Southern Cochlear Implant Programme

Health Information Privacy Policy

Introduction

The aim of this Policy is to set out in summary form some of the main aspects of our health information privacy policies and procedures.

Our team will understand, comply with and implement the privacy policy and procedures as outlined in the Policy Statements below and in the attached documents which state the processes to be followed by the staff in handling health information.

"Health information" relates to the health information of identifiable patients, including:

- information about a patient's health, medical and treatment history;
- information about an individual collected before or in the goods, services and facilities provided to a patient where the services purport to improve or protect a patient's health;
- information collected before or in the course of, and incidental to provision of any health service to a patient information relating to and contact with any health or disability service providers and information about donations of blood or organs.

Health information does not apply to anonymous or aggregated statistical information where individuals cannot be identified.

SCIP will ensure that:

- SCIP will collect, store, and use health information in a manner that complies with the Health Information Privacy Code 1994 and will collect, store, and use personal information in a manner that complies with the Privacy Act 1993.
- SCIP complies with the Health Information Privacy Code 1994 when destroying health information and the Privacy Act with personal information.
- SCIP complies with Health Information Privacy Code 1994 requirements when correcting and disclosing health information.
- SCIP will follow the procedures set out in this Policy when dealing with requests for information.
- SCIP will ensure confidentiality of information.
- SCIP will follow the procedures set out in this Policy to deal with transferring patients' information.
- SCIP will display a privacy poster in the waiting room.
- SCIP will make available a brochure relating to privacy for patients on request.
- All staff will have adequate training to ensure they comply with Privacy legislation.
- The appointed privacy officer is responsible for monitoring privacy issues and acting on feedback from clients (referred to as "patients") and staff.

Privacy Officer

SCIP will have a Privacy Officer who has received training and is aware of their responsibilities.

The Privacy Officer is the General Manager.

- The Privacy Officer is responsible for: Ensuring that SCIP complies with the Privacy legislation in relation to employees, and any individual contractors, and the Health Information Privacy Code 1994 in relation to patients; and
- Dealing with requests made to SCIP about personal or employment information; and
- Working with the Privacy Commissioner or investigating officer should the need arise.

Privacy Officer Responsibilities:

The responsibilities of the Privacy Officer include:

- Ensuring that SCIP has the required privacy policies and procedures up-to-date and stored in a readily accessible format (electronic or Privacy Folder).
- Ensuring that all team members have read and understood the policies and procedures and have updated their personal training record to that effect.
- Be available to answer questions relating to privacy issues and know when to refer queries and problems.
- Briefing SCIP team on changes to processes.
- Alerting SCIP team to privacy complaints received and what will be done to prevent the same thing happening again.
- Up-skilling SCIP team on workshop information /case studies (i.e. providing training in staff team meetings).
- Organising any external training as the Privacy Officer sees fit.
- Overseeing the Orientation (privacy) process.
- Advising management or the Board of Trustees about recommended training opportunities to up skill the team.
- Ensuring training records are up to date.
- Ensuring that the privacy complaints received are dealt with in the correct manner.
- Ensuring that there are clear guidelines on who can access patient information and that handling health information is done according to SCIP policies and procedures.
- Liaising with audiologists and other members of management regarding any privacy concerns and implementing changes to promote health information privacy.

Collection of Health Information

When collecting health information from patients, SCIP must:

- Only collect the information for the purpose of treating the patient or for some other necessary and legal purpose. Purposes include recording and providing the care, treatment and safety of patients for their benefit and the benefit of others; administration, promotion, marketing, business and financial reasons; teaching, training and education; research and development; monitoring patient care, treatment and health status; plan for and fund health services; publication of scientific literature; inform organisations associated with the performance of cochlear implants; and for statistical purposes.
- Collect the information directly from the patient unless SCIP believes on reasonable grounds, that one of the other exceptions to this (rule 2 of the Code) applies. An exception includes where SCIP has reasonable grounds to believe that the patient has authorised collection of the information from

someone else, such as a referral from a health/educational provider, or where the patient is under the age of 16 and collection is from the patient's representative; and

- Tell the patient that the information is being collected, give the patient reasons/purpose for SCIP collecting the information, whom will have access to the information, the name and address of the health agency collecting the information and the agency holding the information, whether or not the information is voluntary or mandatory (and if mandatory, the law requiring the information), the consequences for the patient if the information is not provided, and that the patient is entitled to access and correct the information. This should be provided on forms provided by SCIP prior to the patient consenting to our health services.
- Generally, we do not need to tell patients the above where staff have collected the same type of information from them before.
- Only collect health information by lawful means that in the circumstances are fair and do not intrude to an unreasonable extent upon the patient's personal affairs.

To inform patients about the fact we collect information, we ensure that we have a Privacy poster displayed in a prominent place on the waiting room notice board.

Storing Health Information

We ensure that the health information held by our programme is stored securely so that it cannot be accessed, lost, modified, disclosed, misused or used by unauthorised people. For example:

- Paper records are stored in the filing cabinets in the reception area away from public access. Any records that are being used by staff in the reception area should not have any details accessible to the public.
- Computerised records are password protected.
- Computer screens at reception cannot be viewed by passers-by. If a staff member leaves their PC unattended for any length of time, we should either place our system on stand-by, use a screensaver password or log off.
- Screens and monitors must be turned off at the end of each work day.

- Staff may only use media storage devices (for example, but not limited to, floppy disks, pen drives etc) on their, or another employee's, assigned computer system with express authorisation from management. Such consent is generally approved for purposes of travel for work but not for staff to work from home.

When transferring patients' health information to someone else, we must do what we can to prevent unauthorised people from discovering or using the information.

SCIP reserves the right to inspect and review our assigned computer system including, but not limited to usage, contents of computer directories including folders and files, and internet access and emails at any stage. The individual user retains responsibility for the introduction (accidental or otherwise) of any virus or infection to SCIP's system through the receiving of any e-mail or file. SCIP may delete messages if they have any reason to believe there is any potential danger to the firm computer system.

Computerised Records

SCIP records are with servers hosted by a computer system and hard drive, which is responsible for security and back up of the data which is done on a daily basis. In case of the failure of this network, SCIP deploys another system to access the servers. Local terminals are protected by antivirus software. There is a restriction of websites used by staff to prevent any malicious threats via the internet. Staff members are not allowed to upload information to USB Sticks or CD-ROMS for their own purposes or for illegal copying or transfer of information.

Access to the electronic health records is by password which is individual to each staff member. Currently all staff have access to the medical records. Administration staff have access only for the purposes of efficient administration of patient services.

Website Health Information

- SCIP does not refer to patients' information on the website except where SCIP has the express consent of the patient or their representative. Generally SCIP will only provide information about patients where their accounts have been published in the media.
- SCIP does not disclose patients' personal information to others, except with their permission and in accordance with the Health Information Privacy Code 1994 and any other legislation.

Disposal of Health Information

Our policy is to follow the guidelines of the Health Retention of Health (Information) Regulations 1996. See the Medical Council of New Zealand (ref: 5 par 5 – a, b, c. Maintenance and retention of patient records) (attached at **Appendix A**).

In summary:

- SCIP may dispose of information at 10 years and 1 day following **the date of the last consultation**, if the designated patient's audiologist is satisfied this is reasonable.
- Note is made of MCNZ – section 5 (b) regarding longer term retention of records for significant patient conditions.

Safe Management and Disposal of Health Information

Information may be destroyed if it is not considered clinically important to retain or there is a copy of this information. When information is no longer needed, SCIP will shred any paper with patient identifiable information or engage a document destruction service. Computers that contain health information that are not being used or are leaving SCIP should have the data rendered irretrievable.

Patient's rights to access and correct health information

Patients have the right to find out whether SCIP holds their health information, and access health information, unless we have lawful reasons for withholding the

information. Patients are entitled to ask SCIP to correct the information that we hold about them.

Assist Patients Requesting Access to Information

We must assist patients who ask to access their health information:

- Patients should be asked to complete a form requesting access to their health information. Patients should be asked to be as specific as possible so that our response is quicker. Patients should state if their request is urgent.

- We should satisfy ourselves of the identity of the person before releasing information. A copy of a driver licence, birth certificate or similar ID is required. Requests received electronically need to attach some form of identification.
- We should consider keeping a sample of signature on file for comparison.

Decision to provide information

We must decide whether or not to entitle patients access to their notes. Patients should be provided access except in certain circumstances.

Exceptions to providing patients with access to their health information are set out at ss 27 -29 of the Privacy Act 1993. For example, SCIP is not required to provide patients with access to their health information where disclosure would be likely to prejudice the physical or mental health of a patient (see s 29(1)(c) of the Privacy Act).

If in doubt staff should not release the information until checking with the Privacy Officer.

Timeframe

We have 20 working days to indicate whether we will action a request, and what form we will release the information (such as by providing a copy to read). We can refuse a request, but only for limited reasons. We will inform the patient of any related costs associated in providing access to their records.

In most cases we should also be able to provide information requested within 20 working days, although this may depend on the amount of information requested.

How to provide access to information

When providing access to information:

- Staff should provide information in the form requested by the patient (such as orally, or providing them with a copy of specified notes) unless an exception applies. This will normally be provided as photocopies. We can make access available in a different form if providing it in the form requested would impair efficient administration; be contrary to any legal duty of the agency; or prejudice the interests protected under ss 27-29 of the Privacy Act 1993.
- If there is a good reason for withholding some of the information in a document, a copy of the full document may be made available with any necessary deletions or alterations. Where this happens, SCIP will give the

patient reason for withholding the information, and, if requested, the grounds for doing so.
- Requests for information by another party generally require a written consent except in cases where another health agency e.g. hospital requests information which relates specifically to the problem at hand.
- Give a copy to the patient or other party, always keeping the records intact.

Withholding information

Where SCIP **withholds** a patient's information, we should inform the patient:

- The reason for refusal (ie exactly which reason is being relied on);
- The supporting grounds; and
- That the patient has a right to complain to the Privacy Commissioner and to seek an investigation and review of the refusal (s 44 of the Privacy Act).

If this is unacceptable then advice should be sought from the Privacy Officer or Officer of the Privacy Commissioner.

Charging for Access to Information

SCIP may only charge a patient for accessing health information where either: the patient has requested access to the same or substantially similar information, and SCIP has provided this information, within the last 12 months; or SCIP has provided a copy of an X-ray, video recording, MRI scan photograph, PET scan photograph or CAT scan photograph.

If SCIP intends to make a charge as above that is likely to be above $30, it must provide the patient with an estimate of the charge before dealing with the request.

Transfer request

Where SCIP does not hold a patient's health information, or believes that another health organisation is more closely connected to the patient's request for information, SCIP must transfer the request, and in any case within 10 working days. SCIP must inform the patient that the request has been transferred.

Correction of Health Information

A patient can request correction of information and request that there be attached to the information a statement of the correction sought but not made. Where the patient seeks a correction, the audiologist/General Manager should take steps to ensure the information is accurate, up to date, complete and not misleading.

If SCIP is not willing to correct the information, we must, if requested, attach the information relating to the correction sought to any health-related notes.

SCIP must tell the patient of its decision and steps taken, and as reasonably practicable, tell other people and agencies who have received the information about those steps.

Accuracy of Health information

Before using patients' health information we must take reasonable steps to ensure that the information is accurate, complete, relevant, up to date and not misleading. The steps that we will need to take will vary depending on the circumstances, such as the age and reliability of the information, and the risk of relying on inaccurate information in the circumstances, and the probability, severity and extent of potential harm for the individual should the information be accurate.

From time to time, SCIP should ask a patient if their health records, and personal contact details are up to date, so that all health records are up to date.

Use of Health Information

We should only use patients' health information for the purpose for which we have collected the information unless the patient or their representative has consented to us using the information for another purpose, or the disclosure is directly related to one of the purposes in connection with which the information was obtained, or one of the other exceptions in the Health Information Privacy Code (rule 10) applies.

Staff must consult our programme's Privacy Officer before using a patient's health information without the patient's consent.

Disclosing Health Information

SCIP should only disclose information to an individual concerned, or to their 'representative' (such as parent or guardian where the individual is under the age of 16) and where the individual is unable to give their authority, unless we have the patient's authority to disclose information to someone else, or disclosure is for one of the purposes with which information was obtained (such as a treatment), or the source of the information is publicly available.

Staff seeking a patient's authority to disclose information, should:

- Specify what information we are planning to disclose;
- Specify to whom we plan to disclose the information;
- Seek their authority to disclose this information, and whether we need to seek their information again in the future.

We must not disclose a patient's health information without their consent (or the consent of their representative) unless we reasonably believe that it is not desirable, or not possible, to obtain the patient's consent, in accordance with rule 11 and:

- The disclosure is related to one of the purposes for which we collected health information;
- The disclosure is to the patient's caregiver and the patient hasn't objected to the disclosure;
- It is necessary to disclose the information to prevent a serious and immediate threat to the patient or another person's life or health;
- The disclosure is made for the purposes of a criminal proceeding;
- The patient is, or is likely to become dependent on a drug that we need to report under the Misuse of Drugs Act 1975 or the Medicines Act 1981;

- The disclosure is to a social worker or the police and concerns suspected child abuse;
- The disclosure is made by a doctor to the Director of Land Transport Safety and concerns the patient's ability to drive safely.

Policy Statement:

- Where disclosure of information is required by law then it would be prudent for SCIP to inform the patient that this is going to happen and that we are required to disclose the information.
- There are other situations where disclosure without consent may be justified, such as disclosing information to agencies such as the Police. Staff must discuss any proposed disclosure with our programme's Privacy Officer before disclosing the information.
- Staff must consult with SCIP's Privacy Officer before disclosing a patient's health information without his/her consent.

Children under 16

- We can refuse to give information to a person under the age of 16 ("child") if we think it is not in their interest.
- Parents do not automatically have the right to access their children's files. As a child's representative, the parent's right to access information falls under s22F of the Health Act 1956, which allows us to refuse information them access if:
    - The disclosures would be contrary to the child's interests;
    - The child does not or would not want the information released; or
    - There would be good grounds to refuse the child access under ss 27-29 of the Privacy Act 1993.
- Staff must take care in situations where the child may have attended without their parent. In these circumstances we may need to preserve the child's confidentiality, even from the parents, unless we have the child's agreement otherwise.
- We generally check with the child and their parents/guardians regarding who shall access health information, and who may be allowed access to health information.

Another Provider

If requested to provide information to another provider we must do so promptly. We cannot withhold the information to the patient or another provider on the grounds that we are owed money by the patient (s22F Health Act 1993).

Insurance Company, ACC

Where health information is subject to a request by an insurance company, ACC or any other organisation where a significant amount of data (especially if the data might be considered sensitive or may have significant impact on that patient's health or entitlements) is requested, confirmation (verbal is adequate) should be obtained from the patient before complying.

In the case of requests for information by those unable to give consent themselves (deceased or incompetent) then all efforts must be made to confirm that consent is given by the appropriate legal representative such as the executor of the will. If in

doubt consult the Privacy Officer, Medical Protection Society or the Office of the Privacy Commissioner.

Transfer of Health Records

Notes to be transferred should first be reviewed by the audiologist, and then the General Manager. Full copies of notes are kept unless advised otherwise by the audiologist/General Manager.

SCIP may transfer patient files to patients, their representatives and other health providers. Electronic Notes are sent electronically via Profile computer system to ensure confidentiality. Paper notes are sent by post to the nominated doctor/specialist after ensuring the address is accurate. Patients going overseas may be given a copy of their notes if it seems impractical to send them to their clinician overseas. A scanned copy of their file should be kept if this is the case in the event of loss of the file.

Confidentiality

This will be ensured by the use of the Privacy legislation and with duty of medical practitioners to maintain confidentiality, and by having signed confidentiality provisions in agreements with all staff and contractors.

Organisational

All SCIP team members should have signed agreements relating to privacy provisions.

Contractors (including temporary workers') Confidentiality Agreements are stored in the Privacy folder.

All hard copy health information is stored in the back office accessible to staff only.

Relevant Resources:

- Privacy Act 1993
- Health Information Privacy Code 1994
- On the Record, a Practical Guide to Health Information Privacy 2nd edition
- Legislation website (see Privacy Act 1993): http://www.legislation.org.nz
- Officer of the Privacy Commissioner http://www.privacy.org.nz

Services

- Medical Protection Society – phone 0800 2255677
- Duncan Cotterill Lawyers – phone 03 379 2430
- Office of the Privacy Commissioner – phone 0800803909

Training

All staff must undertake training and dates recorded. Privacy training should take place for all staff every few years, and on induction of new staff member. Privacy training may take the form of an external training session e.g. internal session preferably run by someone who has recently undertaken external training. New staff members employed should demonstrate that they have undertaken recent training relevant to SCIP. In addition they will read the documents attached to this policy in connection with ensuring Privacy.

Dealing with Complaints and Breaches

Where a patient wishes to make a complaint about privacy, the patient, or their representative, is encouraged to raise a formal complaint by completing a form (attached at **Appendix B**). The privacy officer shall investigate the complaint, or require one of the audiologists to investigate the complaint.

SCIP has a designated person (General Manager) who deals with complaints alleging a breach of the Code to facilitate a fair and efficient resolution. Where practicable, the audiologist/General Manager who deals with the complaint will not be the same person accused of breaching the Code, so that there is independence.

Complaint – Where a patient complains about a breach of the Code:

- SCIP must acknowledge to the patient, in writing, that it has received a complaint of a breach of the Code, within 5 working days of receiving the complaint.

- SCIP must inform the patient of any relevant internal and external complaint procedures (including this policy); and

- The agency must document the complaint and actions of SCIP in writing.

- Within 10 working days of acknowledging the complaint, SCIP must decide whether or not it considers the complaint is justified. If SCIP requires further time to investigate the complaint, SCIP must determine the amount of additional time required – and if SCIP requires more than 20 working days to determine whether or not there has been a complaint, we must inform the patient of this delay, and the reasons for it.

- As soon as practicable after deciding whether or not to accept that a complaint is justified, SCIP must inform the complainant of the reasons for the decision; any actions that SCIP proposes to take; any appeal procedures which SCIP has in place; and the right to complain to the Privacy Commission.

Breach – Where there has been a breach of a patient's privacy:

- **Contain the breach –** SCIP will endeavour to take immediate steps to contain the breach and stop any further loss or disclosure of health information;

- **Investigate and evaluate –** SCIP shall investigate how the breach occurred, and evaluate the risks associated, including the potential consequences, and the sensitivity of the information concerned.

- **Notify –**SCIP shall notify patients concerned at SCIP's discretion, and depending on the level of the risk, it may be appropriate to notify external agencies such as the Office of the Privacy Commissioner.

- **Prevent** –SCIP shall prevent any further instances of the breach taking place.

Variation and Amendment

These policies are subject to variation, updating and introduction on an as and when needed basis. Staff are expected to be familiar with these policies, any changes will be brought to their attention as and when they occur.

SCIP appreciates feedback on the policies contained in this document.

Appendix A (to Policy):

MEDICAL COUNCIL OF NEW ZEALAND

AUGUST 2008 www.mcnz.org.nz

The maintenance and retention of patient records

Introduction

Records form an integral part of any medical practice; they help to ensure good care for patients and also become critical in any future dispute or investigation.

01 Maintaining patient records[i]

(a) You must keep clear and accurate patient records that report:

- relevant clinical findings
- decisions made
- information given to patients
- any drugs or other treatment prescribed.

(b) Make these records at the same time as the events you are recording or as soon as possible afterwards.

02 Practice systems

(a) Council recommends that every practitioner has access to systems for recall of patients who need regular checks or treatment.

(b) Doctors should have systems in place to ensure that test results are acted upon in a timely manner, including notification of patients as appropriate.

03 Fees and patient records

(a) Section 22F of the Health Act 1956 states that transfer of patient records cannot be refused because of money owing or conflicting commercial interests.

(b) A patient or representative of the patient cannot be charged for copies of his or her records unless they have previously requested the information within the past year. Video recordings, x-rays and CAT scans are exceptions to this rule.[ii]

(c) Patients have a right of access to information in their records because the information belongs to the patient, whereas the record belongs to the doctor.[iii]

(d) When sending information to patients it is advisable to ask the patient what method is preferred because message services, facsimiles and e-mails are not always secure.

04 Transferring patient records

(a) It is advisable to transfer patient records using some form of registered mail so that tracing the records is possible if they go missing in the mail.

(b) The Medical Protection Society strongly recommends that medical practitioners retain a copy or summary of any patient records that are transferred, for subsequent reference, particularly if there may be disciplinary action to follow.

i Refer to *Good medical practice*. Cole's Medical Practice in New Zealand contains further guidance on record management.

ii Part III (6) Health Information Privacy Code 1994

iii There may be situations where a doctor feels it is unwise to provide access to all the information. Rule 11 of the Health Information Privacy Code 1994 provides situations where a doctor may not have to disclose all health information about the patient.

Level 13, 139-143 Willis St, PO Box 11-649, Wellington, Tel 04 384 7635, 0800 286 801, **Fax** 04 385 8902, **Email** mcnz@mcnz.org.nz

Appendix B (to Policy): Privacy Complaint

Please ask for a copy of our complaints procedure

Writing a Complaint
Please complete this form if you wish to formally make a complaint about a potential breach of my privacy at Southern Cochlear Implant Programme.

Should you wish to make a complaint, please contact the General Manager Neil Heslop so that your complaint can be logged: email neil.heslop@scip.co.nz or phone 0800 500 405.

We accept complaints from patients, and from any person who makes a complaint on a patient's behalf (such as a family member, friend or advocate).

Facts
Please set out the facts. It is helpful for our organisation if you provide as much detail as possible with respect to your concerns. In your written statement, please state:

- What happened;
- When did it happen (date, time);
- Did anyone witness what happened;
- What is the issue of concern;
- Is there anything else relevant that you want to tell us.

Facts relating to the potential breach of your privacy (and rule under Health Information Privacy Code 1994 that may have been breached):

How has this affected you?

Have you already attempted to resolve this issue, and what was the outcome?

How would you like the matter resolved?

If you are writing the complaint on behalf of a patient, please give your name and the patient's name, the relationship between you and the patient and their consent for you to make the statement on their behalf?

Details of your advocate/solicitor, if you are represented by someone

Signature of Patient (or advocate) Date