GIG CYMRU NHS WALES
Bwrdd Iechyd Prifysgol
Betsi Cadwaladr
University Health Board

Data Security and Confidentiality Agreement

(For Staff not covered by a professional body for example Non-fixed Contracts, Agency, Volunteers or Temporary Personnel including Students, Work Placements/Work Experience)

In the course of your placement with Betsi Cadwaladr University Health Board (BCUHB) you may 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 his/her information to be dealt with the highest possible level of confidentiality. In dealing with this type of information you should work within the Health Board's policies and procedures (in particular the IM&T Security, Data Protection and the Confidentiality Code of Conduct). These can be found on the Health Board's policies and procedures intranet site or obtained from your supervisor/line manager (or the person you are reporting to). In addition to these policies, this document explains the Health Board's expectations with regard to confidentiality of information, what your responsibilities are and what consequences a breach of confidentiality may be applied. This agreement must also be read in conjunction with the Health Board's Raising Staff Concerns/Whistle Blowing Policy.

Confidentiality – General Guidelines

- Information which the Health Board holds includes patient, clinical, financial employee or contractual details. This list is not a definite list and therefore if you have any doubts about the confidentiality of information it must be regarded as confidential unless you are advised otherwise by your supervisor/line manager. If your supervisor is not available then you should contact either the Caldicott Guardian/Data Protection Officer or a member of the Information Governance Team.

- You must not use any personal, sensitive or patient identifiable information you come into contact with or as part of your duties, other than as part of your job role.

- You must not reveal or disclose personal, sensitive or patient identifiable information to friends or relatives.

- You must not discuss the patient with his/her friends of relatives without the patient's consent.

- You must not discuss individual patients with another member of staff in patient areas.

- You must not reveal or disclose personal, sensitive or patient identifiable information to individuals, people making inquiries, or other agencies without the permission of your supervisor/line manager. (This includes not disclosing/discussing information on social network sites).

- Access to a patient's medical record is restricted to relevant hospital staff dealing with the patient care.

- Enquiries from the press or police seeking information should be directed to your supervisor 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 should be checked. Ask for a telephone number so that they can be called back by the person to deal with the enquiry.

- You must not download any information onto personal devices such as USB sticks, phones, cameras etc.

- You must not allow individuals to be identified during training or other health service activities.

- This duty of confidentiality continues to apply indefinitely to deceased patient information.

- 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.

- This duty of confidence will continue indefinitely following completion/end of your placement.

General Legal and Professional Principles
The Data Protection Act 1998, 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.

The Data Protection Act covers the processing of personal data on living individuals held in any form, for example paper (health records) computer records, audio and video tapes. This act requires that data is 1) processed fairly and lawfully; 2) processed for a specified purpose; 3) adequate, relevant and not excessive; 4) accurate and up to date; 5) not held for longer than necessary; 6) processed in accordance with the rights of the data subject; 7) kept secure against unauthorised access, alteration, disclosure or destruction and 8) is not transferred outside the European Economic Area (EEA) unless adequate safeguards exist.

Patient information is defined under the Data Protection Act as “sensitive data” and additional specific conditions covering its use exist. Obtaining or disclosing such information without appropriate authority is a criminal offense.

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 and/or even prosecution.

- In addition, serious breaches of confidentiality involving personal and sensitive personal information may result in legal proceedings being instigated under the Data Protection Act 1998.

- Any breaches made by those on work experience may be reported to the relevant education establishment.

Further Guidance

Any concerns you have in respect of the above issues should be raised with your supervisor/line manager (or the person you are reporting to), the Caldicott Guardian/Data Protection Officer or a member of the Information Governance Team.

Acceptance

I confirm I have read and understood the above statements and agree to adhere to the guidelines regarding the confidentiality of information 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