Policy Section:	Effective Date:	Reviewed Date:	Approved By:
Organizational	December 2024		Board of Directors

Privacy Policy

POLICY STATEMENT

Ancient Rivers Family Health Team (ARFHT) is committed to keeping clients' personal health information safe and confidential.

ARFHT collects, uses and discloses of this information in compliance with the *Personal Health Information Protection Act 2004*, by the implementation of the following privacy principles:

Principle 1 – Accountability for Personal Health Information

ARFHT is responsible for the personal health information under its control. The Executive Director (ED) has been designated as the Privacy Officer for ARFHT. They oversee compliance to this policy, related procedures, and legislation. The ED can be reached by phone at 613-554-9551 ext. 101 or by mail at 100 Health Village Lane, Suite 101, Renfrew ON K7V 0C3.

All team members working at ARFHT are responsible for maintaining confidentiality and privacy of all information collected, accessed, or disclosed during and after their employment or professional contact. Staff are required to abide by a confidentiality agreement.

Principle 2 – Identifying Purposes for the Collection of Personal Health Information

ARFHT may collect personal health information for the following purposes:

- To provide clients with safe and effective healthcare, programs, and services;
- To help plan programs and services;
- To monitor and evaluate the quality of service(s);
- To contact clients regarding upcoming events;
- To meet legal and regulatory requirements.

ARFHT staff shall explain to clients the purposes for which information is being collected.

This Privacy Policy will be available to clients on the ARFHT website and on request.

A privacy notice shall be posted in the waiting room of the ARFHT.

Principle 3 – Consent for the Collection, Use and Disclosure of Personal Health Information

The knowledge and consent of the client is required for the collection, use or disclosure of personal health information, except where inappropriate due to legal, medical or security reasons.

A client's request for care implies consent for the ARFHT collection, use and disclosure of their personal health information for purposes related to care. These purposes are identified in Principle #2 above.

To provide clients with comprehensive health care, their personal health information may be shared among those directly involved with their care.

ARFHT will obtain a client's express consent before disclosing personal health information to any third party who is not in the client's circle of care and who is not authorized by other existing statutes to receive the client's personal health information without expressed consent.

In certain circumstances, legal and regulatory requirements compel ARFHT to disclose personal health information without a client's consent. Examples include disclosures to the Ontario Ministry of Health and Long-Term Care for billing purposes and mandatory reporting of certain diseases, as well as law enforcement personnel in cases where ARFHT's ED is presented with a valid court order or subpoena.

ARFHT senior administrative or clinical staff may also disclose personal health information to hospital and emergency staff where there is an immediate threat to a client's health and safety or the health and safety of another individual.

Principle 4 – Limited Collection of Personal Information

ARFHT will limit the amount and type of information collected to what is necessary to fulfill the purposes identified. All information will be collected by fair and lawful means.

Principle 5 – Limiting Use, Disclosure and Retention of Personal Health Information

ARFHT will not use or disclose personal health information for purposes other than those for which it was collected, except with the consent of the client or as required by law.

Personal Health Information will be retained only for as long as necessary for the fulfillment of those purposes or as required by law.

Principle 6 – Accuracy of Personal Health Information

Personal health information collected by the ARFHT will be as accurate, complete, and up to date as possible and is necessary for the purposes for which it is to be used.

Principle 7 – Ensuring Safeguards for Personal Health Information

ARFHT staff use appropriate security measures to protect clients' personal health information from theft, loss, and unauthorized access, copying modification, use, disclosure, and disposal.

Methods of protection include:

- Physical measures such as locked filing cabinets and restricted access areas;
- Administrative measures such as policies and procedures with respect to privacy and security; and
- Technical measures such as the use of passwords, firewalls, and virtual private networks.

Care will be used in the disposal or destruction of personal health information to prevent third parties from gaining unauthorized access.

ARFHT will ensure that staff, students, and volunteers are aware of the importance of privacy and confidentiality and that they abide by a signed confidentiality agreement.

Principle 8 – Openness about Personal Health Information Policies and Procedures

ARFHT will make available to clients and the general public, information regarding the policies and practices relating to the management of personal health information in a format that is generally understandable. This information will include the contact information for the designated Privacy Officer.

This Privacy Policy will be available to clients on the ARFHT website and on request.

A privacy notice shall be posted in the waiting room of the ARFHT.

Principle 9 – Individual Access to One's Own Personal Health Information

Upon request, a client will be informed of the existence, use, and disclosure of personal health information and will be granted access to that information unless the physician deems that access to that information could be harmful to the client or a third party.

Clients may request to have access to, or a copy of, their personal health information. All physical records remain the property of ARFHT.

Clients may challenge the accuracy and completeness of their information and ask to have it amended as appropriate.

Principle 10 – Challenging Compliance with the Privacy Officer

A client may challenge the ARFHT compliance with the above principles by addressing any of their concerns with the designated Privacy Officer and completing the Client Complaint form.

The Privacy Officer will investigate all complaints. If a complaint is found to be justified, appropriate measures will be taken, including amending policies and practices if necessary.

This privacy policy continues to apply when working from home and other remote sites. The following additional considerations apply.

Because of the serious risk of loss or theft, patient information will only ever be removed from the premises by those Team Members who have a real need to do so to carry out their duties (for example, Team Members who have been authorized to work from home, which may include conducting virtual patient appointments, or who provide care to patients at other sites such as home visits or community settings). This applies to electronic files, paper copies and information on mobile devices such as laptops, smart phones, disks, and memory sticks (USB keys and portable hard drives), printers, scanners, and any other formats.

For electronic files, remote access to patient information should be through our secure server (our virtual private network), where we can protect it. Every time patient information is saved to a mobile device there is a chance it may be lost or stolen. Therefore, we will do this only when absolutely necessary to carry out our jobs and if so, only on an encrypted mobile device.

Do not use unsecured WiFi to access our secure system.

Where there is no choice but to take information off-site, patient information will be deidentified if possible. Note; merely removing someone’s name from a record does not necessarily anonymize the record.

If patient information must remain identifiable when off site (or if new patient information must be collected and documented outside the secure server):

- For paper records:
    - Keep papers in a locked box or bag for transport and do not leave files in your car or public transit. Files must be kept on your person;
    - Patient information should not be stored at home except in extremely limited circumstances and if the Team Member is required to keep paper copies of patient information at home, it must be held securely, and care should be taken to avoid family or friends or other visitors from having any access;
    - Do not print records containing patient information at home unless absolutely necessary;
    - Paper records no longer needed must be either shredded with a crosscut or confetti shredder on-site (meaning at home or other remote work location) or brought back to the workplace for secure destruction. Do not put paper records containing personal information in the garbage or recycling.
- For Electronic Records:
    - Only save to a mobile device with strong encryption. Strong encryption is more than just password protected. If you are not sure how to encrypt a mobile device, ask the Privacy Officer.
    - If patient information must remain identifiable and there are no encrypted mobile devices to use, unencrypted mobile devices containing personal health information must not be left on the seat or in the trunk of an unattended car, even for just a few moments.
- Steps should be taken to avoid drawing attention to patient materials or unencrypted mobile devices (such as keeping them in an unmarked bag or contained),
- When transporting patient information, go directly to the destination, making the journey as short as practicable.

If working on a personal device, Team Members must:

- Have authorization to do so.
- Password protect the device.
- Ensure the personal device has up-to-date anti-virus software enabled.
- Ensure WiFi connections are secure.
- Sign in and out of the secure remote server at each time of use and not have a saved password to the secure remote server on any personal device that others could utilize.
- Not download patient information onto personal devices or make printouts of patient information from remote access.
- Check the “Temporary Downloads” or “Scanned Files” before signing off the device to ensure nothing work related was accidentally saved on the personal device, and if it was, delete the work-related record.

- Keep the device safe and secure from loss or theft and if it is lost or stolen erase the contents of the device remotely, if possible.
- Report to the Privacy Officer immediately a lost or stolen personal device that has access to the workplace network and/or email and/or that contains patient information.

For remote workspaces:

- Take care that people with whom you share space cannot see or overhear your work conversations and work products on screens or paper.
- Lock your computer when not in use by you or when left unattended,
- Do not reuse your passwords.
- Protect your own personal privacy when working remotely by blocking your personal/home number and not using personal email addresses to communicate with patients or colleagues. If you need assistance to block your number, ask the Privacy Officer for instructions on how to do so.

Policy Section:	Effective Date:	Reviewed Date:	Approved By:
Organizational	December 2024		Board of Directors

Privacy Breach Protocol

The Privacy Officer (Executive Director) of the Ancient Rivers Family Health Team (ARFHT) will submit a Privacy Breach Report to the Information and Privacy Commissioner/Ontario (IPC/O) and report the same to the Board of Directors.

The following steps will be taken by the Privacy Officer (or delegate) if they believe there has been a privacy breach.

Step 1: Respond immediately by implementing the privacy breach protocol

- Ensure appropriate staff members with the ARFHT are immediately notified of the breach, including the Privacy Officer and clinicians whose patients are potentially affected by the privacy breach.
- Address the priorities of containment and notifications as set out in the following steps.

Step 2: Containment – Identify the scope of the potential breach and take steps to contain it.

- Retrieve the hard copies of any personal health information that has been disclosed.
- Ensure that no copies of personal health information have been made or retained by the individual who was not authorized to receive the information and obtain the person's contact information in the event that follow-up is required.
- Determine whether the privacy breach would allow unauthorized access to any other personal health information (i.e. electronic information system) and take whatever necessary steps are appropriate (i.e.. Change passwords, identification numbers and/or temporarily shut down a system).
- Consider notifying the Information and Privacy Commissioner/Ontario (IPC/O) and/or legal counsel if appropriate.

Step 3: Notification – Identify those individuals whose privacy was breached and notify them of the breach.

- At the first reasonable opportunity, any affected patients (or those whose personal health information has been affected) will be notified.
- The type of notification will be determined based on the circumstances (such as the sensitivity of the personal health information, the number of people affected, and the potential effect the notification will have on the patient(s).

- For example, notification may be by telephone or in writing, or depending on the circumstances, a notation made in the patient's file to be discussed at their next appointment.
- Provide details of the extent of the breach and the specifics of the personal health information at issue.
- Advise affected patients of the steps that have been or will be taken to address the breach, both immediate and long-term.
- Consider notifying the IPC/O and/or legal counsel if appropriate.

Step 4: Investigation and Remediation

- Conduct an internal investigation into the matter. The objective of the investigation will be to:
  - Ensure the immediate requirements of containment and notification have been addressed.
  - Review the circumstances surrounding the breach.
  - Review the adequacy of existing policies and procedures in protecting personal health information.
  - Address the situation on a systemic basis.
  - Identify opportunities to prevent a similar breach from happening in the future.
- Change practices as necessary.
- Ensure staff are appropriately re-educated and re-trained with respect to compliance with the privacy protection provisions of PHIPA and the circumstances of the breach and the recommendations of how to avoid it in the future.
- Continue notification obligations to affected individuals as appropriate.
- Consider notifying the IPC/O and/or legal counsel as appropriate.
- Consider any disciplinary consequences with staff or contact issues with independent contractors or vendors that follow from the privacy breach.