OTAGO MEDICAL SCHOOL
Te Kura Hauora o Ōtākou

Guidelines on Maintaining Confidentiality of Clinical Material

Health professionals, including medical students, have privileged access to patient information, all of which is confidential. Inappropriate release of such information is unlawful under the Privacy Act. This information may be inadvertently released through theft or loss of this material. You are obliged to minimise this risk. The following is intended to assist you in this.

The Code of Professional Conduct for Medical Students at the University of Otago includes:

5. Maintaining patient confidentiality:

Patient information is confidential. Disclosure without the patient's permission or other justification is inconsistent with the trust required in medical practice and has the potential to cause harm. Patient information may be discussed with peers and professional staff who are directly involved in the care of that patient, and, on occasion, with colleagues in a setting where confidentiality is protected.

As a medical student I will:

5.1. Hold all patient information in confidence, including when the patient has ended treatment or died.
5.2. Respect a patient's right to determine who should be provided with their personal information.
5.3. Not remove or copy patient-related material without specific permission, and handle such material in accordance with 5.4.
5.4. Ensure that all my documents and images containing patient information are de-identified, kept in a secure place in a way that prevents unauthorised access, and securely destroyed when no longer required.
5.5. Become aware of the limited circumstances in which breaches of confidentiality may be justified.
5.6. Not access patient information unless I am directly involved in their care, or have a legitimate reason and permission from those authorised to do so.

For even greater clarity in relation to 5.4, this means that you must ensure that you protect the confidentiality of any patient data that you may be using, for example to write up a case history or other clinical presentation. Remember that bags, laptops, and other portable media can be lost or stolen. Such events are personally distressing to you, but if someone's confidential information becomes public knowledge this is very distressing for them and will lead to formal inquiries into how this came to occur, with implications for the person who lost the data, the medical school and the health care providers. It should be remembered that breaches of confidentiality might seriously damage trust between the patient and the individual, and the standing of the profession.

Remember also that confidentiality can be breached by discussion of a patient, or their details, outside a specific clinical setting. It is not acceptable to discuss patient information in the cafeteria or any other social settings.

This guideline focuses on maintaining confidentiality of paper and electronic records.

Preventative steps

Do not include identifying data on case histories. Do not record names, NHI numbers, or dates of birth in these case histories – Ms. A, age x years is sufficient. If this information is later stolen, it goes some way to protecting the individual patient's data.

You may be required to separately identify the patient whose illness you are documenting and when you saw them, but do this on a separate piece of paper/file, kept separately (and securely) from the other notes.

You should never copy or take images of case records. Investigation results should not be copied unless there is a particular reason to include an image of an ECG, X-ray or similar. If you do this, make sure the image does not include identifying data about the patient.

The photographic, video or audio recording of patients should not be undertaken unless explicitly directed by teaching staff and undertaken in full accord with University and health provider policies.

Security

Paper records

Make sure any paper notes are kept securely, you know where they are, and that you keep that place locked. If you are in a shared flat, that means at least keeping them in a locked drawer. Once you no longer need them, ensure their secure destruction in a shredder or secure destruction bin in the hospital or medical school.

Electronic records

If you are recording confidential patient information on a computer, such as when writing up a case history, make sure the file is password protected, using a strong password. For information on strong passwords, see: the University ITS webpage on creating strong passwords

In addition, you are strongly encouraged to have password protection on all electronic devices (including web-based storage) where you store or backup confidential data.

Encryption of your hard drive and any electronic devices containing sensitive information (back up drives, portable media memory sticks, CDs, DVDs, back up drives, etc) is also encouraged. For information about encryption, See: the University ITS webpage on encrypting files

As soon as you no longer need the confidential material, you are required, under the Privacy Code, to destroy it. Remember that merely deleting a file from your hard drive does not erase it; it only removes the file name from the directory. To erase the file, select the 'secure empty trash' option from the Finder menu (within the Finder window) on a Mac, or for a PC running Windows there are a number of tools available, which can be used.

After Theft/Loss

If you find that despite these measures you have had confidential data *stolen*, you should contact the police. You should also contact the Student Affairs office.

If you have *lost* confidential material, contact the Student Affairs office as soon as possible.