



GIG  
CYMRU  
NHS  
WALES

Bwrdd Iechyd Prifysgol  
Betsi Cadwaladr  
University Health Board

## Data Security and Confidentiality Agreement

(This applies to all individuals working for or on behalf of Betsi Cadwaladr University Health Board (BCUHB), and will include non-fixed contracts, agency, volunteers, temporary personnel including students, work placements/work experience etc)

In the course of your work with BCUHB you may come across, or have access to, sensitive and confidential information concerning patients, staff, the business of the organisation and other third parties.

Everyone has the right to expect their information to be dealt with the highest possible level of confidentiality. In dealing with this type of information you must work within the Health Board's policies and procedures (in particular IM&T Security, Data Protection and Confidentiality Code of Conduct).

These can be found on the policies and procedures [intranet](#) site or obtained from your supervisor / line manager (i.e. the person you are reporting to). In addition to these, this document sets out the Health Board's expectations with regard to confidentiality of information, your responsibilities and consequences of a breach of confidentiality. This agreement must also be read in conjunction with the Health Board's Raising Staff Concerns/Whistle Blowing Policy.

### Confidentiality – General Guidelines

- The Health Board processes personal data about patients, staff and other third parties, as well as business sensitive information such as financial or contractual information. If you have any doubts about the confidentiality of information, regard it as confidential unless you are advised otherwise by your supervisor / line manager. If your supervisor is not available then you should contact a member of the [Information Governance Team](#).
- You must not use any personal or business sensitive data you come into contact with or as part of your duties, for any reason other than as part of your job role.
- You must not reveal or disclose personal or business sensitive data to friends or relatives.
- You must not discuss patients with their friends or relatives without patient consent.
- Care must be taken to respect confidentiality if discussing individuals in public areas.
- You must not reveal or disclose personal or business sensitive data to any individual or agency (including via social media) without the permission of your supervisor / line manager.
- Access to a patient's medical record is restricted to relevant hospital staff dealing with the patient's care.

- Enquiries from the press / media seeking information should be directed to the [Communications Team](#). If the enquiry is made out of hours you must contact the administrator on call for the Health Board area.
- Enquiries from the Police seeking information should be directed to your supervisor / line manager or a member of the [Information Governance Team](#). If the enquiry is made out of hours you must contact the administrator on call for the Health Board area.
- The identity of all callers must be verified. Request a telephone number so that a staff member can return their call.
- You must not download any personal or business sensitive data onto personal devices such as USB sticks, phones, cameras, laptops etc.
- You must not allow individuals to be identified during training or other health service activities e.g. only dummy data should be used when demonstrating a system for training purposes.
- Your duty of confidentiality continues to apply indefinitely even after your work with the Health Board has ceased.
- All confidential records, including computerised material, documents and other papers, together with any copies or extracts thereof, made or acquired by you in the course of your placement shall be the property of the BCUHB and must be returned on the subsequent cessation of your placement.
- You must complete BCUHB's Information Governance training or provide evidence that you have completed confidentiality training elsewhere.

### **General Legal and Professional Principles**

Data Protection legislation, Human Rights Act 1998 and the Common Law Duty of Confidentiality all refer to the protection of privacy and confidentiality. You will be required to adhere to this legislation at all times.

Patient data is defined under Data Protection legislation as “special category data” and additional specific conditions covering its use exist. Obtaining or disclosing such information without appropriate authority is a criminal offence.

You should be aware that you will be personally liable for any contravention of the above legislation and that the duty of confidence lasts indefinitely.

All requests for copies of information should initially be discussed with your supervisor / line manager or a member of the [Information Governance Team](#).

**The Computer Misuse Act 1990** establishes three offences which refer to unauthorised access, either casually or for a more sinister purpose, to the modification of information and introduction of malicious programmes:

1. It is an offence to knowingly cause a computer to perform any function with intent to secure unauthorised access to any programme or data held in any computer;
2. An offence under point 1 is committed with the intent to commit or facilitate a further offence, whether by the offender or by another person;
3. Knowingly to do any act which causes an unauthorised modification of the contents of any computer; to impair the operation of any computer; to prevent or hinder access to any program or data held and to impair the operation of the program or the reliability of the data.

### **Breaches of Confidentiality**

- You must be aware that unauthorised access to, modification, or disclosure of information held by the Health Board is strictly forbidden and attempts to do so will result in the immediate termination of your placement.
- In addition, serious breaches of confidentiality involving personal data may lead to prosecution under Data Protection legislation.
- Any breaches made by those on work experience may be reported to the relevant education establishment.

Any concerns you have in respect of any of the above issues should be raised with your supervisor / line manager (or the person you are reporting to), or a member of the [Information Governance Team](#).

### **Acceptance**

I confirm that I have read and understood all of the above statements and agree to adhere to them to ensure the confidentiality of information at all times within Betsi Cadwaladr University Health Board.

I also understand that any failure to adhere to these rules could result in further action being taken against me.

Signature	Date
Print Name	Department