Staff Agreement –
Confidentiality of Patient & Other Personal Information and Appropriate Use of ADHB Systems & Technology

Introduction

In the course of carrying out your duties you are likely to have access to systems containing a broad range of patient and other personal information. All ADHB staff/contractors are therefore in trusted positions, and are expected to perform their duties responsibly. These duties include upholding the law by meeting the requirements of the Privacy Act 1993 and the Health Information Privacy Code 1994, and complying with ADHB Policy with respect to how patient and other personal information is managed, and appropriate use of ADHB's systems and technology.

ADHB's Obligations Under the Law

According to the Health Information Privacy Code 1994, ADHB must ensure that patient information is protected against access, use, modification or disclosure by anyone, other than for patient care or other authorised purposes. We must also ensure that if health information is used for authorised purposes other than patient care, then wherever possible the information must be used in a form in which individual patients are not identified, and should not be published (i.e. printed) in a form that could identify individual patients. Patients have a right to expect their information will be managed appropriately.

To ensure compliance with the law, the Board Policy on Access to Patient Information states that "*Only those staff members involved in the care and treatment of a patient may have access to that person's clinical records*". This Policy also states that any staff wishing to view their own clinical records should request to view their records. Furthermore, the Board Policy Legal Issues Related to Children in Hospital states that parents and guardians must officially request access to the clinical records of their children, and that "*parents and guardians do not have an automatic right to access their child's clinical records*".

Expectations of All Staff/Contractors

ADHB accepts that you will need to access/use patient and other personal information at times to perform your duties; however this does not entitle you to access/use patient information beyond the specific requirements of your job. You are expected to observe ADHB policy at all times. Any misuse of ADHB's information systems will be regarded as a breach of ADHB Policy which could result in disciplinary action, including termination of employment/contract. Regular audits are conducted on ADHB's information systems to identify potential breaches of ADHB Policy (including inappropriate access to patient information), and all staff are subject to systematic audit on a regular basis. Internet use (including sites visited) is also monitored on a regular basis and any inappropriate Internet use will have Internet access for that user removed without notice.

All staff/contractors are expected to comply with the following:

a) You must never share your logons/passwords with others.
b) You will be held accountable for all transactions that occur in any of ADHB's information systems that used your logon/password.
c) You must only ever access information in ADHB's information systems (including all test, training, development and production systems) for the purpose of performing the specific duties associated with your job.

…/continued

d) If you require access to your own or your child's clinical record, you must contact the Release of Information staff in the Clinical Record Department for assistance.
e) If your job requires you to access the clinical record or any other information pertaining to a patient with whom you have a personal relationship (e.g. a relative or a friend) it is recommended that you ask another staff member to perform the duties associated with accessing the clinical record/information, rather than you accessing the clinical record/Information yourself. Please seek advice/support from your team leader or manager regarding this.
f) You must always act in accordance with ADHB Policy with respect to email and Internet use, information systems security, and computer software licensing.
g) If Internet access has been authorised by your manager, you are expected to read and comply with the ADHB Policy on 'Internet Use' at all times. Your key responsibilities are to ensure that:
   - anti-virus software is installed on the PC and your login script participates in the automatic update upon login to the domain
   - software downloaded from the Internet is licensed as per the ADHB Computer Software Licence Policy
   - any software installed on the PC as a result of being downloaded from the Internet, or software that comes from an external supplier that does not have the approval of Information Management & Technology Services and causes the PC to malfunction, fail or require rebuilding will incur the following
     - the software will be removed in the first instance to see if that removes the fault
     - if the PC requires a rebuild of operating system and application software, the RC responsible for the PC will be charged $500 and the job will attract lower priority over urgent support work.

ADHB Management recognises that staff with access to the Internet may use this resource for private use. While incidental private use is acceptable, excessive private use is not (refer to the Internet Use Policy for more information re the definition of Unacceptable Use).

Note that browsing of Internet sites that contain sexually explicit material or would contravene the ADHB Sexual Harassment Policy is disallowed. Internet use (including sites visited) is monitored on a regular basis and any inappropriate Internet use will have Internet access for that user removed without notice, and could result in disciplinary action, including termination of employment.

Agreement

I have read and understood the information above and agree to comply with the expectations stated of me as an ADHB employee/contractor with respect to maintaining the confidentiality of patient and other personal information, and complying with ADHB Policy at all times.

_____	_____	_____
(Signature)	*(Printed Name)*	*(Date)*
_____	_____	
(Job Title)	*(Department)*	

This document will be retained in the employee's personal file.