

POLICY and PROCEDURE

| | | |
|------------------------|---|------------------------------------|
| Title: | Electronic Patient Files – Management of | No. 18 |
| Area: | Clinic | |
| Date Effective: | 1/7/2017 | Date Ratified: 1/7/2017 |
| Date Reviewed: | 1/11/2020 | Next Review Date: 1/11/2023 |

Purpose:

- To ensure total confidentiality of personal and clinical information in accordance with the Privacy & Personal Information Act 1998 and Health Records & Information Privacy Act 2002.

Policy:

- Patient or client information is any information about a patient or client, whether they are identifiable from that information or not, and includes but is not limited to:
 - Clinical records of patient history, examinations performed, diagnoses, and treatment implemented
 - Correspondence between health care providers
 - Photo, video or audio recordings
 - Results of assessments (e.g. Xray images, pathology)
- No identifiable patient / client information is to be unattended or stored in any other format except in the designated clinic secured filing systems. Currently this is Best Practice (BP) for general practice (GP) and Visual Outcomes (VO) for Access & Inclusion, allied health and student-led clinics. It is inappropriate to store identifiable information in any other program or system. E.g. Patient/client information **MUST NOT** be saved to desktop or in personal files.
- **De-identified** patient/client information may be used for the following purposes, provided the client has provided written consent for the specific purpose on their intake form or in a subsequent consent form, and this consent has not been withdrawn:
 - Teaching students from any discipline within the clinical environment
 - Teaching students from any discipline in a non-clinical environment, including in lectures, tutorials etc.
 - Use in learning materials, which can be distributed to students using electronic or physical means, including via blackboard, USB, email
 - Use in student assessment (e.g. assignments or case studies presented by students, examinations)
 - Use in third party cloud based analysis applications where access is limited to staff or students of SCU who are inducted to the clinic, but can be accessed outside of the clinical environment (e.g. SiliconCoach Live)
 - Use in research. This does not negate the need for appropriate ethical approval.

- Patients have a right to refuse to provide consent for their information to be used for any or all of the purposes listed in the above paragraph and can revoke their consent at any time.
- Any information gathered via photography, video or voice cannot be shared on any social media platforms and only used for the above identified applications as the patient provides consent for.
- Capturing recordings:
 - Patient recordings (including photography, videography or audio recordings) must be captured using equipment that is the property of the clinic or school.
 - Personal equipment of clinical educators may only be used if:
 - Equipment of the clinic or school cannot be used to capture the recordings (e.g. technical limitations, access to equipment), and
 - Written authorisation is provided in advance by clinic management, and
 - The information is deleted from the clinical educator’s equipment immediately following transference of recordings to clinic storage.
 - Personal equipment of students must not be used to capture recordings.
- If it is not possible to reasonably de-identify a recording, it should not be used outside of the clinical environment.
- If there is a need for de-identified patient/client information to be re-identifiable, the recordings should be marked with the client’s Visual Outcome User ID.

Procedure:

- If notes are made in a program other than Visual Outcomes, they need to be printed, deleted and then scanned into Visual Outcomes to be attached electronically to the client’s health file. Only then is that information automatically saved and encrypted by the University Information Technology department in accordance with the Health Clinic’s obligations.

De-identification

- De-identification involves removing or altering identifying information until the patient or client is no longer be identifiable or reasonably identifiable from the remaining information. The patient or client is “reasonably identifiable” if, with the assistance of other information sources (whether these are Health Clinic information sources or not), their identity can be determined from the information.
- Generally, de-identification includes two steps
 - removing personal identifiers, such as an individual’s name, address, date of birth or other identifying information, and
 - removing or altering other information that may allow an individual to be identified, for example, because of a rare characteristic of the individual, or a combination of unique or remarkable characteristics that enable identification.

- If recordings are to be de-identified for an approved purpose:
 - Capture as little identifiable information as possible when making the recording. E.g: Avoid including identifiable features in images/video: face, birthmarks, tattoos, work uniforms. Avoid using client full name in audio or video recordings etc.,
 - Recordings may be digitally altered within the clinic to further reduce identifiable information.

Supervisors and mentors are responsible for implementing this policy.

YOUR PERSONAL SAFETY SHALL BE THE PRIORITY AT ALL TIMES

Related Legislation:

Infection Control AS4187
Workplace Health & Safety Act 2011
National Safety & Quality and Health Service
Standards
Privacy & Personal Information Act 1998
Health Records & Information Privacy Act 2002

Reference / Consulting Body:

Clinic Operations Meeting
Clinical Governance Committee