Privacy Responsibilities Policy

Title: Privacy Responsibility Policy	Privacy Policy No.: 3.0
	Pages: 1 of 6
Initial Issue Date: January 16, 2016 Date of Revision: December 2018, April 2020, January 2022, November 2024	
Reviewed by: Coordinator ARGI/Best Care	Review: Annually
Approvals: Coordinator ARGI/Best Care	

ARGI recognizes the right to privacy as a principle of respect for patient autonomy, based on the individual's right to control information related to their healthcare. Patient privacy and a patient's right to access their health records are protected by law under the Personal Health Information Protection Act (PHIPA). ARGI must obtain individual's consent when they collect, use or disclose the individual's personal information. The individual has the right to access, personal information held by an organization and to challenge its accuracy, if need be. Personal information can only be used for purposes for which it was collected. If an organization is going to use it for another purpose, consent must be obtained again. Individuals should also be assured that their information will be protected by specific safeguards, including measures such as locked cabinets, computer passwords or encryption. Patients may withdraw their consent to the collection, use, and disclosure of their PHI for the purpose of providing healthcare to them.

Personal Information:

Personal information includes any factual or subjective information, recorded or not, about an identifiable individual. This includes information in any form, such as:

- Age, name, ID numbers, income, ethnic origin, or blood type
- Opinions, evaluations, comments, social status, or disciplinary actions
- Employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant

Personal information does not include the name, title or business address or telephone number of an employee of an organization.

10 Privacy Principles that must be followed are:

Principle 1 – Accountability

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

Principle 2 – Identifying Purposes

ARGI, at the time personal information is collected, will identify the purposes for which personal information is collected. The primary purposes are the delivery of direct patient care, the administration of the health care system, to conduct quality improvement initiative and research and to comply with legal and regulatory requirements.

Principle 3 – Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Principle 4 – Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

Principle 5 – Limiting Use, Disclosure, and Retention

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

Principle 6 – Accuracy

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

Principle 7 – Safeguards

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

Principle 8 – Openness

An organization shall make readily available to individuals' specific information about its policies and practices relating to the management of personal information.

Principle 9 – Individual Access

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Principle 10 – Challenging Compliance

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

These principles are usually referred to as "fair information principles". They are included in the Personal Information Protection and Electronic Documents Act (PIPEDA), Canada's private-sector privacy law.

Rules for the Use and Disclosure of PHI for the Purpose of Providing Patient Care

Patient Requests for Access to Records

Patients contact ARGI via email at bestcare@argi.on.ca to request access to, or copies of, their clinical records of PHI.

Accuracy of Records

Patients may contact ARGI to challenge the accuracy and completeness of their information as contained within their medical record, and to request a correction. If a challenge/correction request is not resolved to the satisfaction of the patient, they have the right to appeal ARGI's decision to the Information and Privacy Commissioner of Ontario (IPC), and/or to submit a statement of disagreement, which ARGI will store in the patient's medical record.

Patient-Requested Audits

Patients may contact ARGI Privacy to request an audit log of accesses to their electronic medical record.

Consent Directive/Lockbox

Patients may withdraw their consent to the collection, use, and disclosure of their PHI for the purpose of providing healthcare to them. This is commonly referred to as a "lockbox". Clinicians must request consent to override a lockbox for the purpose of providing care, either from the patient or the substitute decision maker (SDM) for the patient. The clinical user may override the lockbox citing an emergency only when:

- it is not reasonably possible to obtain this consent, and
- the risk of not accessing the locked information may lead to serious harm.

Information and Privacy Commissioner

Patient privacy concerns should be escalated to ARGI's Privacy Office. In situations where ARGI Privacy is unable to resolve a concern, patients will be advised that they may contact the IPC by email at info@ipc.on.ca.

Cooperation with the ARGI Privacy Office

All ARGI agents are required to cooperate with Privacy Office staff during a complaint, breach investigation, containment or remediation of a privacy issue, a privacy impact assessment, or an audit. Failure to cooperate with Privacy Office staff in their attempts to ensure or support compliance with ARGI policy or provincial privacy laws may result in disciplinary measures.

Consent

ARGI collects, uses, and discloses PHI with the consent of the patient or their Substitute decision maker (SDM), or as is otherwise permitted or required by PHIPA. Where consent of an individual is required, the consent must:

- be of the individual
- be related to the information
- not be obtained through deception or coercion

The individual must be informed:

- of the purpose of the collection, use or disclosure of the information, and
- that consent may be provided or withheld.

Express and Implied Consent

ARGI may rely on express or implied consent when collecting, using, or disclosing PHI for the purpose of providing patient care. PHI may be used and disclosed with assumed implied consent to healthcare professionals within a patient's circle of care, which includes, but is not limited to nurses, respiratory therapist, doctors, administrative staff supporting the provision of care, other employees assigned to care for a patient, and learners.

A patient's express consent is required for a patient's PHI to be disclosed:

- to a person that is not a health information custodian (HIC); or,
- for a purpose other than providing healthcare or assisting in healthcare.

Obtain Consent from the Capable Patient

When consent is required for the collection, use, or disclosure of an individual's PHI, the consent must be obtained from the patient when the patient is capable of consenting to the collection, use, or disclosure. An individual is capable of consenting to the collection, use, or disclosure of PHI if the individual is able to:

- understand the information relevant to deciding whether to consent to the collection, use, or disclosure of PHI, and
- appreciate the reasonably foreseeable consequences of giving, not giving, withholding or withdrawing the consent.

Where the individual is not capable of consenting to the collection, use, or disclosure of PHI, consent must be obtained from the patient's SDM.

Security of Systems and PHI

ARGI protects PHI through appropriate physical, administrative, and technical safeguards. The safeguards are consistent with industry best practices to protect PHI while being transferred, processed, or stored. These safeguards include security software and encryption protocols, firewalls, locks and other access controls, privacy impact assessments, threat-risk assessments, staff training, and

confidentiality agreements. The Privacy Office and Digital Security monitor the security of PHI by conducting audits of clinical systems and business units.

Vendor and External Party Access to ARGI PHI

All vendors, contractors, consultants, or other external parties who require access to ARGI IT and/or ARGI PHI must enter into a signed written agreement with ARGI, reviewed by Legal Affairs, that includes:

- ARGI Confidentiality Agreement
- ARGI Information Practices Agreement

Retention, Archiving and Destruction of PHI

ARGI has established information retention guidelines that define consistent minimum standards and requirements for the length of time records of PHI are to be maintained. ARGI has established appropriate practices and timelines for the secure disposal of PHI, consistent with confidentiality, legal, and regulatory requirements. Researchers are responsible for the storage/retention of research data, as defined in their approved research protocol.

Rules for the Use and Disclosure of Patient Data for Purposes Other Than for Care (Research, Quality Improvement, Education)

PHI or anonymized data that is sent from or received by ARGI for research, quality improvement, or educational purposes must be handled in compliance with ARGI's policies. Any necessary consents and/or internal approvals must be obtained prior to use or transfer.

Limiting PHI and the ARGI De-identification and Anonymized Data Standard

ARGI and its agents must only collect, use, disclose, and retain the minimum amount of PHI required to achieve the research, quality improvement, or education purpose. De-identified information should be used instead of PHI whenever it is feasible to do so. When ARGI agents are not able to anonymize information to meet the Standard, the Privacy Office must be consulted for advice and recommendations on risk mitigation.

Use of Anonymized Information

Anonymized information is considered an ARGI corporate resource. Any use or transfer outside of ARGI of anonymized information must comply with ARGI policies. Any necessary approvals must be obtained prior to use or transfer.

Anonymized patient/participant information may be used for ARGI-supported purposes (including patient care, research, quality improvement, or education) provided it is used in a manner that:

- does not jeopardize the safety or well-being of patients/participants and the ARGI community
- does not reflect poorly on ARGI
- is consistent with ARGI's stated values
- does not expose ARGI to unacceptable ethical, reputational, legal, regulatory or technical risks

When publishing, sharing, or presenting anonymized information ARGI will do its best to not add information that would cause the data to become identifiable, or unnecessarily increase the risk of re-identification and ensure that descriptions and commentary related to anonymized information are professional in both tone and content.

Research

Research project proposals involving the collection, use, or disclosure of PHI, anonymized or any other ARGI data must be reviewed and approved by an approved external Research Ethics Board (REB). The REB will address consent requirements for the use of PHI.

Quality Improvement Project Proposals

Quality improvement (QI) projects must:

- be submitted to the ARGI Quality Improvement Review Committee for review and institutional approval prior to proceeding, and
- have approval by the appropriate manager/director/executive sponsor, depending on the scope of the project.

Consent and QI Projects with External Data Sharing

Except where the patient's express consent has been obtained for such disclosure, PHIPA does not permit the disclosure of PHI to external parties (nor in publications) in relation to QI projects. (For example, the transfer of ARGI PHI to a multi-site QI project without patient consent is not permitted.)

Education

PHI may be used without consent for the purposes of educating ARGI agents. For internal ARGI use, a supervising clinician, department head, or manager must approve the use of PHI for educational purposes where the trainee/agent is not in the patient's circle of care. Where training agents outside of the circle of care, PHI should be anonymized to the greatest extent possible to achieve the purpose.

Privacy Operations Services

Privacy Incidents

ARGI agents must report privacy incidents, including instances when an agent knows, or has reason to believe, that PHI was collected, used, or disclosed without proper authorization and when PHI is lost or stolen. An ARIG agent must also report situations that present a risk to patient privacy.

ARGI relies on agents to participate in the review of privacy incidents in order to determine the extent of a breach, to mitigate its impact, and to prevent or reduce the recurrence of similar incidents. Early reporting of privacy incidents can result in mitigation strategies that reduce the extent of the breach and its consequences.

When privacy incidents occur, ARGI Privacy will assist agents to:

- identify the scope of the breach and take steps for containment;
- notify the individuals affected by the breach, as soon as reasonably possible, and include certain required information in the notice, including a statement that the individual is entitled to make a complaint to the IPC; and
- notify any staff (and other custodians, as appropriate) who need to be advised of the breach.

Where required by PHIPA, ARGI Privacy will notify the IPC and/or the regulatory colleges as appropriate.

System Audits

The Privacy Office conducts audits of information systems used to collect, use, document, and disclose PHI for the purpose of detecting and deterring unauthorized activity. Site visits are also conducted on request or as part of a review or investigation.

Accessing Records of PHI

ARGI agents may only access records of PHI as needed for the purposes of their ARGI-authorized role. Any other access is considered a privacy breach and may be reportable to the Information and Privacy Commissioner of Ontario and incur discipline. ARGI agents may not directly view their own health records in ARGI's electronic systems. These systems are only to be used for work-related purposes.

Training and Awareness

ARGI makes its agents aware of the importance of maintaining the confidentiality of personal health information. All ARGI agents must sign a Confidentiality Agreement and complete ARGI privacy training at the onset of their association with ARGI and annually thereafter. Ongoing educational efforts will be delivered by ARGI Privacy to ensure all ARGI agents are provided with tools, training, and support, as appropriate, to assist them in fulfilling their duties as it relates to the privacy of PHI.

Ministry of Health, Government Agencies & Government-Funded Agencies

The law permits ARGI to disclose PHI to organizations such as the Ministry of Health, Ontario Health, Public Health Ontario, Canadian Institute for Health Information, Institute for Clinical Evaluative Sciences (ICES), and other similar organizations for the planning and management of the health system. An agreement must be in place between ARGI and the organization before any PHI is disclosed to the organization.

PHI from Outside Organizations

Whenever an agent of ARGI is provided with records of PHI from an outside organization for the purpose of the provision of care (such as a hospital, researcher, or government agency), ARGI policies and procedures governing the handling and retention of PHI must be followed with respect to the external records. These records become part of the patient chart.

Enforcement and Sanctions

ARGI applies progressive discipline in dealing with privacy breaches; however, any breaches of this policy, including, but not limited to, repeated or intentional breaches and breaches of related privacy policies may result in suspension or termination, and reporting to the relevant regulatory college and the Information and Privacy Commissioner of Ontario.

Collection, use, or disclosure of PHI in contravention of PHIPA may result in fines. ARGI will not normally cover or insure individuals for fines resulting from the collection, use or disclosure of PHI in contravention of PHIPA and this policy.

Employee Privacy

ARGI is committed to protecting the privacy of its employees. Employee personal information will only be collected, used, and disclosed as per Personal Information Protection policy.

Policy Review

This policy will be reviewed at least once every two years and as issues arise, including amendments to legislation or new guidance from the IPC. The Privacy Office will be responsible for ensuring that any relevant changes to this policy are communicated to ARGI agents, patients, and visitors.