Electronic Health Records 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 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 (PHC) Remote staff with an overview for the management of Electronic Health Records for clients of remote health centres including User access, training and resources, security, managing outages and data management.

Guideline

1. General Information

The Electronic Health Record (EHR) is a systematic collection of electronic health information about individual clients. The EHR is the primary health record into which client demographic and health data is entered (unless the client states they do not want the information entered). Two main EHR systems operate within PHC remote health centres. These are the Primary Care Information System (PCIS) and East Arnhem Communicare Systems (EACS).

PCIS and EACS interface with other databases such as:

- the eHealthNT Clinical Portal (NTCP) via PCIS which provides access to the Northern Territory (NT) My eHealth Record and the National My Health Record and on EACS access is via individual icons to the NT and National eHealth Records. These records provide a secure online summary of an individual's health information that can be securely exchanged between a range of health care providers such as doctors, hospitals and other healthcare providers.
- Childhood Immunisation Database
- Rheumatic Heart Disease Database
- Synapse system

Authorised Users of EHRs and other Databases must abide by the DoH Privacy Policy, Information Act, National eHealth Record System Participation Policy, National eHealth Record System Implementation Guidelines and the NTPS Code of Conduct as per Privacy of Health Information Overview.

Information in this document includes:

- Primary Health Record
- User Access
- Training and Resources
- Electronic Health Records Security
- Managing Outages
- Electronic Health Records Data Management
- Management of Historical Hard Copy Medical Records

2. Procedure

2.1 Electronic Health Records - Primary Health Record

The EHRs are the primary health records for clients of PHC remote health centres. All relevant personal and health information must be recorded in these systems. Superseded hard copy records are for reference only and no new information is added to those records.

2.1.1 Privacy and Confidentiality

Only authorised persons may access EHRs. There is an obligation on all PHC staff to ensure a high level of confidentiality is maintained and only appropriate use of client information occurs. Access to records must be strictly in accordance with the DoH Privacy Policy, the Information Act and the NTPS Code of Conduct.

These principles apply equally to access to linked non-PHC health records such as the NT My eHealth Record, National My Health Record, Rheumatic Heart Disease, Childhood Immunisation and Synpase PACS System databases. For further information see Privacy of Information Overview.

Staff must ensure that the process described in the Requests for Health Records Flowchart is followed before release of any client health information.

2.2 Electronic Health Record - User Access

EHR User Access is granted to individuals with a legitimate requirement to access or contribute to PHC client health records. Different levels of access are available according to the role of the applicant. For further information see Electronic Health Record User Access.

2.3 Training and Resources

Training	All authorised Users are required to undergo initial training with a Digital Health Services Training Advisor. When an approved Application for EHR User Access has been received that includes a new user training request (tick box on page 2 of the application form), the user will be contacted via email by a Digital Health Services Training Advisor and scheduled into the next available training session. Training is provided to suit User's role and responsibilities. Users may also contact service.centre@nt.gov.au or 1800 000 254 and request to speak to a Training Advisor to arrange any additional training.
PCIS	Users will be provided with a generic login for the PCIS Training system (for fictitious client records) at the time of training.
EACS	There is no specific training system but Users may access Fictitious Client records for training purposes. Information in these records are not included in any EACS reports.
Resources	The Training and Support sites (PCIS / EACS) provide a range of resources which support the training provided to all EHR Users. In addition, the Digital Health Services Training Advisors are available to provide assistance Monday - Friday 8:00 am to 4:21 pm. EHR resources are developed and endorsed either by the PCIS / EACS Teams or PCIS / EACS Reference Group, depending on the nature of the information.

	EHR User Reference Guides also provide the Business Rules that define PHC endorsed PCIS / EACS processes. When new EHR resources have been endorsed, the new document is uploaded onto the PCIS / EACS site and notification is sent to the PHCM and staff generic e-mails as well as to individual Departmental email accounts by the EHR Team. PHCMs must ensure that staff are made aware that the new resource is available.
PCIS / EACS Reference Group	The PCIS/ EACS Reference Group provides a single review body across all PCIS and EACS items to: - promotes consistent practice wherever possible, across the NT - collaborate with expert clinicians in the review of existing careplans to ensure optimum usability for clinicians - investigate, critically review and endorse proposed changes to PCIS / EACS items and proposed practice changes - endorse User Reference Guides, service / clinical items and care plans as appropriate The PCIS / EACS Reference Group welcome suggestions of issues for investigation. Staff may e-mail or complete the PCIS Referral Form to refer a particular idea to be considered by the PCIS / EACS Reference Group.
EHR System Upgrades	EHR systems are upgraded periodically. A User Impact document highlighting new features and enhancements of EHR upgrades will be e-mailed to Users when a new version is released. When training for the upgrade is required Users will be sent an online training schedule. It is strongly recommended that PHCMs set aside time for staff to attend training sessions.
Note: replacement, ordering or issues with hardware (computers, printers etc) are the responsibility of the NTG Service Centre.	

2.4 Electronic Health Record - Security

To meet their obligations Users must at all times ensure the privacy of client personal and health information according to the:

- Information Act, Schedule 2 and Information Privacy Principle (IPP 4) and
- Information, Communication and Technology (ICT) Acceptable use of computers, email and the Internet standard (see Standard 5 Logging in and passwords and Standard 6 Privacy and computers)

This includes strategies such as ensuring password security, using screen savers, appropriate positioning of computer monitors and where multiple Users access the computer individual Users loging off the EHR when leaving a computer unattended. It also includes the management of hard copy documents generated by the EHR system, such as reports, or documents that need to be scanned into the system.

Staff must ensure that computers left unattended cannot be accessed by unauthorised persons and computer screens must be positioned in a way that prevents unauthorised viewing of client information. Staff must access client health records only as necessary in the course of their duties.

Password and User Id Protection	Individuals with authorised User Access to EHRs are assigned a unique User Id and Password for their personal use **only**. **These details must never be disclosed to others.** All information entered under this electronic signature is legally attributable to the User. To allow more than one staff member access to the EHR via an individual computer, Users are required to log onto the computer (Windows) via the generic health centre G70 account user name for that location. See Getting Started – Logging On/Off (PCIS / EACS). Where more than one User may have an EHR consultation open on a particular computer in a health centre, Users must be particularly vigilant not to enter information under the signature of another User. The User Id displays at the top of the screen and must always be checked before entering any data. **Where multiple Users need access to the computer, locking computers is not recommended. Individual Users must log off the EHR when leaving a computer unattended.**

PCIS Password Management	After PCIS access has been created, Users are emailed with instructions to contact NTG Service Centre (service.centre@nt.gov.au or 1800 000 254) to obtain a password. To be provided with a password, Users must authenticate themselves by answering their ePASS Challenge questions. If a User does not have Challenge Questions, or there are issues, they will be transferred to the Digital Health Services User Access Group for further assistance. For security purposes passwords must then be changed every 30 days. When a password expires a 'change password' prompt will display and the password must be changed. See PCIS Password for information on how to manage passwords and password changes.
EACS Password Management	After EACS access has been created, users are emailed with instructions to contact NTG Service Centre (service.centre@nt.gov.au or 1800 000 254), and ask to be transferred to the Digital Health Services User Access Group to obtain a password. To be provided with a password, Users must authenticate themselves by answering their ePASS Challenge questions. Users are responsible for the security of their own passwords and must change passwords on the first working day of each month or whenever they have reason to believe the password has been compromised. EACS does not prompt staff to change passwords. See EACS Password for details.
Security of Hard Copy Materials related to an EHR	Hard copy personal and/or health information must be managed in accordance with the security requirements for EHRs including that they must not be accessible to anyone who does not have authorised EHR User access.
Printed EHR Reports	To protect the privacy of individuals and confidentiality of communities that may be directly or indirectly identified by printed electronic reports such as recall and specialist referral lists, these must be kept in a place where they are not accessible to unauthorised persons. Reports must be shredded or de-identified as soon as they are no longer required. Daily reports should be shredded at the end of each day and weekly reports at the end of each week.
Forms – Hard Copy	Documents such as EHR hard copy consultation forms which are used for outstation visits or during power outages must be stored securely until the data has been entered into the EHR and the original form has been scanned in as a document. The hard copy must be placed in the 'EHR Hard Copy' archive box.
Other Non-Electronic Health Information	A number of other documents such as hard copy letters or reports or results of procedures such as ECGs must also be scanned into the EHR. The hard copy must be placed in the 'EHR Hard Copy' archive box.
Amending Electronic Health Records	For medico-legal reasons, Users do not have the security access to allow the reopening and changing of consultations after they have ended the consultation. Requesting data correction includes PCIS Users notification via PCIS Inbox Messages and EACS Users notification via e-mail: - the person requesting correction of data sends a message to the PHCM / Clinical Supervisor - the PHCM / Clinical Supervisor verifies that the consultation is to be reopened and forwards the Inbox Message to Helpdesk, PCIS for actioning of the request.
Storage of Information outside the Government Records Management System	EHR Users must abide by the NTG End User ICT Services Policy which defines how the NTG Records Management system must be used. All Users are responsible for ensuring that DoH business and health information is securely recorded on an electronic NTG system that is backed up immediately or as soon as possible. Section 8 of the Policy is particularly relevant to users of Portable Storage Devices (PSDs).
Portable Storage Devices (PSD)	PSDs are portable devices designed to store digital data and include laptops, mobile phones, CDs or DVDs, USB sticks and digital cameras or any other portable device that contains identifiable client personal or health information or any other Departmental information. PSDs provide a convenient way to store DoH information, especially for staff that are required to travel to remote communities. However, privacy of personal information can be compromised through the loss, theft or malfunction of these devices.

	USBs are the devices most likely to be lost and also pose more of a risk of introducing viruses into NTG ICT systems than other PSDs. To help protect the information stored on PSDs staff are advised: - to avoid the use of USBs, if possible - if USBs are used, use them only with authorised computers that are virus-protected - securing the USB by encryption prior to commencing use - password enable or PIN protect devices - use CDs and DVDs that are writeable one time only - keep PSDs in a secure location, especially when in transit. Information recorded on these devices must be downloaded onto a DoH server at the first available opportunity. Users of Smartphones must abide by the DoH Smartphone Policy. Refer to NTG information on IT and Telecommunications Security for further information.
Northern Territory Government (NTG) Information Security Incidents	While many security incidents can be resolved in the workplace, some incidents will require further investigation. All incidents must be reported using RiskMan. Serious incidents will be reported to the Chief Information Officer or the Director ICT. If the incident involves activity of an illegal nature, the matter will also be referred to the Northern Territory Police after informing the Chief Executive.

2.5 Managing Outages

Outages which affect EHR systems can occur from time to time for a variety of reasons. These may be the result of a planned or unplanned NTG or EHR outage or unexpected power or telecommunications network failure. Health centres will be notified by email of planned Local Area Network (LAN), PCIS or EACS Outages.

Procedures to manage these outages, record consultations during outages and transfer data into the EHR after the outage must be followed to maintain business continuity and ensure the integrity of client records.

2.5.1 Preparation for Outages – General Information

DoH remote health centres have an Uninterruptible Power Supply (UPS) which is an electrical apparatus that provides emergency power when mains power fails located in the Communications Cabinet. The UPS keeps network systems live but does not provide power to the dedicated emergency laptop or any other emergency equipment in the health centre.

Emergency Laptop	The emergency laptop/s in health centres must always be fully charged and connected to an emergency power point (where an emergency power supply such as a generator exists). To promote battery maintenance it is recommended that the emergency laptop/s battery be fully discharged periodically (once a month). This will promote battery maintenance and maximise the duration the emergency laptop will function using battery only power. It is recommended that this be done overnight and the laptop re-connected to the power supply in the morning to charge. Once connected to the power supply, the laptop can also be used as required. EHRs will be available during power outages if battery or emergency power is available to the laptop or to any other computer that may be connected to the emergency power supply. EHRs will not be available on any computers during planned system outages or if the telecommunication network fails.
EHR Hard Copy Consultation Forms	The PHCM must ensure that that there is an adequate supply of blank hard copy Consultation Forms (PCIS) / (EACS) in a dedicated location known to all staff. A copy of the form must also be saved to the desktop of the dedicated emergency laptop.
PCIS – Mass Print Client Summary Report	The Mass Print Client Summary Report is sent to each health centre's PHCM weekly and provides summary health record information to be available during outages. The PHCM must ensure that each new copy of this vital information is saved to the desktop of the dedicated emergency laptop under the generic staff logon. Always use the same document name to ensure that older version of the Summary is overwritten. See PCIS

	Mass Print Client Summary Report and quick guide Mass Print Client Summary Report PHC Remote CAHS Information Sheet. In some cases, such as when there is a planned network outage an unexpected failure of the telecommunications network, the Mass Print Client Summary Report saved to the emergency laptop will be the only source of client health information.
EACS – Data Sync Client Backup Laptop/s	The dedicated Emergency Room laptop has EACS Data Sync Client Offline Communicare installed. This laptop must be backed up daily to ensure that client data is current and can be used to access client records during outages. Some health centres have a second laptop for use when conducting consultations outside the health centre. This must also be backed up daily and can also be used during outages. It is recommended that the task of initiating daily back-up be allocated to a staff member responsible for the task. The back-up process can be time-consuming and can slow down performance of EACS in the health centre. It is therefore recommended that this be done at the end of every working day to avoid inconveniencing Users.
ehealthNT Clinical Portal	When there is a planned PCIS outage, all clinicial Users are advised to reset the eHealthNT Clinical Portal (NTCP) password, so during the outage, Users can access the NTCP via the URL.

2.5.2 Managing Health Records following an Outage

Consultations conducted during an outage must be recorded on the printed hard copy EHR Consultation Form using a black pen[1] (to enhance reproducibility).

Each health centre must have a dedicated secure location for storing completed hard copy Consultation Forms. Forms must remain in this location until the system has been restored and data can be entered into the EHR by the person who conducted the consultation.

Recording the hard copy consultation into the EHR is a two-step process:

1. enter the data into the EHR to to ensure that the data is available for clinical and reporting purposes
2. the original document must be scanned and imported into the client record to ensure that there is a permanent, accessible record of the original information. Information on how to scan and import a document can be found in Basic Steps (PCIS – *scroll down the web page to Scanning & Importing table) /* EACS Scanning and Importing.

The recording process for hard copy records is as follows:

- keep forms in a dedicated secure location until the data is entered and the form scanned
- enter the data into the client EHR as a backdated PCIS Visit Consultation / EACS Recording Consultations (this must be done by the person who conducted the original consultation)
- sign and date the form to indicate who entered the data / scanned the form and when it was done
- scan and import the document into the client record, and name it using the following format: **yymmdd_pcis_consultation_form | yymmdd_eacs_consultation_form**
- the hard copy form should be placed in the 'EHR Hard Copy' archive box used for this purpose. These hard copy records are to be retained in accordance with the Retention and Disposal Schedule.

2.6 Electronic Health Record Data Management

Adding Hard Copy Information	See process described in Managing Health Records following an Outage above.
Adding Third Party Information	If a person whose normal duties do not necessitate accessing the EHR has important health related information to convey, this must be put in writing and reported to another health practitioner with authorised access to health records. The information must then be recorded by that person following the process described above. In addition:

[1] Australian Standard for Paper-based Health Care Records, (AS 2828)

	- add a Progress Note to record who the information came from - if necessary, notify the health practitioner/s who need to be made aware of the contents of the document. PCIS Users use a PCIS Inbox Message for this purpose. EACS Users may send an e-mail message.
Data Correction	See process described in Amending Electronic Health Records above.
Restricted Access – PCIS only	In some instances access to a particular event in PCIS can be restricted. PCIS Users may restrict an event to the person who is entering the information onto the health record or to a Medical Officer. Clients have the right to request sensitive information in PCIS be restricted. However, clients must be advised that restricting access will mean ongoing care may be compromised and must also be reassured about the privacy obligations of all PHC staff. PCIS allows restriction to 'Doctors Only' or to 'Me Only'. PHC strongly discourages the use of these restrictions and recommends that 'Me Only' be used with extreme caution. The 'Me Only' restriction means that no other practitioner will be able to access any component of the restricted event. Medical Practitioners will not be able to access or witness pathology or other results attached to that event. Any member of the health centre clinical team is able to restrict access to 'Doctor Only' and, if doing so, should send the medical practitioner an Inbox Message to explain the circumstances. Even this restriction should be used with caution to avoid compromising care. Generally, the restrictions cannot be lifted, even in an emergency. However, in extreme cases, and only with adequate justification, the restriction may be lifted with the approval of the General Manager. *Note: Restricted Access functionality is not available in EACS.*

2.7 Management of Historical Hard Copy Health Records

The management of superseded hard copy health records (client file, patient file) remains a vital part of the client's total health record, and appropriate storage must be maintained to ensure that records are stored securely, but are accessible when they are required. No further information must be added to these records.

These historical hard copy health records in health centres have been, or are in the process of, being archived and transferred to Secondary Storage facilities in Darwin and Alice Springs. These historical health records are held in these facilities awaiting archiving or a destruction date, in accordance with the Disposal Schedule for Patient Records of the NT. See Retention and Disposal intranet site.

Compliance

Adverse events must be recorded in RiskMan and followed up by relevant Managers	Manager PHC CAHS: Clinical Nurse Manager, Quality and Safety PHC TEHS: Safety and Quality Manager

Document Quality Assurance

	Method	Responsibility
Implementation	Document will be accessible via the Policy Guidelines Centre and Remote Health Atlas	Health Policy Guidelines Program
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	PCIS User Access and WebClient Application Form EACS User Access and Webclient Application Form Rural Medical Practitioner (RMP) Electronic Health Record Systems User Access Form EACS Outage Consultation Form (Hard Copy) PCIS Consultation Forms (Hard Copy) RiskMan down time form (ONLY to be used in the event of outages)
Key Legislation, By-Laws, Standards, Delegations, Aligned & Supporting Documents	Electronic Health Records User Access PHC Remote Guideline Health Records Documentation PHC Remote Guideline Privacy of Health Information Overview PHC Remote Guideline Requests for Access to Health Information and Records PHC Remote Guideline Requests for Health Records PHC Remote Flowchart Mass Print Client Summary Report PHC Remote CAHS Information Sheet. DoH Freedom of Information and Privacy website DoH Privacy Policy Information Act NTPS Code of Conduct NT My eHealth Record – provides directions to access: NT Childhood Immunisation Register NT / SA Rheumatic Heart Disease Register National eHealth Record System Participation Policy National eHealth Record System Implementation Guidelines National My Health Record Records Management (intranet) Retention and Disposal Records Management Policy (intanet) To access the following standard go to Australian Standards Online Premium and search by the standard number or name: AS 2828: Health Records - Paper-based Health Records NT Government ICT Policies NTG Helpdesk

	Health Services Information PCIS intranet site Training and Support web page - *includes recommended training per health professional* Access web page – *user access applications* Consultation Forms (Hard Copy) Getting Started – Logging On/Off Inbox Messages Making Corrections to a PCIS Health Record Mass Print Client Summary Report PCIS Password Scanning & Importing *(Basic Steps tab scroll down the web page to Scanning & Importing table)* Visit and Non-Visit Consultations EACS intranet site Training and Support webpage Access web page – *user access applications* Data Sync Client Offline Communicare EACS Outage Consultation Form Information Sheet EACS Password Electronic Records Validation Checklist & Tool Getting Started – Logging On/Off Scanning and Importing NTG Central - ICT Documentation NTG End User ICT Services Policy Acceptable use of computers, email and the Internet standard IT and Telecommunications Security (intranet) DoH Smartphone Policy Security intranet page: Information Security Incident Guidelines Encryption of USB Drives Instruction.
References	As above

Definitions

Preferred Term	Description
Hard Copy Health Records:	any printed or written records containing health centre client personal or health information. This document includes two categories of hard copy health records, namely: - 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.
Childhood Immunisation Database:	the NT Centre for Disease Control (CDC) immunisation database that links to the Australian Childhood Immunisation Register (ACIR). It is the primary source of NT childhood immunisation records for PHC remote clinical staff.

Preferred Term	Description
Rheumatic Heart Disease Register:	a register of clients with Acute Rheumatic Fever or Rheumatic Heart Disease.
Synapse:	provides access to the NT Picture Archiving Communication Systems (PACS) where radiology information and images may be be accessed.

Evidence Table

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