Appropriate Policy Document
Schedule 1 Part 4 Data Protection Act 2018

This document meets the requirement for an Appropriate Policy Document (APD) to be in place when processing special category (SC) and criminal offence (CO) data under certain specified conditions.

2.1 Conditions relating to employment, health and Research

Employment, social security and social protection:

- Processing personal data concerning health in connection to the UHB's rights under employment law
- Providing human resources and occupational health facilities for employees
- Processing data relating to criminal convictions in connection with recruitment, discipline or dismissal

2.2 Substantial public interest condition

Equality of opportunity or treatment:

- Ensuring compliance with our obligations under legislation such as the Equality Act 2010 and Sex Discrimination Act 1970

Preventing fraud:

- Disclosing personal data in accordance with the Cabinet Office's National Fraud Initiative

Safeguarding of children and of individuals at risk:

- To assess and evaluate safeguarding concerns so that we can work effectively with NHS partners and other agencies to help promote the welfare of children or adults and to protect them from abuse and neglect

Disclosure to elected representative:

- Providing information to elected representatives such as Members of Parliament in response to a data subjects request for assistance

Procedures for securing compliance:

Article 5 of the General Data Protection Regulation sets out the data protection principles. These are our procedures for ensuring we comply with them:

Principle 1 – Lawfulness, fairness and transparency

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. The UHB will:

- ensure that personal data is only processed where a lawful basis applies and where processing is otherwise lawful
- only process personal data fairly and will ensure that data subjects are not misled about the purposes of any processing
- ensure that data subjects receive full privacy information so that any processing of personal data is transparent

Principle 2 – Purpose limitation

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with the purposes. The UHB will:

- only collect personal data for specified, explicit and legitimate purposes and will inform data subjects what those purposes are in a privacy notice
- not use personal data for purposes that are incompatible with the purposes for which it was collected. If personal data is used for a new purpose that is compatible we will inform the data subject first

Principle 3 – Data minimisation

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. The UHB will:

- only collect the minimum personal data that is needed for the purposes for which it is collected
- ensure that the data we collect is adequate and relevant

Principle 4 – Accuracy

Personal data shall be accurate and where necessary, kept up to date.
The UHB will:

- ensure that personal data is accurate and kept up to date where necessary. We will take particular care to do this where our use of the personal data has significant impact on individuals.

Principle 5 – Storage limitation

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. The UHB will:

- only keep personal data in identifiable form for as long as is necessary for the purposes for which it was collected or where we have a legal obligation to do so. Once we no longer need the data it shall be deleted or rendered permanently anonymous.

Principle 6 – Integrity and confidentiality (security)

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing against accidental loss, destruction or damage, using the appropriate technical or organisational measures.
The UHB will:

- ensure that there are appropriate technical or organisational measures in place to protect personal data.

Accountability principle

The data controller shall be responsible for and be able to demonstrate compliance with these principles.
The UHB information Governance team are responsible for ensuring the UHB are compliant with these principles. The team will:

- ensure that records are kept of all personal data processing activities and these are provided to the Information commissioner on request
- enable completion of Data Protection Impact Assessments for any high-risk personal data processing and consult the Information commissioner if appropriate
- have appointed a Data Protection Officer to provide independent advice and monitoring of the UHB's personal data handling and that this person has access to report to the highest management level
- have in place internal processes to ensure that personal data is only collected, used or handled in a way that is compliant with data protection law.

Retention and erasure of personal data
We will ensure, where special category personal data is processed that:

- there is a record of that processing and that record will set out, where possible, the envisaged time limits for erasure of the different categories of data
- where we no longer require special category data for the purpose for which it was collected, we will delete it or render it permanently anonymous

- data subjects receive full privacy information about how their data will be handled and that this will include the period for which the personal data will be stored or if that is not possible, the criteria used.

For further information about Cardiff and Vale University Health Board's compliance with Data Protection law, please see our Patient Privacy Notice, Privacy Notice for All Workers and Employees or contact us via email.