Privacy of Health Information Overview PHC Remote Guideline

Target Audience	All Employees
Jurisdiction **Jurisdiction Exclusions**	Primary Health Care Remote CAHS; Primary Health Care Remote TEHS N/A
Document Owner	Kerrie Simpson Atlas Development Officer Primary Health Care Remote CAHS
Approval Authority	Chair Primary Health Care Executive CAHS; Primary Health Care Remote Safety and Quality Committee TEHS
Author	PHC Safety and Quality Team

The attributes in the above table will be auto-filled from the PGC System. Do not update in this document.

Purpose

To provide Primary Health Care Remote staff with a guideline on the principles for the management of privacy for client health information and records in remote health centres.

Guideline

1. General Information

The Northern Territory (NT) Department of Health (DoH) Privacy Policy is based on the Northern Territory Information Act which provides a framework for the management of government information and records in the NT. The Act addresses the issues of Freedom of Information, privacy, records and archives management. It is designed to promote the free flow of government information, subject only to the need to protect essential public interests and the private and business interests of individuals.

At the heart of the Information Act are 10 Information Privacy Principles (IPP, see Schedule 2 of the Act) that aim to protect information privacy. These principles cover the whole cycle of information from collection and handling, to storage and disposal. The principles are not intended to prevent the legitimate use of personal information to provide government services. They merely require public sector organisations to shift the emphasis to give people more control over what personal information they give to an agency and how it is used. The principles can be summarised as:

- the right information
- to the right people
- for the right reason
- in the right way
- at the right time.

2. Definitions

Personal Information: government information from which a person's identity is apparent or is reasonably able to be ascertained.

Health Information: all personal information collected in the provision of a health service is considered to be health information or sensitive information under the IPPs and according to the DoH Privacy Policy.

Information Privacy: refers to the right of an individual to exercise appropriate control over the extent to which personal information about him / herself is available to others.

Confidentiality: refers to the restriction of access to personal information to authorised persons, entities and processes at authorised times and in an authorised manner.

Electronic Health Record (EHR): a systematic collection of electronic health information about individual clients. The EHR is the primary health record into which client personal and health information must be entered.

Hard Copy Health Records (Hard Copy): *any* printed or written records containing health centre client personal or health information. See Section 4.1.3 Hard Copy Records / Information for details.

3. Responsibilities

3.1 Employees

(In this instance includes: volunteers and students working for DoH, contractors providing services to and on behalf of DoH and private health care or welfare agencies or providers, researchers or others who have authorised access to information in the custody of the DoH.)

- Comply with the Information Act, Information Privacy Principles (see Schedule 2 of the Act) and the DoH Privacy Policy

4. Procedure

4.1 Access to Health Records

4.1.1 Access and Confidentiality

Personal and health information in health records may be accessed by authorised staff for the purpose of providing health care or to meet PHC operational requirements and must not be accessed for any other purpose without specific authorisation. This applies equally to Electronic and Hard Copy Health Records.

Information must only be accessed by or disclosed to staff members when it is clearly established that there is a legitimate right to that information. This is supported by the NTPS Code of Conduct No 14, Use of Information acquired in the Course of Employment.

Staff must take reasonable steps to protect the personal information in all health records from misuse, loss, unauthorised access, modification or disclosure (IPP 4: Data Security).

4.1.2 Electronic Health Record

In Primary Health Care (PHC) the EHR is the primary health record. All relevant client personal and health information is to be recorded in the EHR.

See Electronic Health Record User Access and Electronic Health Record Overview for details on processes to ensure confidentiality of these records.

4.1.3 Hard Copy Health Records / Information

All written and printed materials with client health information are classified as hard copy health records. Hard copy health records therefore include:

- the superseded hard copy secondary client health records (also known as client file or patient file)
- all hard-copy client personal and health information related to or generated by EHR systems such as recall lists and printed reports, correspondence from outside sources and any other relevant written or printed materials

Specific processes for managing the security of the superseded secondary hard copy health records can be found in Electronic Health Record Overview.

Hard copy health information related to or generated by the EHR, such as recall lists, as well as letters or reports from external sources and results of procedures such as ECGs must be scanned, imported in to the client's EHR and the hard copy stored as described in Electronic Health Record Overview.

4.2 Prevention of Incidental Breaches of Confidentiality

Breaches of confidentiality can occur during the course of everyday activities. Ensure that those who do not have the right to access information cannot overhear work related discussions or see any messages or written information that include personal information.

If it is necessary to leave a voicemail message, this must not contain confidential information.

PCIS Users must send client information through the secure Inbox Message system.

The EACS Intray provides a secure messaging system for investigation results and other documents, but not for provider-to provider messages. EACS Users may send information of this nature by e-mail.

For further details on the security of information, see Electronic Health Record Overview.

4.3 Prevention of Breaches of Confidentiality through Portable Storage Devices

Portable storage devices (PSDs), including laptops, CDs, DVDs, USB sticks, mobile phones and digital cameras provide a convenient way to store information. Confidentiality of personal and health information can be compromised through the loss or theft of these. Devices must be kept in a secure location and must have an active password or Personal Information Number (PIN). Additionally it must be secured by turning on security features or by encryption. See Encryption of USB Drives Instruction and Electronic Health Record Overview for further details.

4.4 Breaches of the NTPS Code of Conduct through Social Network Sites

PHC staff must ensure that breaches of confidentiality related to the workplace do not occur through careless use of social networking sites such as Facebook and Twitter.

The NTPS Code of Conduct can be applied to social networking entries where there is a connection between a posting on a social site and work or work-related activities. This applies equally to comments made from work or home computers. If considered serious PHC Branch can utilise the disciplinary provisions of the Public Sector Employment and Management Act.

Document Quality Assurance

	Method	Responsibility
Implementation	Document will be accessible via the Policy Guidelines Centre and Remote Health Atlas Distribution will be by e-mail notification	Health Policy Guidelines Program Director of Nursing and Midwifery PHC CAHS and TEHS
Review	Document is to be reviewed within three years, or as changes in practice occur	Atlas Development Officer, Primary Health Care CAHS
Evaluation	Evaluation will be ongoing and informal, based on feedback.	Atlas Development Officer, Primary Health Care CAHS

Key Associated Documents

Forms	Nil
Key Legislation, By-Laws, Standards, Delegations, Aligned & Supporting Documents	Electronic Health Record Overview Electronic Health Record User Access Information Act Information Privacy Principles, see Schedule 2 Information Act Department of Health (DoH) Privacy Policy Health Information Privacy – brochure DoH Freedom of Information and Privacy website NTPS Code of Conduct PCIS Website URG PCIS Inbox Messaging Tips PCIS Inbox Messages EACS Website NT Health intranet documents: Encryption of USB Drives Instruction Social Media Policy Social Media Policy Frequently Asked Questions
References	As above

Evidence Table

Reference	Method	Evidence level (I-V)	Summary of recommendation from this reference
N/A	N/A	N/A	N/A