian), and delegated responsibility for non-medical records to the Director of Corporate Governance (as the Senior Information Rights Officer SIRO).

Document Title: Data Protection Procedure	8 of 34	Approval Date: 20 Sep 2016
Reference Number: UHB 350		Next Review Date: 20 Sep 2019
Version Number: 1		Date of Publication: 08 Mar 2017
Approved By: Information Governance Sub Committee		

The Director of Corporate Governance – SIRO

The Director of Corporate Governance has a particular responsibility for ensuring that the UHB corporately meets its legal responsibilities, and for the adoption of internal and external governance requirements.

Medical Director - Caldicott Guardian

The Caldicott Guardian has a particular responsibility for reflecting patients' interests regarding the use of patient identifiable information. The Caldicott Guardian is responsible for ensuring patient identifiable information is shared in an appropriate and secure manner.

Head of Information Governance and Assurance

The Head of Information Governance and Assurance is responsible for the overall development and maintenance of Data Protection and Confidentiality practices throughout the UHB, in particular for raising awareness of confidentiality and the Caldicott principles and promoting compliance with the Data Protection Act Policy and associated procedures to ensure compliance with the Act.

Corporate Governance Senior Information and Communication Manager

Acts as the Data Protection Manager and will be responsible for monitoring, documenting and communicating the UHB's Data Protection Policy and associated procedures relating to DPA, and Information Governance (IG) where relevant to DPA.

This individual will ensure the UHB Notification Registration with the ICO is managed as required.

Provide additional DPA and IG training to staff as required to ensure that employees remain aware of their obligations for compliance with DPA and will have processes in place to ensure that all staff are aware of their responsibilities under DPA.

Ensures that area specific audits are completed and contribute to local audits and those carried out by Internal and District Audit. In addition this individual will also be responsible for overseeing the subject access process in respect of non-health personal records.

Will provide advice and guidance to staff on DPA and where there may be unclear or contentious issues will seek advice from solicitors and the Information Commissioner's Office when required.

All Managers

All Managers will be responsible for ensuring that their staff are aware of the procedures and they abide by the requirements of the procedure and Policy.

Document Title: Data Protection Procedure	9 of 34	Approval Date: 20 Sep 2016
Reference Number: UHB 350		Next Review Date: 20 Sep 2019
Version Number: 1		Date of Publication: 08 Mar 2017
Approved By: Information Governance Sub Committee		

All Managers must ensure that their staff complete the training required for Data Protection and information governance.

Managers responsible for the processing of personal data will ensure that they have registered their processing with the IG Department. Managers will also be responsible for notifying the IG Department of any changes to their processing or of any new purposes for processing.

All Staff

All UHB staff, whether clinical or administrative, who create, receive and use personal/patient identifiable information should be aware of their responsibilities under the Act and should attend appropriate training.

All UHB employees must adhere to the [UHB Consent to Examination or Treatment Policy](#).

Staff are only permitted to process (i.e. access, read, record, disclose) personal data if it is a legitimate part of their job to do so. Employees **are not** permitted to:

- Access their own, a relative's or friend's personal data for their own purpose.
- Access any personal data where it is not a specific requirement of their job to do so.
- Ask someone else who may have access to personal data to access that personal data for them; unless the access is undertaken for an authorised UHB purpose.

The DPA 1998 creates numerous criminal offences for breaching the legislation. These criminal offences can be prosecuted by the Information Commissioner or by the Director of Public Prosecutions. It is unlawful under the Act (section 55) for an employee to knowingly or recklessly, without consent of the UHB, access, obtain or disclose personal data or the information contained in personal data. It is also unlawful for an employee to knowingly or recklessly procure the disclosure to another person of any information contained in personal data, and sell or offer for sale data obtained in breach of the DPA.

Individual employees who process personal data are personally liable for their actions under the Act and may be guilty of an offence or bound by any decision of the Information Commissioner. Additionally, failure by any employee of the UHB to abide by the DPA Policy, these supporting procedures and the requirements of the DPA will be viewed as a serious matter and may result in disciplinary action, including possible dismissal and criminal prosecution.

Document Title: Data Protection Procedure	10 of 34	Approval Date: 20 Sep 2016
Reference Number: UHB 350		Next Review Date: 20 Sep 2019
Version Number: 1		Date of Publication: 08 Mar 2017
Approved By: Information Governance Sub Committee		

Breaches of data security in cases where guidance/policy/procedures have not been followed may expose the UHB/individuals to prosecution under the Data Protection Act 1998 and other legislation, by the Information Commissioner.

The All Wales NHS Employment contract states:

“You must, at all times, be aware of the importance of maintaining confidentiality and security of information gained by you during the course of your duties. This will, in many cases, include access to personal information relating to service users. You must treat all information, whether corporate, staff or patient information, in a discreet and confidential manner in accordance with provisions of the Data Protection Act 1998 and organisational policy”.

5 DISCLOSING PERSONAL DATA

Strict rules and protocols exist around the sharing and disclosure of personal information held by the UHB. Anyone receiving personal information in order to provide care is bound by a legal duty of confidence.

Information **must not** be given to anyone who does not have a specific need for it and who is unauthorised to have access to it. Health professionals must make sure that anyone to whom personal information is disclosed understands that it is given to them in confidence, which they must respect.

When disclosing personal data employees must ensure that the purpose(s), for which the person they wish to disclose to are going to process that data, are compatible with the purpose(s) for which the UHB obtained the personal data (i.e. same or similar reasons).

When disclosing personal data, care must be taken to ensure that we only disclose sufficient personal data to satisfy the purpose of that disclosure (not excessive).

Routine disclosures

These be made as long as the appropriate conditions as contained within schedule two and schedule three (for sensitive information) can be met. Routine disclosures can also be made where such disclosure is complying with appropriate documentation such as:

- Information Sharing Protocol (ISP)
- Data Disclosure Agreement (DDA)
- Data Sharing Agreement (DSA)

Non-routine disclosures

Document Title: Data Protection Procedure	11 of 34	Approval Date: 20 Sep 2016
Reference Number: UHB 350		Next Review Date: 20 Sep 2019
Version Number: 1		Date of Publication: 08 Mar 2017
Approved By: Information Governance Sub Committee		

Non-routine disclosures of personal data to a recipient or third party must not be made unless:

- The data subject has been informed of the disclosure or, the disclosure could be reasonably envisaged by the data subject, as required by the fair processing code, or
- The data subject has consented to the disclosure, or
- There is an exemption within the Act that allows the disclosure to be made (part iv sections 28-36 and schedule 7 of the Act), and in all the above cases.
- It is within your power to make the disclosure.

All non-routine disclosures of personal data must be documented and recorded. More information can be found in the following guidance documents:

[Personal Information Use and Disclosure of and Duty to Share Guidance.](#)
[Confidentiality Code of Conduct](#)

Consideration must also be made to the [Mental Capacity Act](#) when seeking consent.

6 PROCESSING PERSONAL DATA

Department Specific Processing

When departments process data for their specific functions, (e.g. recruitment, staff administration, monitoring, medical purposes, research), individuals must consider the requirements of relevant statutes or codes of practice, as well as the duty of confidentiality, to ensure any data processing undertaken is lawful.

Incompatible Processing

If a data subject's personal data is to be processed for an incompatible purpose (i.e. a different purpose than the original purpose processed) then the data subject's consent will normally be required.

The purpose(s) of all processing, both automated and manual, must be reported to the Information Governance Department to ensure that the processing falls within the UHB's Notification to the Information Commissioner.

The Information Governance Department will provide advice and guidance regarding compliance with 'Processing Purposes', and any further processing of personal data. Where an issue is unclear or contentious, legal advice will be sought from a solicitor or the ICO.

7 USE OF DOCUMENTATION AND FORMS USED FOR OBTAINING PERSONAL DATA

Document Title: Data Protection Procedure	12 of 34	Approval Date: 20 Sep 2016
Reference Number: UHB 350		Next Review Date: 20 Sep 2019
Version Number: 1		Date of Publication: 08 Mar 2017
Approved By: Information Governance Sub Committee		

- All forms (both computerised and manual) used to obtain personal data must comply with the requirements of DPA. Personal information must be adequate, relevant and not excessive, and specifically no unnecessary information to be included.
- Forms will be reviewed by the author and/or responsible manager and will be periodically audited to ensure that the personal data being processed complies with the DPA.
- The IG Department will be responsible for providing advice and guidance regarding compliance with 'Adequate Data'. Legal advice will be sought for any unclear or contentious issues.

8 ENSURING ACCURACY OF DATA

The source of personal data, if not the data subject, must be recorded.

- Whenever personal data is updated the updated information must be communicated to recipients or third parties to whom the data has previously been disclosed or where the processing will have a direct effect on the data subject.
- There must be appropriate plans in place within individual areas to minimise risks of holding inaccurate personal data. Where necessary an appropriate risk assessment must be completed and retained where it is identified that damage may be caused by processing inaccurate personal data. Action plans should be produced to minimise any risks identified in the assessment, to including an area specific protocol for managing the realisation of risks.
- As soon as inaccurate data is discovered, the data must be corrected as soon as the inaccuracy is apparent and the inaccuracy communicated if relevant as above.
- There should be periodic audit completed wherever personal data is processed to ensure compliance with the DPA. There must be robust processes in place for accurate data entry and procedures for ensuring that any systems that exist do not introduce inaccuracies into the data and are robust.

9 RETENTION OF DATA

- Personal information should not be routinely stored indefinitely. Departments and individuals must ensure that they have regular reviews of the information they hold and store in every format and they

Document Title: Data Protection Procedure	13 of 34	Approval Date: 20 Sep 2016
Reference Number: UHB 350		Next Review Date: 20 Sep 2019
Version Number: 1		Date of Publication: 08 Mar 2017
Approved By: Information Governance Sub Committee		

must have regular “culling” of information that is no longer required to be held

- Departments and staff must comply with the UHB [Records Management Retention and Destruction Protocol](#), which supports the Records Management Policy. This protocol has a full records retention schedule which details all the relevant retention periods for documents and records within the UHB. The retention schedule also details the correct method of disposal to ensure compliance with DPA Principle 7 (personal information must be secure).
- When information is destroyed in accordance with the appropriate retention requirement a destruction certificate must be completed and retained indefinitely. The destruction certificate can be accessed from the Records Management Retention and Destruction Protocol.
- All practicable measures must be taken to ensure that personal data, when disposed of, is destroyed to the extent that the personal data cannot be reconstituted.

10 COMPLYING WITH THE REQUIREMENTS OF SUBJECTS RIGHTS

- Individuals have the right to access any personal data that is processed by an organisation subject to any exemptions that may apply. Requests made under subject access rights (Section 7 of the DPA) are set out in the UHB Procedure for Dealing with Subject Access Requests.
- Employees are required to co-operate, without delay, with any subject access requests they are asked to assist with. They must notify the appropriate person of any subject access request received by them, or in accessing data when a subject access request is being processed, to ensure the UHB provides the requested data within 40 days, as required by DPA.
- Staff should not be given access to their own personal files directly, as this could breach the DPA by disclosing the identity of third parties. If staff wish to receive a copy of their personal data they must complete a subject access request form and return it to the IG Department for it to be actioned in accordance with the requirements of the DPA.

Full details can be found in the [UHB Procedure for Dealing with Subject Access Requests](#).

11 SECURITY OF PERSONAL DATA

Document Title: Data Protection Procedure	14 of 34	Approval Date: 20 Sep 2016
Reference Number: UHB 350		Next Review Date: 20 Sep 2019
Version Number: 1		Date of Publication: 08 Mar 2017
Approved By: Information Governance Sub Committee		

- All UHB systems that process personal data automatically, and employees who operate them must comply with the UHB's [IT Security Policy](#).
- UHB employees and agents having access to patient identifiable data (PID), should be able to demonstrate a legitimate care relationship with those patients in the performance of their clinical or other duties on behalf of the UHB and be able to show appropriate authorisation via access control to UHB systems, or under an information sharing agreement with other agencies.
- Where Patient/personal Identifiable Data (PID) is required to be stored, transported or transmitted by legitimate users (as defined above), these users must demonstrate awareness of and compliance with acceptable practice, in accordance with UHB Patient Data Security Guidance Appendix 1 and the [UHB's IT Security Policy](#) and associated procedures.
- Where, in an individual case, adherence to the Patient Data Security Guidance is felt to constrain the business or clinical functions of that service or individual, it is the responsibility of that service or individual to seek a risk assessment by the UHB IT Security staff in order to ameliorate any risk, by encryption or other methods.
- Whilst Appendix 1 specifically applies to patient identifiable data, the Guidance should also be applied, following an assessment of risk, to other personal data; e.g. staff personal data capable of being used for identity theft.
- Employees who process person identifiable data using a computer whilst mobile or off a UHB site must comply with the 'Off-Site/Mobile Computing Policy'.
- All manual personal data must be stored in a secure environment. Manual records of sensitive personal data must be stored in lockable cabinets with restricted access. Sensitive personal data must be locked away when the office is not in use and must not be left on desks overnight or over weekends and holiday periods.
- Members of staff must only access the personal or patient identifiable information that they need in order to do their job. Access to personal data **must be restricted to employees who process the data as part of their duties**, and who have received guidance regarding their responsibilities under the DPA.

Document Title: Data Protection Procedure	15 of 34	Approval Date: 20 Sep 2016
Reference Number: UHB 350		Next Review Date: 20 Sep 2019
Version Number: 1		Date of Publication: 08 Mar 2017
Approved By: Information Governance Sub Committee		

- Employees must take all practicable measures to ensure that personal data, whilst it is being processed, cannot be inadvertently viewed by unauthorised persons.
- Managers should undertake a risk assessment of the damage that may be caused by unauthorised disclosures of personal information. Managers should also ensure action plans are put in place to minimise risks identified in the assessment, including a protocol for managing the realisation of these risks.
- If an employee becomes aware that they have accidentally disclosed personal data to an unauthorised person, they must report this to their Line Manager and the Head of Information Governance. The accidental disclosure will be investigated by the Head of Information Governance, with a view to ensuring that further accidental disclosures can be avoided. Dependent upon the seriousness of the disclosure an incident should be then logged within e-datix and a decision on notification to the Information Commissioner will be made by the Caldicott Guardian or SIRO.
- Any deliberate inappropriate disclosures or breaches of the DPA must be reported via the e-Datix system.
- Members of staff must only access the personal or patient identifiable information that they need in order to do their job.

12 SAFE USE OF FAXES

When sending or receiving personal data by fax machine the following 'safe haven' principles should be followed:

Sending

- Ensure the fax machine displays the correct date, time and department name.
- Always include a fax front cover sheet that does not contain personal data but does provide your name and contact details.
- Ensure that you are faxing to the correct number. If in doubt, confirm.
- Do not walk away while the fax transmits. Remove originals and wait for the confirmation of transmission.
- Ensure the fax will be collected.
- Use the minimum personal data and anonymise the data wherever possible.

Receiving

- Ensure that you are available to receive an expected fax.

Document Title: Data Protection Procedure	16 of 34	Approval Date: 20 Sep 2016
Reference Number: UHB 350		Next Review Date: 20 Sep 2019
Version Number: 1		Date of Publication: 08 Mar 2017
Approved By: Information Governance Sub Committee		

- Do not agree to receive a fax as you leave work or go to a meeting. It will be left unattended.
- Ensure faxes are passed on to the intended recipient. If it is not addressed to you do not read the content.
- If faxes arrive addressed to a person unconnected to you/your department, inform your manager. Do not ignore it.

13 SAFE USE OF E-MAIL

- The transfer of sensitive personal data by email **must only** be sent to/from email addresses ending in @wales.nhs.uk. This remains the policy of the UHB pending the development of secure arrangements by the NHS Wales Information Service (NWIS); however, it is recognised that strict appliance of this can and will put patients at risk in certain clinical and social circumstances.
- In the context of cross boundary services where the risk to a patient's health and wellbeing outweighs the likelihood and severity of a data security breach there might be a need to transfer sensitive personal data via email as the only effective option. Where such **rare** occasions arise, pre agreed arrangements with the Caldicott Guardian can be explored. Only then, on a risk based assessment, the UHB might agree to use email.
- The outcome of the risk assessment will be judged by the Caldicott Guardian and his team, in discussion with clinical colleagues. Where transfer outside @wales.nhs.uk is agreed, the patient must be made aware of the disclosure.
- This is based on the current position where email encryption has not yet been provided for the Digital All Wales Network and where the balance of risk of a data security breach must be struck with the need to ensure the safety of patients. Once an encrypted email service is available, ALL sensitive personal data MUST be sent by this method. Encrypted email (when available) must also be used where any personal data in an email could put the subject at risk; e.g. personal data that could be used for identity theft.
- Whether or not staff believe they have a legitimate requirement to send sensitive personal data and they have a secure method to do so; advice must be sought from the Information Governance Department and/or IM&T Security Manager. This is to ensure that the 'at risk' definitions are met and in general as to whether or not the proposed method complies with the requirements of the Data Protection Act Principles. Advice will be taken from the Caldicott Guardian on individual cases where complex and contentious issues arise.

Document Title: Data Protection Procedure	17 of 34	Approval Date: 20 Sep 2016
Reference Number: UHB 350		Next Review Date: 20 Sep 2019
Version Number: 1		Date of Publication: 08 Mar 2017
Approved By: Information Governance Sub Committee		

- Where personal data is disclosed to a Data Processor or to a service provider (e.g. the repair or maintenance of computer hardware or systems), this must be carried out under a contract (Principle 7, Data Protection Act 1998). The UHB has a "Data Processor Agreement" that **must** be used for this purpose. The Information Governance Department can be contacted for the form.
- In circumstances where regular communication of sensitive information needs to be sent to partner organisations (such as English Trusts/Local Authorities) the Secure File Sharing Portal is available to facilitate such regular communication in a secure manner, however a genuine business need is required for its use.
- Whilst patient identifiable data is allowed to be shared via the portal, staff are not permitted to share any information which may be considered: unlawful, harmful, abusive, harassing, defamatory, obscene, pornographic, libellous, infringes any copyright.

14 DATA PROTECTION ACT BREACHES

- All employees must report breaches of the DPA to the Information Governance Department.
- All personal data security breaches (e.g. lost data, disclosures to the wrong person, unsecure disclosures of data, unauthorised access to data) **must** be reported on e-Datix and investigated by the manager responsible for the data. In addition, breaches must also be reported to the Information Governance Department. All patient identifiable data security breaches must also be reported to the responsible managers Executive Director, the Medical Director and an e-Datix incident completed indicating that it is a Data Protection Breach for review by the Information Governance Department.
- The Medical Director will make any decision on reporting personal data security breaches to the Information Commissioner's Office.
- The Information Governance Department will provide advice and guidance regarding compliance with Data Security.
- The number and type of incidents will form part of the performance reporting criteria to the Information Governance Sub Committee.

15 TRANSFERS OF PERSONAL INFORMATION OUTSIDE THE EUROPEAN ECONOMIC AREA (EEA)

Document Title: Data Protection Procedure	18 of 34	Approval Date: 20 Sep 2016
Reference Number: UHB 350		Next Review Date: 20 Sep 2019
Version Number: 1		Date of Publication: 08 Mar 2017
Approved By: Information Governance Sub Committee		

All personal data that is, or is likely to be transferred outside the EEA must be notified, prior to transfer, to the IG Department.

All UHB employees should note that posting of personal data would constitute a transfer outside the EEA. Where personal data for which the UHB is Data Controller are placed on the internet, the person responsible for placing the personal data on the internet must ensure they have informed consent from the data subject(s) to do so, where required.

16 TRAINING

- All staff must undertake the mandatory training in Information Governance / Information Security and Confidentiality. This training should normally be completed before or at the start of their role. All staff must undertake refresher training in Information Governance / Information Security and Confidentiality every two years.
- Staff must be trained in the processes and use of the information systems they will be required to use, before being provided with access to those systems.
- Training will form part of the individual's objectives or Knowledge and Skills Framework (KSF).

17 AUDIT

These procedures will be subject to periodic review by both internal and external auditors. Any recommendations will normally be implemented after review by either senior IG management, the Information Governance Sub Committee.

18. DISTRIBUTION AND REVIEW

This Procedure will be made available on the UHB Intranet and Internet sites and will be reviewed every three years or sooner if appropriate.

Document Title: Data Protection Procedure	19 of 34	Approval Date: 20 Sep 2016
Reference Number: UHB 350		Next Review Date: 20 Sep 2019
Version Number: 1		Date of Publication: 08 Mar 2017
Approved By: Information Governance Sub Committee		

APPENDIX 1

DATA PROTECTION PROCEDURE

PATIENT DATA SECURITY GUIDANCE		
<p>Personal responsibilities</p> 	<p>- Individuals must be able to justify processing any Patient Identifiable Data (PID) on a laptop or portable media device.</p>	<p>- Processing must be relevant to your job and you must have a legitimate professional relationship with the patient.</p>
<p>- The guidance below details how individuals can store PID safely.</p> <p>- Any processing (using/disclosing/storing) of PID on a PC or Laptop that is carried out and is not covered by the issues below MUST be referred to the IM&T Security Office for Risk Assessment prior to any approval.</p> <p>- If any of the guidance below restricts or prevents current processing of PID and you believe there is a justifiable reason to process the data you MUST contact the Information Governance Department or the IM&T Security Office for advice; you MUST NOT ignore the issues.</p> <p>PID is data that includes any clinical content or identifies that a patient has a particular condition and has enough information to identify patients directly or indirectly. Please contact the Information Governance Department or the IM&T Security Office (details below).</p>		
	Acceptable Practice	Unacceptable Practice 
1 Saving and storage of Patient Identifiable Data (PID)		
<ul style="list-style-type: none"> - All PID data is to be saved and stored to 'H' or 'S' drives or the Clinical Application hosted on the UHB Network. - PID can be stored on the C; drive of a UHB laptop or desktop but requires encryption which will be configured by UHB IT. - Security costs will be included with equipment purchases. - The PID stored locally must be backed up on a regular basis to the UHB Network. 		<ul style="list-style-type: none"> - Saving PID on a 'C' drive of a desktop or laptop (e.g. My Documents) and not encrypted. - Not backing up encrypted PID on a desktop or laptop on a regular basis. - Saving PID to a non-UHB laptop. - Temporary saving PID to a device, pending daily uploading to UHB network, unless a Risk Assessment has been agreed with the IM&T Security Office.
2 Data Sticks and Cameras		
<ul style="list-style-type: none"> - All PID data can only be stored for transfer purposes only on Encrypted Data Sticks and then 		<ul style="list-style-type: none"> - PID transferred on a non-encrypted Data Stick. - Encrypted Data Sticks being used

Document Title: Data Protection Procedure	20 of 34	Approval Date: 20 Sep 2016
Reference Number: UHB 350		Next Review Date: 20 Sep 2019
Version Number: 1		Date of Publication: 08 Mar 2017
Approved By: Information Governance Sub Committee		

✔ Acceptable Practice	Unacceptable Practice ✘
<p>deleted once the transfer has taken place.</p> <ul style="list-style-type: none"> - Images on cameras must be transferred to a UHB server ASAP and the memory card re-formatted. 	<p>for long term storage of PID data.</p> <ul style="list-style-type: none"> - Storing PID on cameras (including mobile phones) and any other personally owned device.
3 Portable media devices. (PDA's / Mobile Phones)	
<ul style="list-style-type: none"> - All PID must be configured to save to the UHB Data Network not the device, see item 10. 	 <ul style="list-style-type: none"> - PID data stored for any period of time on the device's local storage media.
4 Laptop security	
<ul style="list-style-type: none"> - Laptops can only be used by staff the laptop was issued to. - The laptop must be kept secure when not in use. 	 <ul style="list-style-type: none"> - Not complying with items 1 and 2 above. - Using a laptop in a public place without risk assessing the situation.
5 Sending portable media by post (CD's / DVD)	
<ul style="list-style-type: none"> - Only the minimum PID should be sent - All PID data must be encrypted; if not possible, secure packaging and recorded delivery or courier delivery (subject to risk assessment). - In all cases a copy of sign out/sign-received protocol (available IM&T Security Office) must be included with the PID. 	 <ul style="list-style-type: none"> - Sending PID not encrypted - Non-use of protocol. - Sending in a standard envelope by regular (1st/2nd class) post.
6 Patient identifiable data (PID) in email.	
<ul style="list-style-type: none"> - Disclosing PID is allowable, but must be justifiable and can only be sent to email addresses ending in '@.wales.nhs.uk' (see Data Protection Procedure). - An acceptable address would be; joe.bloggs@wales.nhs.uk - Saved emails (.pst files) can only be saved to the UHB network ('P' drive) - An acceptable alternative to email is the Secure File Transfer Portal. Contact the IM&T Security 	 <ul style="list-style-type: none"> - Unacceptable email addresses would include; <p>Joe.bloggs@cardiff.ac.uk</p> <p>Joe.bloggs@cardiff.gov.uk</p> <p>Joe.bloggs@yahoo.co.uk</p>

Document Title: Data Protection Procedure	21 of 34	Approval Date: 20 Sep 2016
Reference Number: UHB 350		Next Review Date: 20 Sep 2019
Version Number: 1		Date of Publication: 08 Mar 2017
Approved By: Information Governance Sub Committee		

✔ Acceptable Practice	Unacceptable Practice ✘	
Manager for details.		
7 Contributing to on-line databases (e.g. a clinical registry).		
<ul style="list-style-type: none"> - All PID remote access must be authorised by the UHB IT Security Manager. - The browser must have a (https://) address. - Compliance with the Data Protection Act 8th Principle (patient consent likely). - Note; it is the 's' in https that denotes a secure site. So, https://wales.healthdept.org is a secure site. 		<ul style="list-style-type: none"> - http://www.cardiff.gov.uk is not a secure site, to send patient information. - http://www.cardiff.ac.uk is not a secure site, to send patient information.
8 Recipients external to the UHB – use of PID		
<ul style="list-style-type: none"> - Recipient must have a legitimate care or research relationship with any patient identified from the data. - Sharing Agreements must be in place where there is a regular flow of PID between the UHB and another organisation. For more information on Sharing Agreements contact the UHB's Caldicot Guardian. - A Duty of Confidentiality is fully understood by the recipient. - No PID further disclosed by recipient without permission (including method of disclosure). 		<ul style="list-style-type: none"> - Storing/processing PID where there is no legitimate relationship with patients. - Recipient using PID in a manner not approved by the UHB (i.e. for a purpose the UHB is not aware of). - Duty of confidentiality not applied to PID. - Insecure disclosure of PID (e.g. email sent over the internet).
9 Access to UHB network by non-UHB staff (e.g. Social Services, Cardiff University)		
<ul style="list-style-type: none"> - Only staff with Honorary contract and/or Confidentiality Agreement in place are able to access UHB PID resources with an approved UHB network account and system account. 		<ul style="list-style-type: none"> - Any other method
10 Remote Access		

Document Title: Data Protection Procedure	22 of 34	Approval Date: 20 Sep 2016
Reference Number: UHB 350		Next Review Date: 20 Sep 2019
Version Number: 1		Date of Publication: 08 Mar 2017
Approved By: Information Governance Sub Committee		

 Acceptable Practice		Unacceptable Practice 
<ul style="list-style-type: none"> - Access to UHB PID resources are acceptable using the following on-line access and configured by IT - 3G Orange - Home-working Secure-id - 'GOOD' software - CISCO ISE - UHB wireless network 	 	<ul style="list-style-type: none"> - Any other method - The use of personal devices to store data, that are not configured by IT
11	PC Disposal	
<ul style="list-style-type: none"> - All PCs and laptops must be disposed in line with UHB policy via the UHB Procurement Department and this service is free. <p>For disposal contact: UHB PC; tel UHW 42795 Cardiff University; tel 01443 434675</p>		<ul style="list-style-type: none"> - PCs and laptops given or sold to anyone. - PCs and laptop left lying around in office's, store rooms etc.
12	Sending of Hard Drives To Third Parties for system maintenance	
<ul style="list-style-type: none"> - Advice must be sought from the IM&T Security Office. - Disclosure subject to a Risk Assessment - See item 5 		<ul style="list-style-type: none"> - Any other method.

Document Title: Data Protection Procedure	23 of 34	Approval Date: 20 Sep 2016
Reference Number: UHB 350		Next Review Date: 20 Sep 2019
Version Number: 1		Date of Publication: 08 Mar 2017
Approved By: Information Governance Sub Committee		

Ann
Morgan

Information Governance
Department

029 2074 4870

Ann.morgan4@wales.nhs.uk
[IG Department](#)

Document Title: Data Protection Procedure	24 of 34	Approval Date: 20 Sep 2016
Reference Number: UHB 350		Next Review Date: 20 Sep 2019
Version Number: 1		Date of Publication: 08 Mar 2017
Approved By: Information Governance Sub Committee		

APPENDIX 2

RELEVANT LEGISLATION AND INFORMATION

- [Data Protection Act 1998](#)
- [WHC \(2000\) 111 'Data Protection Act 1998'](#)
- WHC (98) 90 'The Caldicott Report 1997'
- [The Access to Medical Records Act 1990](#) (where it still applies)
- [The Freedom of Information Act 2000](#)
- [WHC \(2000\) 71 'For the Record'](#)
- [Welsh Assembly Government Confidentiality: Code of Practice for Health and Social Care in Wales \(August 2005\)](#)
- [The Human Rights Act 1998](#)
- [Computer Misuse Act 1998](#)
- Information Security Standard ISO 20071
- [Regulation of Investigatory Powers Act 2000 Telecommunications \(Lawful Business Practice\)\(Interception of Communications\) Regulations 2000](#)
- [Health and Social Care Act 2001](#)
- [The European Data Protection Directive EC 95/46](#)
- Common Law Duty of Confidentiality
- [Information to Share or not to Share](#). Government Response to the Caldicott Review September 2013
- [Mental Capacity Act 2005](#)
- [NHS Act 2006](#)
- [Criminal Justice and Immigration Act 2008](#)
- [Protection of Freedoms Act 2012](#)
- The Medical Record Act Principles
- The NHS Baseline Security Standards
- [Guidance for Access to Health Records Requests](#)

Document Title: Data Protection Procedure	25 of 34	Approval Date: 20 Sep 2016
Reference Number: UHB 350		Next Review Date: 20 Sep 2019
Version Number: 1		Date of Publication: 08 Mar 2017
Approved By: Information Governance Sub Committee		

APPENDIX 3

DATA PROTECTION ACT USEFUL INFORMATION AND DEFINITIONS

1. What are the “Definitions” Under the Act

The Act refers to a number of defined terms:-

Data - Information which is being processed automatically, or forms part of a relevant filing system; it includes information both stored on computer and within manual files.

Personal Data - Data relating to living individuals who can be identified either from that data, or from other information which is either in the possession of or, likely to come into the possession of the data controller. It includes expressions of opinion about the individual.

Sensitive Personal Data - Information about an individual relating to:

- race or ethnic origin;
- political opinions;
- religious beliefs;
- trade union membership;
- physical or mental health or condition;
- sexual life;
- offences or proceedings for any offence committed or alleged to have been committed.

Data Controller - Any person/organisation who determines the purposes, or manner in which, any personal data are to be processed. For the purposes of this organisation the Data Controller is the UHB.

Data Subject - An individual who is the subject of personal data.

Processing - The obtaining, recording, storage, alteration, use, disclosure or destruction of data. The definition is very wide and will cover most situations.

2. What is “Notification” and what does it cover

The UHB is required, in accordance with the Act, to notify the Information Commissioner of the following information, termed in the Act 'the registered particulars'. These are, in relation to the UHB: -

- The UHB name and address,
- a description of the personal data being/to be processed and of the category(s) of data subject to which they relate,
- a description of the purpose(s) for which the data are being/are to be processed,
- a description of any recipient(s) to whom the data controller intends or may wish to disclose the data,

Document Title: Data Protection Procedure	26 of 34	Approval Date: 20 Sep 2016
Reference Number: UHB 350		Next Review Date: 20 Sep 2019
Version Number: 1		Date of Publication: 08 Mar 2017
Approved By: Information Governance Sub Committee		

- the name or a description of any countries or territories outside the European Economic Area to which the data controller transfers or intends to transfer data.

In addition to the registered particulars, the UHB is also required to provide a general description of the security measures taken to protect the personal data.

3. What is “Fair and Lawful Processing” – Principle 1

The DPA requires, in the First Principle, that *"personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless: - at least one of the conditions in schedule 2 is met, and in the case of sensitive personal data, at least one of the conditions in schedule 3 is also met"*.

4. What are Schedules two and three - “Conditions for Processing”?

The conditions set out in Schedules 2 and 3 to the DPA are known as the “conditions for processing”. Organisations that process personal data need to be able to satisfy one or more of these conditions. This will not, on its own, guarantee that the processing is fair and lawful – fairness and lawfulness must still be looked at separately.

The conditions for processing are more exacting when sensitive personal data is involved, such as information about an individual’s health record in such situations. At least one condition in schedule two must be met (to process personal data) and at least one other condition in schedule three must also be met before the processing can comply with the first data protection principle (fair and lawful processing).

One of the conditions for processing of personal data is that the processing is carried out with the consent of the data subject. The EU Directive 95/46/EU defines data subject consent as; *"any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed"*.

5. What are the “Purposes” for processing– Principle 2

The Second Principle of the DPA requires that personal data *"shall only be obtained for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes"*.

6. What is considered “Adequate, relevant and not excessive” – Principle 3

The Third Principle of the Act states that *"personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed"*.

Document Title: Data Protection Procedure	27 of 34	Approval Date: 20 Sep 2016
Reference Number: UHB 350		Next Review Date: 20 Sep 2019
Version Number: 1		Date of Publication: 08 Mar 2017
Approved By: Information Governance Sub Committee		

7. What does “Accurate Data” mean – Principle 4

The Fourth Principle of the DPA states that *"personal data shall be accurate and, where necessary, kept up to date"*.

9. How long should data be kept – Principle 5

The Fifth Principle of the DPA states that *"personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes"*.

10. What are the “rights of data subjects”? – Principle 6

The Sixth Principle of the Act states that *"personal data shall be processed in accordance with the rights of data subjects under this Act"*.

Under DPA an individual, known as the “Data Subject”, has several rights which must be upheld. The DPA provides data subjects with the right to:

- Find out details about data processing – they have the right to know what information about them is being held and what it is being used for.
- Gain access to personal data – they have the right to request access to any personal data an organisation holds about them by making a subject access request (SAR).
- Rectify inaccurate data – they have the right to correct, erase and block (stop processing) of any factual data that is incorrect.
- Object to any automated decision process– they have the right to object against any decision made about them by an automated process i.e. computer system, that significantly affects them.
- Claim compensation – they have the right to claim compensation if damage or distress has been caused by a breach of the act.
- Object to your personal data being used for marketing purposes – they have the right to prevent their information being used for the purposes of marketing.

11. How can we ensure that data is held securely – Principle 7

The Seventh Principle of the Act states that *"appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data"*.

12. Can Transfers be Made Outside the European Economic Area (EEA)

The Eighth Principle of the Act requires that *"personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the*

Document Title: Data Protection Procedure	28 of 34	Approval Date: 20 Sep 2016
Reference Number: UHB 350		Next Review Date: 20 Sep 2019
Version Number: 1		Date of Publication: 08 Mar 2017
Approved By: Information Governance Sub Committee		

rights and freedoms of data subjects, in relation to the processing of personal data."

13. What are the Offences under the Data Protection Act 1998

- It is an offence to process personal data which is not covered by any of the purposes included in the UHB's notification to the Information Commissioner's Office. If an employee has any doubts as to whether any information that they need to process (automated and manual) is of a personal nature and therefore subject to the Act, they should discuss this with the Information Governance Department .
- It is an offence for an employee, without the consent of the UHB, knowingly or recklessly, to: -
 - obtain or disclose personal data or the information contained in personal data, or
 - procure the disclosure to another person of the information contained in personal data.

The Act provides specific exceptions to liability for this offence. The Information Governance Department will provide advice and guidance on the application of these exemptions.

Document Title: Data Protection Procedure	29 of 34	Approval Date: 20 Sep 2016
Reference Number: UHB 350		Next Review Date: 20 Sep 2019
Version Number: 1		Date of Publication: 08 Mar 2017
Approved By: Information Governance Sub Committee		

APPENDIX 4

TEN RULES FOR DATA PROTECTION COMPLIANCE

1. Consent

Wherever possible obtain consent before acquiring, holding or using personal data. Any UHB forms, whether paper or web-based, which are designed to gather personal data should contain a statement explaining what the information is to be used for and who it may be disclosed to.

2. Sensitive data

Be particularly careful with sensitive personal data (i.e. information relating to race, political opinion, physical or mental health, religious belief, trade union membership, sexuality, criminal offences etc). Such information should only be held and used where strictly necessary. Always obtain the consent of the individual concerned and notify them of the likely use(s) of such data.

3. Individual rights

Wherever possible be open with individuals concerning the information being held about them. When preparing reports or appending notes to official documents, bear in mind that individuals have the right to see all personal data and could therefore read any 'informal' comments made about them. Also be aware that this includes e-mails containing personal data and so the same caution should be used when sending e-mails.

4. Review files

Only create and retain personal data where absolutely necessary. Securely dispose of or delete any personal data which is out of date, irrelevant or no longer required. Hold regular reviews of files and discard unnecessary or obsolete data systematically.

5. Disposal of records

When discarding paper records that contain personal data treat them confidentially (i.e. shred such files rather than disposing of them as waste paper). Similarly any unnecessary or out-of-date electronic records should be deleted. Any obsolete UHB computers should have all information stored on it removed or deleted.

6. Accuracy

Keep all personal data up to date and accurate. Note any changes of address and other amendments. If there is any doubt about the accuracy of personal data then it should not be used.

Document Title: Data Protection Procedure	30 of 34	Approval Date: 20 Sep 2016
Reference Number: UHB 350		Next Review Date: 20 Sep 2019
Version Number: 1		Date of Publication: 08 Mar 2017
Approved By: Information Governance Sub Committee		

7. Security

Keep all personal data as securely as possible (e.g. in lockable filing cabinets or in rooms that can be locked when unoccupied). Do not leave records containing personal data unattended in offices or areas accessible to the members of the public. Ensure that personal data is not displayed on computers screens visible to passers-by. Be aware that these security considerations also apply to records taken away from the UHB e.g. for work at home or for an external meeting. Also remember that e-mail is not necessarily confidential or secure so should not be used for potentially sensitive communications.

8. Disclosing data

Never reveal personal data to third parties without the consent of the individual concerned or other reasonable justification. This includes parents, guardians, relatives and friends of the data subject who have no right to access information without the data subject's consent.

Requests for personal information are received from time to time from organisation's such as the police and other government agencies. The UHB will co-operate with these organisation's only after appropriate steps have been taken to ensure that requests are genuine and legitimate.

9. Worldwide transfer

Always obtain consent from the individual's concerned before placing information about them on the Internet (apart from basic office contact details) and before sending any personal data outside the European Union, Iceland, Lichtenstein or Norway.

10. Third party processors

Be aware that if you are using a third party data processor e.g. for bulk mailings or database management and are giving them access to personal data, then there must be a written contract in place to ensure that they treat personal information confidentially, securely and in compliance with the Data Protection Act 1998.

Document Title: Data Protection Procedure	31 of 34	Approval Date: 20 Sep 2016
Reference Number: UHB 350		Next Review Date: 20 Sep 2019
Version Number: 1		Date of Publication: 08 Mar 2017
Approved By: Information Governance Sub Committee		

APPENDIX 5

CALDICOTT GUIDANCE

What is Caldicott?

There was a committee established, chaired by Dame Caldicott, to review the use of patient information in the NHS and the outcome of the review was to recommend seven principles to improve the handling and protection of these records. These are known as the Caldicott Principles and apply to medical records. These principles and the Data Protection Act 1998 enforce strict legal guidelines on the storage, maintenance and access to patient information.

The Freedom of Information Act 2000 and the Information Governance initiative both support the need to maintain the principles of effective confidential data control. While the information management principles are not a legal requirement, they are seen as essential to support the requirements of Data Protection Act.

Confidentiality is part of the day to day activity of all staff who have access to and use personal identifiable information and must be rigorously observed in order to deliver a seamless provision of care.

What are the Seven Caldicott Principles?

1. Justify the purpose(s) of 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
7. The duty to share information can be as important as the duty to protect patient confidentiality

What are the responsibilities for staff within each principle?

Principle 1 - Every proposed use, transfer, sharing or disclosure of personal/patient identifiable information made by staff members must either be required as part of their role or must be part of the responsibilities that they have been expressly authorised to carry out.

Principle 2 – Personal/patient identifiable information items should only be used when there is no alternative. Where possible the NHS number should be used instead of name, address and date of birth or initials and date of birth would also be acceptable

Document Title: Data Protection Procedure	32 of 34	Approval Date: 20 Sep 2016
Reference Number: UHB 350		Next Review Date: 20 Sep 2019
Version Number: 1		Date of Publication: 08 Mar 2017
Approved By: Information Governance Sub Committee		

Principle 3 - Where use of personal/patient identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identification.

Principle 4 - Only those individuals who need access to personal/patient identifiable information should have access to it, in order to undertake tasks within their job role, or tasks which they have expressly been given responsibility for.

Principle 5 - Action should be taken to ensure that staff handling personal/patient identifiable information are aware of their responsibilities and obligations to respect an individual's confidentiality.

Principle 6 – Every use of personal/patient identifiable information must be lawful.

Principle 7 - Professionals should have the confidence to share information where such sharing is in the patient's interests and they should be able to share information within the principles set out within the Caldicott framework with policies to support them.

What is a Caldicott Guardian and who is this?

The Caldicott Guardian is a senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing. Each NHS organisation is required to have a Caldicott Guardian; this was mandated for the NHS by Health Service Circular: HSC 1999/012. In our UHB the Caldicott Guardian is **Dr Graham Shortland** our Medical Director.

What supports Caldicott and is there related legislation?

- The Human Rights Act 1998, which provides a right of respect for private and family life.
- The Data Protection Act 1998, which defines and penalises unlawful processing of information about living individuals.
- The common law duty of confidence, derived from case law rather than statute. This provides individuals with a qualified right to prevent unauthorised disclosure of information concerning them, when it was provided in confidence, for example, to a social worker.

Together with the above legislation, the seven Caldicott Principles form the basis of best practice in information management. They also allow for the secure transfer of sensitive information amongst professionals within the social care service and across partner agencies.

Document Title: Data Protection Procedure	33 of 34	Approval Date: 20 Sep 2016
Reference Number: UHB 350		Next Review Date: 20 Sep 2019
Version Number: 1		Date of Publication: 08 Mar 2017
Approved By: Information Governance Sub Committee		

What is Personal Identifiable Information?

The Caldicott Committee identified key items of information, which could be used to establish the identity of a service user:

1. National Identifier, such a National Insurance Number or NHS Number.
2. Local Identifier, such as CRN or Hospital number.
3. Name.
4. Address.
5. Post Code.
6. Date of Birth.
7. Other Dates, such as Date of Death.
8. Sex.
9. Ethnic Group.
10. Occupation.
11. Information that relates to a service user, which can be used to identify them (for example, the name of their Advocate).
12. The information in question and other information held, or are likely to hold.
13. Any expression of opinion about the service user.
14. Indications of individuals' intentions in respect of the service user (that is if a connection can be made between the information in question and the service user).
15. Images of the service user, for example, via a CCTV camera.
16. An e-mail address, where its format is sufficient to carry enough detail about a service user.
17. Any combination of information that could lead to the identification of a service user(s), (for example, a street name and surname).

Where can I find more information or ask for advice

Further advice and information can be obtained from the Information Governance Department
1st Floor Monmouth House
University Hospital of Wales
Heath Park
Cardiff

Head of Information Governance and Assurance

Marie Mantle (marie.mantle@wales.nhs.uk)
Tel 02920 743747

Corporate Governance Senior Information and Communication Manager

Ann Morgan (ann.morgan4@wales.nhs.uk).

Document Title: Data Protection Procedure	34 of 34	Approval Date: 20 Sep 2016
Reference Number: UHB 350		Next Review Date: 20 Sep 2019
Version Number: 1		Date of Publication: 08 Mar 2017
Approved By: Information Governance Sub Committee		

Tel 02920 74870

Information Governance Officer

Vanessa Clement-Pugh (vanessa.clement-pugh@wales.nhs.uk).

Tel 02920 745624

Information Governance Co-ordinator

Denise Gulley (denise.gulley@wales.nhs.uk)

Tel 02920 745625