Appendix C - Little Red River Cree Nation
Confidential Information Guidelines

1. Purpose

These guidelines are meant to:

a. Document Little Red River Cree Nation – John D'or Health Centre, Garden River Health Centre, and Fox Lake Nursing Station (LRRCN) practices as related to confidential information.
b. Provide guidance to staff as they address challenges associated with handling confidential information.
c. Achieve statutory and regulatory compliance.

2. Definitions and Classification of Information

a. Confidential information, is not limited to, but includes:
    i. all health information pertaining to LRRCN's clients as defined by Alberta's *Health Information Act*;
    ii. all personal information as defined by the federal *Privacy Act* and the *Personal Information Protection and Electronic Documents Act;*
    iii. all protected employee information; and
    iv. all confidential business information.

b. The information listed in 2(a) above is confidential and must be minimally handled and protected as here described; however, these guidelines and the policy documents referenced here are the minimum standards to be used by LRRCN staff.

c. Confidential information of a particularly sensitive nature may be so classified and further limitations upon such information may be imposed by LRRCN management.

3. Roles and Responsibilities

a. Chief & Council and Indigenous Services Canada:
    i. Provides policy guidance and give direction to management and the custodian.
    ii. Approves policy.
    iii. Receives regular reports on non-compliance issues and actions taken; provides guidance and feedback to management and custodian.
b. Custodians with Management support:
    i. Reviews and recommends policy.
    ii. Designates privacy officer.
    iii. Responds to all non-compliance issues and act as appropriate.

c. Privacy officer with Custodian's support:
    i. Identifies privacy compliance issues.
    ii. Ensures that privacy and security policies and procedures are developed and maintained.
    iii. Ensures that all staff, students, volunteers, and contracted personnel are aware of their duties, roles, and responsibilities under applicable privacy legislation.
    iv. Ensures that the education and training requirements for handling confidential information are up to date.
    v. Provides advice to staff regarding release or non-release of health information (stored within records in your office).
    vi. Responds to requests for access to information, or to correct or amend health information.
    vii. Ensures the overall security and protection of health information throughout the practice.
    viii. Ensures the proper retention and archiving of health information.
    ix. Acts as a contact when dealing with the Alberta Office of the Information and Privacy Commissioner (OIPC).

d. All staff:
    i. Protects any confidential information they may have access to through the performance of their job duties.
    ii. Collects, uses and discloses confidential information only in the performance of their job duties.
    iii. Complies with all privacy and security policies and procedures.
    iv. Reports any privacy breaches to the privacy officer.

4. Collection of Personal Information

a. Staff should collect exactly the information required to provide care and/or preform their job function – no more and no less.

b. The quantity and nature of information that is collected from an individual will differ greatly between job functions, but all staff collecting confidential (i.e., personal) information should have a reasonable 'need-to-know' for each piece of confidential information they collect.

   For example, a nurse will need-to-know a client's detailed medical history, while the IT team has no reasonable need-to-know that same information.

c. All staff collecting confidential information should be able to explain why it is needed, how it will be used, how it will be protected and if/how it might be shared.

d. Confidential information is collected directly from the individual who is the subject of the information, or his/her authorized representative, unless:

i. the individual consents to the indirect collection of the information;
ii. direct collection would compromise the interests of the individual, the purpose of collection, the accuracy of the information, or the safety of any other person;
iii. direct collection is not reasonably practicable;
iv. the information is collected for the purpose of compiling a family or genetic history in order to provide a health service to the individual;
v. the information is collected to assess the individual's ability to participate in a program, or receive a benefit, product or health service;
vi. the information is collected to inform the Public Trustee or Public Guardian about clients or potential clients; or
vii. the information is publicly available.

e. Patients in the practice are informed of the purpose and authority for the collection of information, and the availability of the privacy officer to answer questions or concerns.

5. Use of Confidential Information

a. Confidential information may only be accessed by authorized staff.

b. Health information is to be used only as authorized by section 27 of the *Health Information Act* in order to preform assigned duties.

a. Confidential information can be used only for the reason that it was collected. Information collected for one purpose (eg. providing care) may not be used for other purposes without the knowledge and **consent**, consistent with section 34 of the *Health Information Act,* of the subject individual.

c. Files containing Confidential information may only be accessed in accordance with LRRCN's '*Policy on Safeguards for Protecting Confidential Information*'.

6. Storage of Personal Information

a. Files containing personal information are to be stored in accordance with LRRCN's '*Policy on Safeguards for Protecting Confidential Information*'.

7. Disclosure of Personal Information

a. All requests for access to information should be referred to LRRCN privacy officer.

b. Confidential information **will** be disclosed:
i. as requested by the individual about whom the information relates,
ii. with the consent of the individual about whom the information relates, or
iii. as required by law:
1. in cases of suspected abuse of a minor child,

2. to protect public health,
3. to comply with the *Fatality Inquires Act.*

c. Confidential information **may** be disclosed:
    i. to another health provider as required to ensure safe and effective care for the individual about whom the information relates, **and**
    ii. as deemed appropriate by LRRCN privacy officer and the relevant team leader (eg. the Nurse in Charge for medical records etc.).

d. Disclosure requests falling outside of those listed here should be referred to LRRCN privacy officer.

e. Generally, health information is not to be provided to 3rd parties not otherwise identified in the Act, but rather to the individual (or legal guardian) about whom the records relate as authorized in section 33 of the *Health Information Act*. The individual may then provide the record to whomever they see fit.

f. Should an individual insist that a copy of a health record be sent directly to a 3rd party, consent consistent with section 34 of the *Health Information Act* is required.

g. Disclosures of identifying health information without consent occur only as authorized by section 35 through 40 of the *Health Information Act*.

    Personally identifiable health information is generally only disclosed to other custodians providing health services to the individual requiring information to inform their practice or as required under the *Public Health Act* in cases of an outbreak of communicable disease. Specifically, these disclosures are authorized under section 35(1)(a) and (p) respectively as well as 36(a) for the accompanying registration information.

h. Non-identifying health information may be disclosed by the Custodian without consent as authorized under section 32 of the *Health Information Act*. When disclosing such information to another other than authorized custodians under the act, information includes a statement that the OIPC must be notified of any intended use that includes data matching.

i. As required under section 41 of the *Health Information Act*, the custodian must maintain a record of all disclosures including the identity of the person to whom the disclosure was made, the date and purpose of the disclosure, and the type of information disclosed.

j. Disclosure of health information is generally limited to the circumstances described in section 42(2) of the HIA, however, any other disclosures that might occur would be

accompanied by notice of the purpose of such disclosure and the authority under which such disclosure is made.

8. Retention of Personal Information

a. Active client records will be retained for at least 10 (ten) years following the last record date or for two years following the client's eighteenth birthday, whichever is longer.

b. Employee records will be retained for three years after the departure or termination of employment.

c. Financial records will be maintained for seven years following the year in which the record was made (e.g., all records pertaining to fiscal year 2011/2012 must be maintained until fiscal year 2018/2019).

d. Retention schedules for other records containing personal information will be determined by program staff in consultation with LRRCN privacy officer.

9. Archiving Confidential Information

a. At the end of the scheduled retention period, records containing personal information will be sent to Indigenous Services Canada – Alberta Region to determine archival value as per The Government of Canada's *Policy on Information Management*.

b. Records deemed not to have archival value will be destroyed by way of confidential (cross-stitch) shredding or burning only.

c. Records held in electronic form may be wiped from the record in accordance with appropriate technical standards.

d. LRRCN will maintain a record of all confidential information archived or destroyed. This record is to include:
    i. The identity of the subject individual.
    ii. The nature of the personal information.
    iii. The date and reason and method of transfer/disposal.

10. Protection of Confidential Information

a. All staff and contractors shall protect all confidential information collected by LRRCN respect the privacy of the individuals who are the subjects of that information.

b. All reasonable measures are to be taken to prevent unauthorized collection, use, disclosure, modification, or access to confidential information.

c. All staff, contractors and/or volunteers with LRRCN are required to take an oath of confidentiality and to uphold all policies and procedures respecting privacy and security of confidential information.

d. Failure to comply with LRRCN's policies and procedures may result in disciplinary action, including but not limited to, termination of employment or contract.

11. Contracting for Services

a. All contractors are subject to LRRCN's policies and procedures.

b. An agreement and/or contract will be signed between LRRCN and all third parties requiring access to confidential information, information systems, and/or LRRCN's assets. This agreement will clearly outline information security provisions for the contractor and/or bind the contractor to LRRCN's policies and procedures.

    i. If the third party:
        1. processes, stores, retrieves or disposes of health information,
        2. strips, encodes or otherwise transforms individually identifying health information to create non-identifying health information, or
        3. provides information management or information technology services

    an Information Management Agreement (IMA) is required between the third party and the custodian for the health information per section 66 of the *Health Information Act.* The IMA must meet the requirements of section 7.2 of the Health Information Regulation.

c. Contractors will be provided with a copy of all relevant LRRCN's policies and procedures and must sign to acknowledge receipt and declare compliance.

d. All related third-party information security and privacy policies should be made available to LRRCN's Privacy Officer before the contracted work commences. Any revisions occurring after execution of the contract are also to be provided to LRRCN's Privacy Officer.

e. All contractors and their employees who may access/receive/be exposed to personal information or information systems must sign a confidentiality (non-disclosure) agreement before the contracted work commences and which remains in effect even after termination of any business, contractual or employment relationship with LRRCN.

f. Any privacy breach by the contractor or their employees must be reported to LRRCN's Privacy Officer within 24 hours.

g. Agreements or contracts will include provisions for the return or destruction of information assets, including hardware, system documentation, and data upon termination of the agreement and in accordance with contract provisions reflecting records retention and data management policy.

12. Security Breaches

a. All security breaches or privacy compliance issues are reported to the privacy officer and custodian.

b. The privacy officer and custodian will investigate the breach and evaluate the severity based on the risk of harm to the individual, as required under section 60.1 of the *Health Information Act. If it is deemed that there is risk of harm, then the custodian must notify the individual of the breach.*

Risk of harm is defined in the Health Information Regulation section 8.1 as to whether there is reasonable basis to believe:

i. Information may have been accessed by someone and could be used to commit identity fraud or could be misused.
ii. information could cause harm to either the affected individuals physically, mentally, financially or cause them embarrassment.
iii. loss or breach could impact the provision of health care to the individual.

Exceptions (when you do not need to provide notice):

i. Information was encrypted when loss or breach occurred.
ii. Information was destroyed.
iii. Information was recovered without having been accessed.
iv. Information was accessed or disclosed to a person that is a custodian or affiliate that adheres to policies that are HIA compliant. This access was in line with the person's duties or used to disclose the information identify and address the breach.

c. Depending on the evaluated risk of harm, the privacy officer and custodian will notify the individual that is the subject of the breach and the OIPC and they may notify Chief and Council or other investigative bodies that a breach has occurred.

d. The results of the investigation will be communicated to appropriate staff (nurses, supervisory/managerial staff), and corrective action will be taken.

e. Any applicable disciplinary action will be applied by the appropriate supervisory/managerial staff.

13. Policy Review

a. All policy is to be reviewed annually to ensure that current practice, legislation and/or technology is reflected therein.

b. Periodically, at the discretion of the privacy officer and where significant changes to programs and/or practices are contemplated, a thorough risk assessment is to be conducted to determine the effectiveness of current policy and procedures as well as to identify gaps.

c. The privacy officer will also conduct ongoing ad hoc assessments of privacy risk and revise or update LRRCN policies as needed.

14. Compliance

Failure to comply with these guidelines is cause for disciplinary action, and where applicable, a complaint to the relevant legal authority, Privacy Commissioner, or equivalent data protection authority.

15. Enquires

All enquires about this policy should be directed to:

John D'or Prairie Health Centre
Privacy Officer: Kathy Hiebert, NIC
Telephone: 780-759-3773
Email: kathy.hiebert@canada.ca

Garden River Health Centre
Privacy Officer: Monique Barriault, NIC
Telephone: 780-659-3636
Email: monique.barriault@canada.ca

Fox Lake Nursing Station
Privacy Officer:
Telephone: 780-659-3730
Email:

Little Red River Cree Nation

Policy on Safeguards for Protecting Confidential Information

1. Introduction

Where Little Red River Cree Nation (LRRCN) collects personal information from clients, the organization has a responsibility to take all reasonable measures to safeguard that information.

The following guidelines detail the administrative, physical, and technical safeguards implemented by LRRCN to protect individual and client information.

2. Definitions

a. Confidential information, is not limited to, but includes:
   i. all health information pertaining to LRRCN's clients as defined by Alberta's *Health Information Act*;
   ii. all personal information as defined by the federal Privacy *Act* and the *Personal Information Protection and Electronic Documents Act;*
   iii. all protected employee information; and
   iv. all confidential business information.

3. Administrative Safeguards

a. Information privacy and security policies and procedures have been developed and are updated as necessary.
b. Only the least amount of information necessary for the intended purpose is collected, used and disclosed and only by those with a valid need-to-know.
c. Where possible, information will be made anonymous before use or disclosure.
d. Access to health information is restricted to staff who require access to the information in order to perform their job duties.
e. Confidentiality and security of information is addressed as part of the conditions of employment for new staff, and is written into job descriptions and contracts.
f. Staff are monitored for compliance with privacy and security policies and procedures.
g. All staff are required to review the privacy and security policies and procedures, and to sign off that they have read, understood, and will abide by them.
h. All staff are required to attend privacy and security training sessions on an annual basis at a minimum.
i. All staff, students, volunteers, and contracted personnel (e.g., janitors, temporary staff, etc.) are required to sign a Confidentiality Agreement.
j. Confidential information is not transmitted verbally if conversations can be overheard or intercepted.

k. Reception areas are staffed at all times during business hours. No one is permitted behind the reception desk without permission.
l. Patients and visitors are accompanied by a staff member to private or semi-private areas such as examination rooms and/or appropriate offices.
m. Television with closed-circuit health programming and/or overhead radio is played in waiting rooms and throughout all common areas to limit overhearing of personal, health and/or confidential information. All other reasonable steps will be taken to further limit the same (e.g., private offices used for consultation etc.).
n. Before implementing any new administrative practice or information system related to the collection, use and disclosure of health information, a privacy impact assessment (PIA) is completed and submitted to the Office of the Information and Privacy Commissioner (OIPC).
o. All PIAs are to be managed by the privacy officer with the aid of the Custodian and senior management team. PIAs are to be reviewed by this team along with all policy annually.
p. All privacy compliance issues, security breaches, and/or loss of information/equipment assets (including access control items such as keys or fobs) are documented in an incident report and reported to the privacy officer and Custodian and Nurse in Charge/Acting Nurse in Charge.
q. Confidential information is retained in accordance with the records retention provisions stated in *LRRCN's Confidential Information Guidelines* and in accordance with established standards.
r. HIA obligations are clearly passed along by way of contracts or other agreements with information managers, researchers, contractors, and recipients outside Alberta.
s. Management utilizes an arrival/departure checklist to manage and document access to information and/or information systems when staff is hired, their role changes, and/or upon termination.

4. Physical Safeguards

a. LRRCN records, both on-site and off-site, are held and stored in an organized, safe and secure manner.
b. Paper-copy patient charts are labeled using a code, instead of a patient name.
c. Rooms and cabinets used to store confidential information are locked when not in use.
d. Records storage areas are equipped with smoke detectors, fire extinguishers.
e. The distribution of keys is strictly controlled; keys are returned by staff after their employment has ended.
f. Building premises are protected by uniquely assigned building alarms. Alarm codes are disabled upon staff departure.
g. Confidential information is not left unattended in areas to which the public has access.
h. Computer monitors are positioned so that on-screen information cannot be viewed by passers-by.
i. Privacy screens are used where necessary to prevent individuals from viewing confidential information unless looking directly at the screen.

j. The electronic health information system's network server is located in a locked cabinet in a secured area; the room is locked when not in use.
k. When personal, health and/or confidential information is transported to another location, it is placed in a sealed envelope, marked as confidential, and directed to the attention of the authorized recipient.
l. LRRCN staff verifies the identity and credentials of courier services used for the transportation of personal, health and/or confidential information.
m. Patient charts are not to be removed from the building premises unless specifically authorized.
n. Fax machines are located in a secure area.
o. Pre-programmed numbers are used to send fax transmissions.
p. Pre-programmed numbers are reviewed every six months to ensure they are still accurate.
q. All fax transmissions are sent with a cover sheet that indicates the information being sent is confidential.
r. Reasonable steps are taken to confirm that personal, health and/or confidential information transmitted via fax is sent to a secure fax machine, and to confirm that the information was received.
s. Personal, health and/or confidential information in paper format with no archival value are disposed of by confidential shredding or burning.
t. Personal, health and/or confidential information with archival value are transferred to Indigenous Services Canada – Alberta region.
u. All files archived or disposed of are documented by listing the records/files to be archived/disposed, the identity of the subject individual, the nature of the information, recording the date, and having a staff member sign off that the transfer/disposal occurred.
v. All information is wiped clean prior to disposal of electronic data storage devices (e.g., surplus computers, internal and external hard drives, diskettes, tapes, CD-ROMS, etc.), or the device(s) are destroyed.

5. Technical Safeguards

a. All paper or electronic information systems users are assigned a unique identifier (User ID) that restricts access to health information and systems that are required for the administration of their duties.
b. Access to electronic health information systems is password protected.
c. Passwords are kept confidential at all times and are not to be written down, posted publicly, or shared with other staff.
d. Passwords for electronic health systems are changed every three months.
e. Screen saver passwords are used to protect against unauthorized access if a computer is left unattended.
f. Confidential information sent via email over public or external networks is encrypted.
g. Information systems are audited to detect unauthorized access and prevent modification or misuse of health information.
h. Audit trails are reviewed every month, and on an incident basis.

i. Health information is protected from unauthorized external access by a firewall.
j. Virus scanning software is installed to protect health information from unauthorized modification, loss, access or disclosure.
k. Electronic health information systems, once deployed, are backed up nightly.
l. Back-up information is stored in a secure, locked environment off- site. Information intended for long-term storage on electronic media (e.g., tape, DVD, disk) is reviewed on an annual basis to ensure the data is retrievable, and to migrate the data to another storage medium if necessary.

6. Compliance

Failure to comply with these guidelines is cause for disciplinary action, and where applicable, a complaint to the relevant legal authority, Privacy Commissioner, or equivalent data protection authority.

7. Enquires

All enquiries about these guidelines should be directed to:

John D'or Prairie Health Centre
Privacy Officer: Kathy Hiebert, NIC
Telephone: 780-759-3773
Email: kathy.hiebert@canada.ca

Garden River Health Centre
Privacy Officer: Monique Barriault, NIC
Telephone: 780-659-3636
Email: monique.barriault@canada.ca

Fox Lake Nursing Station
Privacy Officer:
Telephone: 780-659-3730
Email:

Little Red River Cree Nation
Policy on Access to Personal Health Information

Purpose

Subject to limited and specific exceptions in the *Health Information Act* (HIA), individuals have a right of access to information about themselves, and the right to request corrections or amendments to this information. This procedure is intended to define a process for facilitating requests for access to and correction of an individual's own health information.

1. General Procedures

a. During the provision of health services, Little Red River Cree Nation staff will share information verbally with the patient or authorized representative and allow access to his/her health information records when practical.

b. When an individual or authorized representative asks for a correction of factual information and can substantiate that the information is incorrect, staff will make the correction to the medical record. (Examples include name, address, telephone number and other demographic information)

c. All requests to access and/or correct health information is to be documented by LRRCN's Privacy Officer, along with pertinent information about the request, the requestor, and any action taken.

d. LRRCN Privacy Officer is to notify relevant custodians of all access and/or correction requests and subsequent action.

2. Procedure to Request Access to Information

a. When access cannot be provided under section 1(a) of this procedure, patients may make a request for access to information in writing. An individual may request access to another person's information only if they are an ***authorized representative***.

b. All written requests for access should be directed to LRRCN Privacy Officer who will determine the appropriate course of action along with the senior management team and/or appropriate custodian where possible.

c. All requests for access to information will be processed in accordance with procedures set out in the HIA and fees may be charged in accordance with the Health Information Regulation. Any health information or personal information about individuals other than the applicant will be severed before disclosure of the records. Requests will be processed within 30 days of receipt.

d. A staff member shall be present if the applicant views the original record in order to answer questions and maintain the integrity of the record.

3. Authentication of Recipient

a. When an authorized representative requests an individual's health information, and is not known to LRRCN, proof of authority may be requested. This may involve asking for a copy of such documents as a guardianship order, power of attorney, personal directive or letters of administration for an estate.

b. Nursing Station staff shall take reasonable steps to verify the identity of the individual or authorized representative before disclosing health information. This may involve looking at a driver's license or other identification.

4. Procedure to Request Correction of Health Information

a. When information cannot be corrected under section 1(b) of this procedure, an individual may make a request for correction or amendment in writing. An individual may request a correction to another person's information only if they have written authorization of the individual the information is about or are an authorized representative.

b. The relevant custodian will review the records to determine whether the request is to be granted or refused. Corrections will only be made to factual information. Corrections cannot be made to professional opinions or observations. The correction process must be completed within 30 days of receipt of the request for correction and in compliance with the rules in the HIA.

c. If a correction is refused, the applicant may provide a Statement of Disagreement of not more than 500 words and this will be placed on the medical record, or the applicant may request the Information and Privacy Commissioner to review the decision.

d. If a correction is made to the record, or a Statement of Disagreement received, the Nursing Station will provide the corrected information or a copy of the statement to any person to whom the record was disclosed in the previous 12 months.

5. Enquires

All enquires about this policy should be directed to:

John D'or Prairie Health Centre
Privacy Officer: Kathy Hiebert, NIC
Telephone: 780-759-3773
Email: kathy.hiebert@canada.ca

Garden River Health Centre
Privacy Officer: Monique Barriault, NIC
Telephone: 780-659-3636
Email: monique.barriault@canada.ca

Fox Lake Nursing Station
Privacy Officer:
Telephone: 780-659-3730
Email:

Little Red River Cree Nation
Privacy Notice

The health information that we are collecting is needed to provide you with diagnostic, treatment, and care services or for other authorized purpose(s) under section 27 of the Health Information Act. It is collected under the authority of section 20(b) of the Health Information Act -- directly related to and necessary to carry out an authorized purpose under section 27.

The confidentiality of this health information and your privacy are protected by the provisions of the Health Information Act.

All Little Red River Cree Nation staff are required to treat all personal and health information as strictly confidential.

If you have any questions about this collection and use of your health information, please talk with anyone of our staff or to our Privacy Officers:

Little Red River Cree Nation
PO Box 30 – John D'or Prairie, Alberta – T0H 3X0

John D'or Prairie Health Centre
Privacy Officer: Kathy Hiebert, NIC
Telephone: 780-759-3773
Email: kathy.hiebert@canada.ca

Garden River Health Centre
Privacy Officer: Monique Barriault, NIC
Telephone: 780-659-3636
Email: monique.barriault@canada.ca

Fox Lake Nursing Station
Privacy Officer:
Telephone: 780-659-3730
Email:

Little Red River Cree Nation

Security Procedures for the Protection of Information Technology

1. Introduction

The following procedures are meant to formalize and document the safeguards Little Red River Cree Nation (LRRCN) has implemented to protect technology assets (computers, etc.) as well as the information housed therein.

2. Scope

These procedures outline responsibilities of LRRCN Information Technology (IT) staff and/or contractors charged with the installation, security, and maintenance of all information environments, networks, applications, and electronic devices (herein after referred to as LRRCN's electronic systems).

All staff, contractors or others accessing LRRCN's electronic systems (herein after referred to as System Users) must support and respect security measures and comply with LRRCN's Guidelines on Acceptable Uses of Electronic Systems and all privacy safeguards and guidelines.

3. System Description

LRRCN maintains two networks that are both logically and physically separated. One of these networks is dedicated for the sole use of the LRRCN (not wireless). The second network (mainly wired, but with controlled building-wide wireless as well) is for the remaining LRRCN programs and staff.

While some of the safeguards identified here may not apply to all networks based on connectivity type or specific Nursing Station requirements, they collectively ensure the security of LRRCN's electronic systems.

4. Administrative Safeguards

4.1. IT staff are to complete an inventory of technology assets (computers, mobile phones, etc.) operating on LRRCN's electronic system. The inventory is to be updated as necessary and reviewed at least annually.

4.2. Network settings, including access points and system passwords, are to be documented. All system documentation shall be securely maintained (e.g., locked or password protected) and a duplicate copy is to be securely maintained off-site for disaster recovery purposes.

4.3. Network access points, wired and wireless, are disabled when not in use.

4.4. All systems are routinely scanned for rogue and unauthorized devices.

4.5. Bandwidth and connectivity is monitored to ensure network integrity. Thresholds breaches and email alerts are sent to a authorized local staff member.

4.6. IT security training material for all staff is to be developed and updated regularly.

4.7. All system users with mobile devices will be provided specific training on mobile computing to ensure physical, technical, and administrative safeguards are implemented.

5. Physical Safeguards

5.1. All security systems are employed at all times.

5.2. Reception areas are staffed at all times during business hours. No one is permitted behind the reception desk without permission.

5.3. The building remains locked during non-business hours.

5.4. The distribution of access control items (keys, identification badges, access cards, fobs, security tokens, security alarm codes, computer passwords etc.) is strictly controlled. Upon termination of staff employment such items are returned and/or reset/cancelled (eg. passwords, alarm codes as needed).

5.5. Building premises are protected by building alarms. Alarm codes are specific to the individual and assist in identifying who has accessed the building and when. The code is then deactivated when the corresponding key is no longer active.

5.6. All areas housing critical and/or sensitive electronic systems are equipped with smoke detectors, and fire extinguishers when possible.

5.7. Connectivity related network infrastructure is securely maintained in a restricted location.

6. Technical Safeguards

6.1 Router

6.1.1 An active firewall has been installed.

6.1.2 Router passwords have been changed from default settings.

6.1.3 Administrator password of the router and network has been synchronized.

6.1.4 Wireless access is password protected using an alphanumeric password.

6.1.5 Systems, networks, and/or drivers are updated regularly.

6.1.6 Simple Network Management Protocol is disabled on all computers/networks accessing Netcare.

6.2 Electronic Devices

6.2.1 Computers and all other applicable devices will be locked to only connect to pre-defined authorized networks.

6.2.2 All computers (and other applicable devices) will have enabled the built-in firewall.

6.2.3 Anti-virus protection installed on all computers with automatic updates (as well as automatic updates installed).

6.2.4 All mobile computing devices accessing confidential information (laptops, PDAs, smart phones, memory sticks, etc.) require layered security protection.

6.3 Technical Safeguards for Computers/Systems Accessing Electronic Health Records

6.3.1 Information systems users are assigned a unique identifier (User ID) that restricts access to each data and application systems to that information required for the administration of their duties. Use of user IDs other than that assigned to an individual is prohibited.

6.3.2 System administrators must each have an administrator account for performing system administration and a limited privilege account for performing non-system administration tasks.

6.3.3 Passwords are to be kept confidential at all times and should not be written down, posted publicly, or shared with other staff except for security purposes. Unique passwords or other authentication controls are required for each desktop, network, server, information system, etc. A strong password standard is used. Passwords for the Windows Operating System and any EMR are changed every 120 days, as prompted by the system.

6.3.4 All monitors used to display Netcare, or other identifying health information will time out after 5 minutes of inactivity and require entry of a password to reactivate the screen. All computers are logged off at the end of the business day.

6.3.5 Each user should have a unique user login and password to access the computer network. User rights and accounts will be assigned and maintained by the clinic's privacy officer. Installation or alteration to system software and hardware will be the responsibility of the clinic's executive director who will ensure that original master copies of software are stored with proper physical controls.

6.3.6 Clinic administrative data (e.g., emails, contact lists, Microsoft documents, etc.) will be backed up daily by the clinic.

6.3.7 The clinic will use an internet service provider to access provincial and regional EHRs. The access will be by a router which acts as a hardware firewall and is regularly patched using approved vendor patches. Each computer in the network has Antivirus that is updated automatically. Patches are applied regularly with critical patches applied as soon as they are released.

6.3.8 The clinic may request access to Netcare for authorized staff. All users will have unique authentication fobs. Alberta Netcare has built the security controls into the system – e.g., use of two factor authentication, encryption of all electronic messages, use of firewalls and intrusion detection systems, logging of all access to the system, and regular auditing. User access is based on role and profession to ensure that users can access the information they need to do their job but, on a need-to-know basis.

7. Compliance

Failure to comply with these guidelines is cause for disciplinary action, and where applicable, a complaint to the relevant legal authority, Privacy Commissioner, or equivalent data protection authority.

Little Red River Cree Nation

Guidelines on Acceptable Uses of Networks and Electronic Devices

1. Introduction

The following guidelines outline requirements and expectations of those accessing Little Red River Cree Nation 's (LRRCN's) information environments, networks, applications, and electronic devices (herein after referred to as LRRCN's electronic systems).

2. Scope

Adherence to this protocol is required for any access to LRRCN's electronic systems.

These guidelines apply to all staff, contractors or others accessing LRRCN's electronic systems (herein after referred to as System Users).

The use of any electronic device, including personal devices, which are used at LRRCN or in the conduct of LRRCN business, is subject to these guidelines.

3. General Requirements

All System Users are responsible for exercising good judgment regarding appropriate use of resources in accordance with all policies, protocols, standards, and guidelines. LRRCN resources may not be used for any unlawful or prohibited purpose.

For security, compliance, and maintenance purposes, authorized personnel may monitor and audit LRRCN's electronic systems. Devices found to interfere with LRRCN's electronic systems, or users of such systems may be disconnected.

4. System Accounts

4.1 System Users are responsible for the security of data, accounts, and systems under their control.

- Passwords are to be kept confidential and secure.
- Providing access to another individual, either deliberately or through failure to secure its access, constitutes a violation of these guidelines.

5. Remote Access

5.1 Unless specifically authorized, System Users are prohibited from storing any client information on personal computers and/or within non-LRRCN controlled environments, including devices maintained by unauthorized third parties.

5.2 Remote access to LRRCN computers and/systems is permitted as authorized. Note that no information is to be stored locally (i.e., On the computer used to access the LRRCN computer).

5.3 Mobile devices such as, but not limited to, flash drive devices are not to be used for the storage or transport of sensitive LRRCN information, including personal and/or health information.

5.4 If mobile devices are authorized for storing, accessing and/or transporting sensitive data, the data is to be encrypted.

6. Computing Assets

6.1 System Users are responsible for ensuring the protection of assigned assets. Any theft or loss of assets is to be reported immediately.

6.2 Devices including computers, personal digital assistants (PDAs), cell phones, laptops, and workstations must be secured with a password-protected screensaver. Screens must be locked or users logged off when the device is unattended.

6.3 Interference with corporate device management or security system software, including, but not limited to, antivirus software is strictly prohibited.

7. Network Use

7.1 System Users are responsible for the security and appropriate use of network resources under their control.

7.2 The following uses of networks and/or resources are strictly prohibited:

- Breaching implemented security, including, but not limited to, accessing data, servers, or accounts without authorization; circumventing user authentication on any device; or intercepting network traffic.
- Disrupting technical services, including, but not limited to, forging routing information for malicious purposes.
- All violations of copyright law, including, but not limited to, illegally duplicating or transmitting copyrighted pictures, music, video, and software. Exporting or importing software, technical information, encryption software, or technology in violation of international or regional export control laws.
- Use of the Internet or LRRCN network that violates LRRCN's policies or local laws.

- The intentional introduction of malicious code, including, but not limited to, viruses, worms, Trojan horses, spyware, adware, and keyloggers.
- Port or security scanning unless authorized in advance and in writing.

8. Electronic Communications

8.1 The following are strictly prohibited:

- The use of non-LRRCN provided or approved email accounts to conduct LRRCN business.
- Inappropriate use of communication vehicles and equipment, including, but not limited to, supporting illegal activities, and procuring or transmitting material that violates LRRCN policies against harassment or the safeguarding of information.
- Sending spam via e-mail, text messages, pages, instant messages, voice mail, or other forms of electronic communication.
- Forging, misrepresenting, obscuring, suppressing, or replacing a user identity on any electronic communication to mislead the recipient about the sender.
- Posting the same or similar non-business-related messages to large numbers of groups.
- Use of an LRRCN e-mail or IP address to engage in conduct that is ethically questionable, unlawful, or violates LRRCN policies and protocols.

8.2 If posting to a public newsgroup, bulletin board, or information portal with an LRRCN e-mail or IP address, caution should be exercised to avoid misrepresenting or exceeding authority in representing the organization.

9. Use of Electronic Devices with Clients Present

9.1 Only those applications directly related to the particular service being delivered may be accessed with a client present.

9.2 Where web-enabled devices are utilized to access applications, care must be exercised to ensure that no confidential information is stored or transmitted unless specifically authorized.

9.3 No LRRCN staff may take and/or utilized for personal purposes images which include LRRCN clients, Little Red River Cree Nation community members, or any circumstance encountered in the completion of assigned duties.

9.4 All images captured by LRRCN staff must be directly related to assigned duties and where applicable, must be accompanied by signed consent forms.

9.5 No images captured by LRRCN staff related to LRRCN or their work within, may be publicly posted or disclosed without expressed authorization.

10. Terminology

Adware: any software which automatically plays, displays, or downloads advertisements to a computer after the software is installed on it.

Forged Routing Information: conceals the identity of the sender or impersonates another computing system.

Keylogging: is the practice of noting (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored.

Port/Security Scanning: used by administrators to verify security policies of their networks and by hackers to identify running services on a host with the view to compromising it.

Spyware: malicious software that is installed on computers and that collects information about users without their knowledge.

Trojan Horse: malicious software that appears, to the user, to perform a desirable function but, in fact, facilitates unauthorized access to the user's computer system.

Virus: a computer program that can copy itself and infect a computer, corrupting or destroying files on that computer.

Worm: a self-replicating computer program. It uses a network to send copies of itself to other computers on the network and it may do so without any user intervention.

11. Compliance

Failure to comply with these guidelines is cause for disciplinary action, and where applicable, a complaint to the relevant legal authority, Privacy Commissioner or equivalent data protection authority.

12. Enquires

All enquires about this policy should be directed to:

John D'or Prairie Health Centre
Privacy Officer: Kathy Hiebert, NIC
Telephone: 780-759-3773
Email: kathy.hiebert@canada.ca

Garden River Health Centre
Privacy Officer: Monique Barriault, NIC
Telephone: 780-659-3636
Email: monique.barriault@canada.ca

Fox Lake Nursing Station
Privacy Officer:
Telephone: 780-659-3730
Email:

Little Red River Cree Nation
Guidelines for the use of Medical Records

1. Purpose

These guidelines are meant to:

a. Document practices as related to confidential information used outside the Nursing Station's premises.
b. Provide guidance to staff as they address challenges associated with handling such records.
c. Achieve statutory and regulatory compliance.

2. Application

These guidelines apply to all staff, contractors, volunteers, or others who may collect or use confidential information on behalf of the Nursing Station outside of its premises.

3. Definitions

a. Confidential information, is not limited to, but includes:
    i. all health information pertaining to clients as defined by Alberta's *Health Information Act* ;
    ii. all personal information as defined by the federal *Privacy Act* and the *Personal Information Protection and Electronic Documents Act;*
    iii. all protected employee information; and
    iv. all confidential business information.

b. Mobile records include all confidential information as here defined which are collected, used, or in any way accessed by staff outside of Nursing Station premises.

4. Existing Policy and Procedures

a. All users of mobile records must comply with the existing Nursing Station polices and guidelines which outline processes for the handling of confidential information including its collection, use, storage, retention, and destruction as well as the transmitting of confidential information by way of fax and email:
    i. Confidential Information Guidelines,
    ii. Policy on Safeguards for Protecting Confidential Information,
    iii. Policy on Access to Personal Health Information,
    iv. Procedure for Provincial Electronic Health Record (Netcare) use, and

v. *Guidelines on Acceptable Uses of Networks and Electronic Devices.*

b. The *Security Procedures for the Protection of Information Technology* applies to all computers which may access health information, or systems in which such information is contained, including Alberta Netcare.

c. In addition, policies and procedures, the *Privacy and Management of Health Information Standards for CARNA's Regulated Members* as well as the provisions of Alberta's *Health Information Act* apply to all community-based health services.
    i. Note that care has been taken to ensure consistency between the Act, CARNA's standards (both of which identify requirements to develop policies and procedures regarding the handling of health information and the protection of the same) and the Nursing Station's policies (which meet these requirements).

5. Guidelines for Mobile Records in Electronic Form

a. Confidential information may only be accessed, collected remotely, or removed from the Nursing Station premises as authorized.

b. All policies regarding the protection of confidential information apply regardless of the site and/or method of collection.

c. Only the minimum amount of confidential information necessary to complete the job function should be collected and/or used remotely.

d. Electronic collection and/or use is preferred for all mobile records.

e. Where possible and appropriate, health staff, when outside of the health centre premises, are to utilize available information technology to access necessary health information remotely rather than physically removing confidential information from the health centre.

f. Confidential information accessed remotely on electronic systems will be:
    i. Encrypted during transmissions or when stored electronically at the provider location;
    ii. Accessed through use of a username and strong password specific to the provider;
    iii. Stored locally, when required, on a locked device or storage location, protected from unauthorized access.

g. Mobile records must be protected at all times. Specifically, the devices or containers containing mobile records must:
    i. Be kept in sight of the individual responsible for them when not protected or secured;
    ii. Be transported in a secured or encrypted format;
    iii. Be transported in a vehicle which remains locked at all times;

iv. Be returned to the health centre at the earliest opportunity;
v. Be kept in a secure and locked facility if return to the health centre is not possible or practical.

h. Mobile drives are not to be used to transport and/or store confidential records unless specifically authorized. All information stored on such devices is subject to 4(c) above and must be encrypted.

6. Remote Access to Alberta Netcare or Health Information Systems

a. Should it become necessary to access Alberta Netcare, or any other system containing health information, remotely (i.e., by on-call health professionals), care must be exercised to ensure that no unauthorized persons have access to the health information contained therein. For instance:
   i. No unauthorized persons should be present when health information is accessed;
   ii. The devise used to access health information must be used by authorized personnel only;
   iii. The remote access should occur only in a location that is private and reasonably secure (such as a home office).

b. Computers used to access Alberta Netcare remotely must only use a secure wired internet connection.

c. Any material printed or transcribed from Alberta Netcare constitutes part of a client's medical record and must be safeguarded accordingly.

   i. Where a health professional is providing medical advice or consulting services from outside the community health centre, the office from where services are provided will be the primary location housing health information.
   ii. All existing policy and procedures (outlined in 4 above) also apply to health information stored in these remote offices.

7. Guidelines for Paper-based Mobile Records

a. Confidential information may only be accessed, collected remotely, or removed from Nursing Station premises as authorized.

b. All policies regarding the protection of confidential information apply regardless of the site and/or method of collection.

c. Only the minimum amount of confidential information necessary to complete the job function should be collected and/or used remotely.

d. Mobile records must be protected at all times. Specifically, confidential information must:
   i. Be kept in sight of the individual responsible for them when not protected or secured;

ii. Be transported in a secured case;
iii. Be transported in a vehicle which remains locked at all times;
iv. Be returned to the Nursing Station at the earliest opportunity;
v. Be kept in a secure and locked facility if return to the health centre is not possible or practical and expressed authorization has been granted.

8. Enquires

All enquires about these guidelines should be directed to:

John D'or Prairie Health Centre
Privacy Officer: Kathy Hiebert, NIC
Telephone: 780-759-3773
Email: kathy.hiebert@canada.ca

Garden River Health Centre
Privacy Officer: Monique Barriault, NIC
Telephone: 780-659-3636
Email: monique.barriault@canada.ca

Fox Lake Nursing Station
Privacy Officer:
Telephone: 780-659-3730
Email:

Little Red River Cree Nation

Procedure for Electronic Health Information System Use

1. Purpose

This procedure is meant to provide guidance to staff accessing the Community Health and Immunization Program (CHIP) and/or Diabetes Case Assessment, Response, and Evaluation (CARE), and/or other electronic health information systems in relation to their handling of confidential information contained therein.

2. Definitions

a. Confidential information, is not limited to, but includes:
   i. all health information pertaining to LRRCN's clients as defined by Alberta's *Health Information Act* ;
   ii. all personal information as defined by the federal *Privacy Act* and the *Personal Information Protection and Electronic Documents Act;*
   iii. all protected employee information; and
   iv. all confidential business information.

b. The Community Health and Immunization Program (CHIP) system refers to the electronic system that LRRCN is using to manage immunization information.

c. The Diabetes Case Assessment, Response and Evaluation (CARE) system refers the electronic system that LRRCN is using to manage diabetes and potential associated complication information.

3. Procedures

d. All users of the CHIP and/or Diabetes CARE system must comply with the following LRRCN polices and guidelines which outline processes for the handling of confidential information including its collection, use, storage, retention, and destruction as well as the transmitting of confidential information by way of fax and email:
   i. Confidential Information Guidelines,
   ii. Policy on Safeguards for Protecting Confidential Information,
   iii. Policy on Access to Personal Health Information,
   iv. Mobile Record Guidelines, and
   v. Guidelines on Acceptable Uses of Networks and Electronic Devices.

e. LRRCN must apply the *Security Procedures for the Protection of Information Technology* to all computers which may access the CHIP and/or Diabetes CARE systems.

f. In addition to LRRCN policies and procedures, the *Privacy and Management of Health Information Standards for CARNA's Regulated Members* as well as the provisions of Alberta's *Health Information Act* apply to all community health programs.

i. Note that care has been taken to ensure consistency between the Act, CARNA's standards (both of which identify requirements to develop policies and procedures regarding the handling of health information and the protection of the same) and LRRCN policy (which meet these requirements).

4. Enquires

All enquires about this procedure, the use of the CHIP system, or immunization information should be directed to:

Dr. Christopher Sarin, MD
Interim Custodian Little Red River Cree Nation – Community Health
PH: 403-613-4169
Email: chris.sarin@canada.ca

All enquires about this procedure; the use of the CARE system should be directed to:

Ojotule Obi-Egwale RN BScN, Home Care
Little Red River Cree Nation
PH: 780-759-2347 Ext 1416
Email: tobiegwale@lrrcn.ab.ca

Little Red River Cree Nation
Research Policy

1. Introduction

Alberta's *Health Information Act* (HIA) contains provisions that expressly govern the disclosure of health information for research purposes.

The following policy details the process by which Little Red River Cree Nation (LRRCN) will respond to or engage in research activities.

2. Definitions

a. Confidential information, is not limited to, but includes:
   i. all health information pertaining to LRRCN's clients as defined by Alberta's *Health Information Act* ;
   ii. all personal information as defined by the federal *Privacy Act* and the *Personal Information Protection and Electronic Documents Act;*
   iii. all protected employee information; and
   iv. all confidential business information.

b. Research is defined as "academic, applied or scientific research that necessitates the use of individually identifying health information" [*HIA* s1(1)(v)].

3. Policy Statement

a. A person who intends to conduct research using health information in the custody or control of a custodian or health information repository must submit a research proposal to a research ethics board (REB) identified in the HIA[1] for review. If a board is satisfied with the proposal the researcher may then approach custodians to ask for disclosure of health information.

b. Prior to responding to a research request, management is encouraged to review further information about steps to take when dealing with such a request in the *HIA Guidelines and Practices Manua*l section 8.15.

[1] REB's identified in the Act include those listed here as well as any having successfully applied to the Minister of Health for such designation.

- Health Research Ethics Board of Alberta;
- University of Alberta – Health Research Ethics Board;
- University of Calgary – Conjoint Health Research Ethics Board.

4. Procedures

a. A custodian may use individually identifying health information in its custody or under its control for the purpose of conducting research or facilitating another person's research [*HIA* s27(1)(d)]:

- if the custodian or researcher has submitted a proposal to a research ethics board;
- if the research ethics board is satisfied with the research proposal;
- if the custodian or researcher has complied with or undertaken to comply with the conditions, if any, suggested by the research ethics board; and
- if the custodian has obtained consent, when recommended by the research ethics board, from the individuals who are the subjects of the health information (subject individuals) to be used in the research.

b. If a research ethics board is satisfied with the proposal, the researcher may then provide the following documents to one or more custodians or a health repository:
- their research proposal;
- the board's response to the researcher's proposal; and
- a written application for disclosure of health information to be used in the research, performance of data matching and/or performance of any other service to facilitate research.

c. Upon receipt of the researcher's application and research documents listed in b above, the Privacy Officer, in consultation with the relevant custodian(s), will decide whether to disclose the health information to the researcher or perform services to facilitate the research. The custodian does **not have** to disclose the information.

d. If the Privacy Officer decides to disclose the health information or perform data matching or other services to facilitate the research, the custodian **must impose** on the researcher the conditions suggested the research ethics board and **may impose** other conditions on the researcher. If the board recommended that consents be obtained, the researcher must obtain the consents **before** the disclosure of health information, performance of data matching, or provision of other services.

e. If the Privacy Officer decides to disclose the health information for research purposes, the researcher must enter into an agreement with the relevant custodian in which the researcher agrees to:
- comply with:
  - the provisions of the *HIA* and any applicable Regulations;
  - any conditions imposed by the custodian regarding the use, protection, disclosure, return or disposal of the information;
  - any requirements to provide safeguards against the identification of the subject individuals or community sites;
  - to use the health information only for research purposes;
- ensure that the information is not published in any form that could lead to the identification of any of the subject individuals involved;
- only contact subject individuals for additional information, when the Health Center has first obtained the individual's consent to being contacted for that purpose;

- pay any costs associated with accessing the information;
- provide the Custodian with the proposed report (or publication) of the results of the research for the Custodian's review. The report (or publication) must include a statement that some of the information used in the study was provided by the Custodian as well as any comments expressed by the Custodian and/or community about the research findings.

f. When a research agreement has been entered into by the custodian, LRRCN may then disclose to the researcher the health information requested, or perform data matching, or other services to facilitate the research. This is to be done with the consent of the subject individuals where recommended by the research ethics board, and without consent where recommended by the research ethics board.

g. If the researcher contravenes or fails to meet the terms and conditions of the agreement with the custodian, the agreement is cancelled.

4. Enquires

All enquires about these guidelines should be directed to:

John D'or Prairie Health Centre
Privacy Officer: Kathy Hiebert, NIC
Telephone: 780-759-3773
Email: kathy.hiebert@canada.ca

Garden River Health Centre
Privacy Officer: Monique Barriault, NIC
Telephone: 780-659-3636
Email: monique.barriault@canada.ca

Fox Lake Nursing Station
Privacy Officer:
Telephone: 780-659-3730
Email:

Little Red River Cree Nation

Policy on the Use of social media

1. Introduction

Social media has become a powerful and useful tool for Little Red River Cree Nation (LRRCN) to connect with the population it serves.

The following policy details the appropriate uses of such media by LRRCN's staff when representing the organization as well as the reasonable limits to the use of client information collected by way of such media.

2. Definitions

a. Confidential information, is not limited to, but includes:
   i. all health information pertaining to LRRCN's clients as defined by Alberta's *Health Information Act*;
   ii. all personal information as defined by the federal *Privacy Act* and the *Personal Information Protection and Electronic Documents Act;*
   iii. all protected employee information; and
   iv. all confidential business information.

b. Social media refers to forms of electronic communication (such as Facebook or Twitter) through which users create online communities to share information, ideas, personal messages, and other content (as videos).

3. Procedures

a. All staff must comply with the following LRRCN polices and guidelines which outline processes for the handling of confidential information including its collection, use, storage, retention, and destruction as well as the transmitting of confidential information electronically:
   i. Confidential Information Guidelines,
   ii. Policy on Safeguards for Protecting Confidential Information,
   iii. Policy on Access to Personal Health Information,
   iv. Mobile Record Guidelines, and
   v. Guidelines on Acceptable Uses of Networks and Electronic Devices.

b. LRRCN must apply the *Security Procedures for the Protection of Information Technology* to all computers.

c. Only sites approved by the Custodian and privacy officer can be used for the purpose of advertising events at LRRCN (e.g., the availability of the annual influenza vaccine or prenatal classes).

d. All mass-scale outgoing communication regarding LRRCN's events or activities must originate from an account approved by LRRCN.

e. If individual staff members receive, on personal social media accounts, specific questions about LRRCN, including events and activities, care must be exercised to ensure that no confidential information is exchanged by way of social media platforms.

f. Information collected about LRRCN clients by way of a personal relationship (online or otherwise) with a staff member is not to be used at or by LRRCN nor treated as a sanctioned method of collecting health information.

5. Enquires

All enquires about these guidelines should be directed to:

John D'or Prairie Health Centre
Privacy Officer: Kathy Hiebert, NIC
Telephone: 780-759-3773
Email: kathy.hiebert@canada.ca

Garden River Health Centre
Privacy Officer: Monique Barriault, NIC
Telephone: 780-659-3636
Email: monique.barriault@canada.ca

Fox Lake Nursing Station
Privacy Officer:
Telephone: 780-659-3730
Email:

Little Red River Cree Nation

Procedure for Provincial Electronic Health Record (Netcare) Use

1. Purpose

This procedure is meant to provide guidance to health centre custodians (i.e., registered nurses who are members of CARNA) accessing Alberta's provincial electronic health record (Netcare), and outlines the administrative, physical, and technical safeguards that must be in place. These apply to any person or computer accessing Netcare information and are in addition to policies and procedures already in place.

2. Definitions

a. Confidential information, is not limited to, but includes:
   i. all health information pertaining to Little Red River Cree Nation (LRRCN) clients as defined by Alberta's *Health Information Act*;
   ii. all personal information as defined by the federal Privacy *Act* and the *Personal Information Protection and Electronic Documents Act;*
   iii. all protected employee information; and
   iv. all confidential business information.

3. Existing Policy and Procedures

a. All users of Netcare must comply with the existing LRRCN polices and guidelines which outline processes for the handling of confidential information including its collection, use, storage, retention, and destruction as well as the transmitting of confidential information by way of fax and email:
   i. Confidential Information Guidelines,
   ii. Policy on Safeguards for Protecting Confidential Information,
   iii. Policy on Access to Personal Health Information,
   iv. Mobile Record Guidelines, and
   v. Guidelines on Acceptable Uses of Networks and Electronic Devices.

b. LRRCN must apply the *Security Procedures for the Protection of Information Technology* to all computers which may access Netcare.

c. In addition to LRRCN policies and procedures, the *Privacy and Management of Health Information Standards for CARNA's Regulated Members* as well as the provisions of Alberta's *Health Information Act* apply to all community health programs.
   i. Note that care has been taken to ensure consistency between the Act, CARNA's standards (both of which identify requirements to develop policies and procedures regarding the handling of health information and the protection of the same) and LRRCN policy (which meet these requirements).

4. Netcare Specific Safeguards

4.1 Administrative Safeguards

a. Information privacy and security policies and procedures have been developed by the Health Director and primary custodian and are updated, as necessary.
b. There is a designated Privacy Officer and Technical Administrator(s) for Netcare computers.
c. Staff are monitored for compliance with privacy and security policies and procedures by the Health Director and Nurse in Charge.
d. The technical administrator and all staff are required to review the privacy and security policies and procedures at the time of employment and at a minimum annually, and to sign off that they have read, understood, and will abide by them.
e. When terminating the employment or contract of a Netcare user, their system access and control items (keys, badges, access cards, fob etc.) must be revoked and retrieved as required.

4.2 Physical Safeguards

a. Access to Netcare will only take place in Health Center premises.
b. On-call health professionals must apply the *Mobile Record Guidelines* when remotely accessing Netcare.
c. Any servers, storage devices, networking equipment, must be locked in a secure area.
d. Computers use for Netcare access must be clearly designated.
e. Computers must be cabled for access to Netcare. There will be no wireless access.
f. Laptops cannot be used for Netcare access outside the health centre, and if used, must be physically secured to prevent theft.
g. Computer monitors are positioned so that on-screen information cannot be viewed by passers-by.
h. Privacy screens are used where necessary to prevent individuals from viewing confidential information unless looking directly at the screen.
i. All information is wiped clean prior to disposal of electronic data storage devices (e.g., surplus computers, internal and external hard drives, diskettes, tapes, CD-ROMS, etc.), or the device(s) are destroyed.

4.3 Technical Safeguards

a. Screen saver passwords are used to protect against unauthorized access if a computer is left unattended, with a maximum inactivity timeout of 30 minutes.
b. Computers with access to Netcare are password protected, using a strong password that is directly tied to a unique user.
    i. Minimum length of 8 characters
    ii. No embedded part of user's name
    iii. A combination of 3 of the 4: alpha-upper case, alpha-lower case, numeric and special characters
    iv. Passwords only valid for 90 days
    v. 24 iterations before old passwords are reused.
    vi. 5 maximum invalid attempts before account is locked out for 30 minutes.

c. Passwords are kept confidential at all times and are not to be written down, posted publicly, or shared with other staff.
d. Passwords are stored and transmitted in an encrypted format.
e. Computers with access to Netcare will only have authorized software installed. The custodian will determine what software is acceptable for these devices.
f. Only the designated Technical Administrator(s) are allowed to install software and will perform audits to verify compliance.
g. Users will have limited access (not able to install software) accounts when accessing Netcare.
h. Confidential information sent via email over public or external networks is encrypted.
i. Health information is protected from unauthorized external access, at minimum, by a local computer-based firewall which is managed by the technical administrator.
j. Virus scanning software is installed which automatically updates and scans devices at regular intervals.
k. Computer operating system is setup to automatically update and install all patches.
l. If laptops are used for Netcare access within the health centre, they must have full drive encryption to prevent privacy breaches in the event of theft.

6. Compliance

Failure to comply with this policy is cause for disciplinary action, and where applicable, a complaint to the relevant authorities and Privacy Commissioner.

Any actual or suspected breach involving Netcare must be reported to Netcare's Information Access and Privacy Office.

7. Enquires

All enquiries about these guidelines should be directed to:

Dr. Christopher Sarin, MD
Interim Custodian Little Red River Cree Nation – Community Health
PH: 403-613-4169
Email: chris.sarin@canada.ca

Ojotule Obi-Egwale RN BScN, Home Care
Little Red River Cree Nation
PH: 780-759-2347 Ext 1416
Email: tobiegwale@lrrcn.ab.ca