Phone: (519) 915 - 1207
Fax: (519) 915 - 1664
2055 Huron Church Rd, Suite 210
Windsor ON N9C 2L6

WE Kidz Pediatrics Privacy Policy

Last updated 5th November 2025

Protecting & Safeguarding Personal Information

WE Kidz Pediatrics is committed to protecting the privacy, confidentiality, and security of all personal health information in accordance with PHIPA and IPC. Our policies outline how health information is collected, used, disclosed, and safeguarded, as well as patients' rights to access and correct their records. We maintain strict privacy training, breach response and accountability procedures to ensure patient information is handled with the highest standard of care and professionalism.

Key Terms:

- Personal Health Information (PHI): Identifying information about an individual relating to their physical or mental health, health history, treatment, or care. This includes but is not limited to test results, billing information and any data that can reasonably identify a patient.
- Information and Privacy Commissioner of Ontario (IPC): The IPC is an independent organization that helps protect your privacy. It ensures healthcare providers follow Ontario's privacy laws and investigates complaints if you believe your personal health information has been mishandled.
- Personal Health Information Protection Act (PHIPA): Ontario legislation governing he collection, use, and disclosure of personal health information by health information custodians and their agents.
- Health Information Custodian (HIC): A person or organization that has custody or control of a personal health information as a part of delivering healthcare services (example: physicians, clinics or hospitals)
- Consent: The permission granted by a patient or their substitute decision maker for the collection, use, or disclosure of their personal health information. This can be expressed or implied and may be withdrawn at any time.
- Privacy Officer: The designated individual at WE Kidz Pediatrics responsible for ensuring compliance with PHIPA, managing privacy breaches, investigating complaints and overseeing staff privacy training and compliance.

1. **Openness & Transparency**
   1.1. We value patient privacy and act to ensure that it is protected.
   1.2. This policy has been developed and reviewed to reflect our current practices and to comply with provincial and federal regulations regarding the protecting of personal health information.
   1.3. This document outlies how WE Kidz Pediatrics collects, uses, discloses, and safeguards personal information, as well as the rights of patients concerning their own health data.
   1.4. We welcome and encourage patients to reach out with any questions and/or concerns about our privacy policies.
2. **Accountability**
   2.1. The physician is ultimately responsible for ensuring all health records under their care are appropriately protected and managed.
   2.2. The designated privacy officer for WE Kidz Pediatrics is Dr. Omar Afandi, who can be reached at admin@wekidzpediatrics.com. Our privacy officer is responsible for overseeing compliance with privacy laws and ensuring that all staff follow our privacy and security protocols. Our privacy officer is responsible for but not limited to:
      2.2.1. Facilitating compliance with PHIPA
      2.2.2. Ensuring all individuals affiliated with WE Kidz Pediatrics are informed of and adhere to their obligations in accordance with PHIPA legislation.
         2.2.2.1. This includes all custodians but is not limited to physicians, employees (both part time and full time), vendors and volunteers.
         2.2.2.2. All custodians are required to receive PHIPA-compliant privacy training prior to start of their employment.
      2.2.3. WE Kidz Pediatrics receives and investigates any complaints or inquiries from patients regarding our privacy policies, practices, or use of personal health information. Each concern is documented, reviewed internally, and addressed in compliance with PHIPA to ensure accountability and to resolve issues quickly and respectfully.
      2.2.4. Patients have the right to access and ask for corrections to their medical records. Requests are evaluated carefully to ensure accuracy, confidentiality, and lawful disclosure. If a request cannot be granted, patients will receive a written explanation outlining the reasons and inform the patient of their options.
   2.3. All custodians and third-party obligations associated with WE Kidz Pediatrics must strictly adhere to the following principles of data protection in compliance with PHIPA (Personal Health Information Act)
      2.3.1. Custodians shall only collect, use, or disclose personal health information with the patient's consent, except where PHIPA expressly authorizes such actions without consent.
      2.3.2. Custodians must not collect, use, or disclose personal health information if the information already collected is sufficient to fulfill the intended purpose. The

collection of and use of patient personal health information must always be necessary, relevant and, limited to what is required to deliver care.

2.3.3. When disclosure of personal health information is required, custodians must ensure that only the satisfactory amount of information necessary to achieve the intended purpose is achieved.

2.3.4. WE Kidz Pediatrics maintains contractual formal privacy agreements and clauses with all third-party vendors to ensure patient health information remains secure and always protected.

2.3.4.1. These agreements require all vendors to comply with the PHIPA and clinic's internal privacy policies. The vendors are obligated to uphold strict confidentiality and safeguard against unauthorized access.

2.3.4.2. Third-party vendors may include, but are not limited to cleaning and security personnel, data processors, IT service providers, and maintenance contractors. Each vendor is required to acknowledge their privacy responsibilities and confirm adherence through signed confidentiality and privacy compliance agreements.

<u>Collection, Use and Disclosure of Personal Health Information</u>

3. **Consent**

Personal health information is extremely sensitive and must always be handled with respect and confidentiality. Unless otherwise required or permitted by law, WE Kidz Pediatrics will only collect, use, or disclose personal health information with the expressed or implied consent of the individual to whom the information relates, or their legally authorized substitute decision maker.

3.1. Implied consent is assumed when it is reasonable to infer that a patient agrees to the collection, use, or disclosure of their personal health information. This can be demonstrated when a patient voluntarily provides their health information to a physician, it is generally implied that this information may be shared in their circle of care for treatment.

3.2. Expressed consent is given directly by the patient, either verbally or in writing. Expressed or explicit consent is typically required when a patient's health information is being collected, used, or disclosed for purposes other than providing direct health care. This can include sharing information with third parties not involved in the patient's treatment.

3.3. The patient will be informed about how their personal health information may be collected, used, or disclosed and will be advised of their rights to withhold or withdraw consent subject to legal or clinical limitations.

4. **Withholding and Withdrawing Consent**

4.1. Patients reserve the right to withhold or withdraw their consent to the collection, use, or disclosure of their personal health information at any time. This right extends to limiting or restricting how their personal information is shared, except where such restrictions are:

4.1.1. Prohibited by law

4.1.2. Compromise patient safety, public health, or regulatory obligations.

4.2. Patients may choose to withhold or withdraw consent in several ways including, but not limited to:

4.2.1. Prohibiting the collection, use, or disclosure of their personal health information entirely.

4.2.2. Limiting disclosure to certain individuals or organizations.

4.2.3. Restricting specific uses or disclosures, such as to external consultants.

4.3. Once the patient has revoked consent, the affected personal health information becomes "locked" within the patient's record. This means it cannot be accessed or used without the patient's expressed authorization. However, withdrawal of consent does not apply retroactively to information that has already been disclosed in accordance with prior consent.

4.4. If the withdrawal of consent prevents the disclosure of information to another health information custodian, WE Kidz Pediatrics will notify the other custodian that the information has been restricted. If we deem the information to be reasonably necessary for ongoing provision of care, we will discuss the implications with the patient, seeking and informed decision.

4.5. In the event that the patient's decision to withdraw or limit consent could compromise the quality, coordination, or safety of their care, WE Kidz Pediatrics will explain the potential consequences to the patient before finalizing the withdrawal. The discussion will focus on maintaining continuity of care while respecting the patient's autonomy.

4.6. All requests to withhold or withdraw consent, as well as related discussions and outcomes, will be clearly documented in the patient's medical record. This allows for transparency, accountability, and ongoing compliance with PHIPA.

5. **Collection of Personal Health Information**

5.1. WE Kidz Pediatrics collects personal health information about patients to provide safe, effective, and continuous medical care. The information allows our custodians to assess, diagnose, treat, and monitor patients while maintaining accurate medical documentation in compliance with PHIPA and other applicable laws. Personal health information is collected directly from the patient or from an authorized individual acting on their behalf. In certain circumstances, information may also be collected from other healthcare sources, with patient consent or as otherwise permitted by law.

5.2. WE Kidz Pediatrics may collect patient health information from a variety of secure sources, including but not limited to:

5.2.1. Direct patient disclosure: Information shared verbally or in writing by the patient or substitute decision maker.

5.2.1.1. This can take form in physical documentations submitted by the patient or substitute decision maker in print form.

5.2.2. Healthcare providers: Referrals, reports and records from physicians, nurses, specialists, pharmacists and other health professionals in the patient's circle of care.

5.2.3. Laboratories and diagnostic facilities: Test results, imaging, and reports related to patient diagnosis or ongoing treatment.

5.2.4. Health Institutions and Insurers: Data provided by hospitals, clinics or insurance carriers (WSIB, OHIP or private third-party insurers).

5.3. Types of identifying personal health information collected may include, but are not limited to:

5.3.1. Demographic information including name, date of birthday, address, and contact information.

5.3.2. Billing and insurance information including the patient's provincial/territorial health card number, private insurance details or other relevant information related to billing claims.

5.3.3. Medical history, presenting symptoms, diagnoses, treatment plans, test and diagnostic results, medications, allergies and family medical history.

5.4. WE Kidz Pediatrics only collects the personal health information necessary for the provision and coordination of care and communication with patients. Information will not be collected or used for any purpose other than patient care with the exception when permitted by law or when expressly authorized consent by the patient. These limitations ensure the collection of only essential and relevant information data, avoiding unnecessary and excessive information.

6. **Use of Personal Health Information**

6.1. Personal Health Information collected from patients is used and disclosed by WE Kidz Pediatrics only for legitimate purposes directly related to the delivery of the clinic. All uses and disclosures comply with PHIPA and other applicable laws. We may use or disclose personal health information for the for the following reasons:

6.1.1. When providing medical care and treatment. This includes assessments, diagnoses, follow-ups, and the ongoing coordination of services among providers in the patient's healthcare team.

6.1.2. When retrieving payment for services such as provincial/territorial insurance and third-party billing or uninsured services.

6.1.3. To plan, administer, and manage clinic operations including maintaining accurate electronic medical records, scheduling, internal audits and coordination.

6.1.4. To support risk and error management by reviewing procedures to prevent, detect and correct potential errors in patient care or data management.

6.1.5. To conduct quality improvement activities such as patient satisfaction surveys, workflow review and initiatives aimed at enhancing patient safety and clinical efficiency.

6.1.6. To educate and train healthcare professionals and students ensuring that all clinical staff maintain high standards of professional competence and privacy awareness.

6.1.7. To compile statistics and perform data analysis by using de-identified information.

6.1.8. To comply with legal and regulatory requirements which includes but is not limited to disclosures to public health authorities or communicable disease reporting and safety investigations.

6.1.9. To securely dispose of and de-identify records when the information is no longer required. This ensures that data is permanently deleted or modified allowing the patient to not be identifiable in research or dataset.

6.1.10. All procedures involving the de-identification of patient data are conducted in compliance with PHIPA and require Research Ethics Board (REB) approval to ensure that data is used ethically, securely, and without risk of re-identificaiton.

6.2. WE Kidz Pediatrics may engage authorized Agents and Service Providers to assist in analyzing patient information for the purpose of improving clinical care and supporting evidence-based decision-making.

6.3. The use of such tools, including traditional and/ or "learning" computer algorithms (commonly referred to as AI) and other data-analysis technologies, is strictly controlled and limited to lawful, ethical and medically relevant purposes. These tools may examine de-identified datasets to:

6.3.1. Identifying patients who could benefit from specialized health interventions.

6.3.2. Evaluating clinical performance.

6.3.3. Enhance safety, consistency and the accessibility of healthcare.

6.4. All information analyzed is de-identified prior to processing. No identifiable health information is used by AI systems without expressed consent from the patient or authorization from PHIPA. This means that the data including names, dates of birth, demographics and other identifiable information is removed prior to examination.

6.5. Agents and Service Providers are bound by strict confidentiality agreements and are prohibited from using and disclosing any information other than those authorized by WE Kidz Pediatrics. Access to raw data is monitored and limited to trained personnel. The goal of using AI and data analytics is to enhance safe, effective and evidence-based patient care. Analytics are not used to replace clinical judgement or to use health information for marketing, commercial or unrelated research.

6.6. Some authorized service providers may store or process information outside of Ontario or Canada, including the United States. When this occurs, WE Kidz Pediatrics ensures that the same, or stronger, privacy and security protections are applied. Data transfers occur only when essential and when possible, data is de-identified or anonymized prior to transfer and processing.

7. **Disclosure of Personal Health Information**

7.1. WE Kidz Pediatrics discloses personal health information in accordance with and described in Section 6 (Use of Personal Health Information) or as otherwise permitted by law. All disclosures are limited to the minimum amount of information necessary to fulfill the purpose of disclosure and facilitated to protect the confidentiality and privacy of the patient.

7.2. Implied consent to disclose personal health information:
    7.2.1. Unless otherwise indicated, patients are presumed to have provided implied consent for WE Kidz Pediatrics to disclose their personal health information to other healthcare providers who are directly involved in their circle of care. By seeking care from WE Kidz Pediatrics, a patient's consent to share relevant information with those assisting in the treatment is implied.
    7.2.2. Relevant information may be shared with, but not limited to:
        7.2.2.1. Other physicians within the practice
        7.2.2.2. Other physicians within the after hours call group.
        7.2.2.3. Consulting specialists, pharmacists, laboratories, imaging facilities, or allied health professionals directly operating within the patient's care.
7.3. Express (verbal or written) consent is required before WE Kidz Pediatrics discloses personal health information to any third parties for any purpose other than to provide care, unless legally authorized to do so.
    7.3.1. Common examples where express consent is required include:
        7.3.1.1. Third-party medical examinations
        7.3.1.2. When providing chart copies or summaries to insurance providers or other legal representatives.
        7.3.1.3. Sharing health information for research, teaching or administrative purposes outside of the patient's circle of care.
    7.3.2. Upon obtaining express consent, WE Kidz Pediatrics will record the details of the consent in the patient's medical record. If consent is provided in writing, a signed consent form will be attached to the patient's chart as an official record. This ensures that all disclosures are traceable and verifiable in accordance with PHIPA.
7.4. In certain and limited circumstances, WE Kidz Pediatrics may be required and/ or authorized by law to disclose personal health information without the prior expressed or implied consent. These disclosures are made only when essential to meet legal, ethical, or public- interest obligations and follow the principles of minimum disclosure and confidentiality protection under PHIPA.
    7.4.1. In situations where WE Kidz Pediatrics is required or authorized to disclose personal health information without consent, only the minimum amount to satisfy the specific legal requirements will be disclosed. Every disclosure will be documented in the patient's chart including recipient and reason for release.
    7.4.2. Examples of situations where disclosure without consent can occur include, but are not limited to:
        7.4.2.1. Billing and payment purposes.
            7.4.2.1.1. Submitting claims to the Ontario Health Insurance Plan (OHIP) or other insurers.
            7.4.2.1.2. Providing supporting medical information when a payment review or audit is requested by an authorized payer.
        7.4.2.2. Public health and safety reporting:

7.4.2.2.1. Reporting communicable diseases, such as COVID-19, tuberculosis and measles, to the public health authorities.

7.4.2.2.2. Reporting individuals who may pose a significant risk of serious bodily harm to themselves or others, when required by law.

7.4.2.3. Mandatory reporting requirements:

7.4.2.3.1. Reporting suspected child abuse or neglect under the *Child, Youth and Family Services Act*.

7.4.2.3.2. Reporting suspected abuse or neglect of vulnerable adults or elders under long-term-care or home-care legislation.

7.4.2.4. Fitness, safety, and licensing assessments:

7.4.2.4.1. Notifying the Ministry of Transportation when a patient's medical condition may impair their ability to safely operate a motor vehicle, as required under the *Highway Traffic Act*.

7.4.2.4.2. Providing reports to occupational health or aviation regulators to verify medical fitness for specific professional duties.

7.4.2.5. Regulatory and professional investigations:

7.4.2.5.1. Cooperating with oversight bodies such as the College of Physicians and Surgeons of Ontario (CPSO), the Ontario Medical Association, or the Information and Privacy Commissioner of Ontario (IPC) when conducting formal investigations, audits and/or reviews.

7.4.2.6. Court orders and legal proceedings:

7.4.2.6.1.1. Complying with a court order, subpoena, warrant or summons that legally compels the release of records.

7.4.2.6.1.2. Assisting law enforcement agencies with lawful investigations, but when disclosure is specifically required.

7.4.2.7. Quality Assurance and peer review:

7.4.2.7.1. Participating in internal and external quality assessment programs that evaluate patient safety, clinical effectiveness and adherence to professional standards.

7.4.2.7.2. Disclosing limited and non-identifying health information for accreditation reviews and medical educational purposes.

7.4.2.8. Risk management and legal consultation:

7.4.2.8.1. Sharing information with the practice's legal counsel, insurers, or risk management advisors for the purposes of addressing an incident, improving patient safety protocols or defending a legal claim.

7.4.2.8.2. When providing relevant information to medical-legal experts when evaluating a potential adverse event or complaint.

7.4.2.9. Emergencies and Public Interest Exceptions:

7.4.2.9.1. Disclosing necessary information to emergency responders when required to prevent or reduce an imminent and serious threat to health or safety.

7.4.2.9.2. Providing details to a substitute decision maker or next of kin when a patient is incapacitated and disclosure is essential for care.

7.4.3. All disclosures of personal health information, whether made with or without patient consent, are handled with the highest level of accountability, transparency, and professionalism. WE Kidz Pediatrics recognize that even when disclosure is legally obligated, patients reserve the right to expect that their information will be shared responsibly and in accordance with PHIPA.

Protection of Personal Health Information

8. **Security Measures**

8.1. WE Kidz Pediatrics is committed to safeguarding all personal health information (PHI) through extensive physical, technological, and administrative controls. These safeguards are designed to prevent unauthorized use, disclosure and loss of personal health information while maintaining integrity and compliance with the Personal Health Information Protection Act (PHIPA) and the professional standards of the practice. Our security measures are continuously evaluated and updated to reflect evolving threats, technologies and legal requirements.

8.2. We use the following physical safeguards to protect the security of personal health information.

8.2.1. Controlled office access:

8.2.1.1. Our practice is secured by a monitored alarm system and restricted entry points.

8.2.1.2. Access to staff and medical-record storage areas are protected by deadbolt entry locks/ keycard/ keypad access systems.

8.2.1.3. Vistor access is restricted and strictly supervised.

8.2.2. Restricted Record Access:

8.2.2.1. Patient charts and files are stored in locked filing cabinets when not in use

8.2.2.2. Access to physical records is granted only on a need-to-know basis and limited to authorized staff

8.2.2.3. A list of individuals with access privileges is maintained and reviewed regularly.

8.2.3. Office layout and privacy design:

8.2.3.1. Reception and front-desk areas are equipped with privacy screens and organized to minimize visibility of confidential information.

8.2.3.2. Soundproofing and white noise systems are used in patient-care areas to ensure conversations cannot be overheard

8.2.3.3. Public and clinical spaces are intentionally separated to reduce incidental exposure of personal health information.

8.3. We use the following technological safeguards:

8.3.1. All electronic systems containing personal health information are protected by strict access control. Some examples include, but not are limited to:

8.3.1.1. Strong unique passwords required with every user, with routine renewal intervals.

8.3.1.2. Automatic session timeouts and inactivity locks to prevent unauthorized use of unattended workstations.

8.3.1.3. Limited search functions which ensure users can only access information relevant to their job duties.

8.3.1.4. Two-factor authorization (2FA) for administrative system access.

8.3.1.5. User authentication protocols in place linking each access event to an identifiable staff member for accountability.

8.3.2. The practice maintains layered system defenses to protect digital data including:

8.3.2.1. Firewalls and network segmentation prevent external access.

8.3.2.2. Up-to-date antivirus and anti-malware software actively monitor for threats.

8.3.2.3. Automatic software updates and security patches ensure current protection.

8.3.2.4. Encrypted data backups stored securely offsite or in a PHIPA-compliant cloud server.

8.3.3. Secure external electronic communications. All electronic communications involving personal health information (PHI) adhere to strict encryption and verification protocols:

8.3.3.1. Encrypted email systems or secure messaging platforms are used for external communication in accordance with expressed patient consent.

8.3.3.2. Internal systems operate on a secure, standalone network separated from public internet services.

8.3.3.3. Fax transmissions and printed communications are sent via pre-programmed numbers to secure, monitored locations and retrieved immediately by authorized personnel.

8.3.3.4. Confidential information is never transmitted through unsecured channels. (example being personal emails or unencrypted apps)

8.3.4. Secure electronic record disposal to prevent recovery of sensitive information from outdated equipment:

8.3.4.1. Electronic storage devices (example hard drives, USB keys, CDs) are permanently wiped using certified destruction software.

8.3.4.2. When physical destruction is required, storage media are shredded and/ or destroyed by an authorized disposal service.

8.3.4.3. Disposal of electronic records is documented and verified by the designated privacy officer or designated IT representative.

8.3.5. Privacy notices and warning flags with enhanced security measures are applied for sensitive and/ or high-risk patient records.

8.3.5.1. Prior to accessing certain electronic health records, a privacy warning notice will remind users of their confidentiality obligations.

8.3.5.2. Privacy flags may be applied to files at the request of the patient if there is an increased privacy risk. (Staff family members, celebrity patient or legal cases.)

8.3.5.3. These flagged files are audited more frequently to ensure compliance and to prevent unauthorized access.

8.3.6. WE Kidz is committed to auditing and monitoring of access of all electronic access to personal health information to detect unauthorized activity and ensure accountability. Some safeguarding practices include, but are not limited to:

8.3.6.1. All access to medical records is logged and traceable to the individual user.

8.3.6.2. Random audits are performed to review access patterns, including:

8.3.6.2.1. All staff who accessed a specific record.

8.3.6.2.2. All records accessed by a specific staff member during a defined period.

8.3.6.2.3. Any access to records belonging to family members or individuals with the same surname as the staff member.

8.3.6.3. Ensuring that records containing privacy flags or consent directives are reviewed more frequently.

8.3.6.4. Any suspicious or inappropriate access is investigated immediately and reported to the privacy officer, following the clinic's Brech Response Policy.

8.3.7. To minimize risks associated with mobile computing devises, portable media and mobile technology:

8.3.7.1. Personal health information may only be stored on authorized mobile devices (example: laptops, tablets, USB keys) with the written approval from the privacy officer.

8.3.7.2. All authorized devices must have:

8.3.7.2.1. Full disk inscription

8.3.7.2.2. Password and/ or biometric authentication

8.3.7.2.3. Automatic screen-lock and timeout features

8.3.7.2.4. Remote tracking and data-wipe capability in case of loss or theft.

8.3.7.3. Personal health information must never be stored on personal or unencrypted devices.

8.3.7.4. Any lost, stolen, or compromised devices must be reported to the privacy officer immediately to initiate breach management and containment.

8.4. WE Kidz Pediatrics maintains strong administrative controls to support ongoing privacy compliance:

8.4.1. All physicians, staff, students, and volunteers receive mandatory privacy and security training at onboarding and annually thereafter.

8.4.2. The privacy officer conducts periodic risk assessments, policy reviews, and compliance audits to ensure adherence to PHIPA.

8.4.3. Incident reports, audit results, and patient inquiries are regularly reviewed to improve safeguards and reduce risks.

8.4.4. A comprehensive Disaster Recovery and Business Continuity Plan ensures that electronic medical records remain accessible and secure during system outages or emergencies.

9. **Communication Policy**

9.1. WE Kidz Pediatrics recognizes that protecting patient confidentiality extends beyond record keeping including how we communicate with patients, families, healthcare partners, and third parties. We are mindful of the privacy of all personal health information (PHI) and ensure that communications are conducted securely, respectfully, and only with appropriate authorization. All forms of communication (verbal, written, or electronic) must adhere to the same standards of privacy and professionalism outlined under the Personal Health Information Protection Act (PHIPA).

9.2. We protect personal and health information regardless of the format or communication method used. All staff, physicians and affiliates are trained to verify patient identity and consent prior to sharing or discussing information (whether by phone, fax, email, electronic messaging or mail). Communications are guided by the following principles:

9.2.1. Only essential information is shared for the intended purpose.

9.2.2. The identity and authorization of the recipient are confirmed prior to any disclosure.

9.2.3. Any exchange of patient information, especially third parties, is documented in the patient's medical record.

9.2.4. Communications are kept courteous, clear and free from irrelevant personal information.

9.3. We use specific procedures to communicate personal information by:

9.3.1. Telephone:

9.3.1.1. Patient preferences regarding phone communication (permission to leave voicemail or to speak to family members)

9.3.1.2. When leaving a voicemail, staff will provide only their name, role, clinic name and callback information, unless the patient has authorized a more detailed message.

9.3.1.3. Calls containing personal health information will be held in private areas of the practice.

9.3.1.4. Staff must confirm the recipient's identity before discussing any confidential details.

9.3.1.5. When possible, calls are to be made directly to the patient, not to workplace numbers or shared devices, unless specifically authorized.

9.3.2. Fax communication:

9.3.2.1. All faxes containing personal health information are sent and received through secure, supervised machines in restricted access areas.

9.3.2.2. Pre-programmed and verified fax numbers are used to minimize errors.

9.3.2.3. Staff confirm recipient details before transmission and include a confidentiality disclaimer on all cover sheets.

9.3.3. Email and electronic communication:

9.3.3.1. Any transmission of personal health information over the internet or public networks is encrypted utilizing PHIPA compliant platforms.

9.3.3.2. Staff are required to ensure that messages are sent only to verified recipients and that patient consent for electronic communication is obtained and documented.

9.3.3.3. Email subject lines should not include patient identifiers or health related information.

9.3.3.4. Firewalls, spam filters and virus scanning software are maintained to prevent unauthorized interception.

9.3.4. Postal mail and courier deliveries:

9.3.4.1. When personal health information is sent by mail or courier, it must be placed in a sealed envelope and clearly marked as "Confidential".

9.3.4.2. Courier deliveries should require a signature upon receipt to confirm secure delivery and accountability.

9.4. Staff training and oversight:

9.4.1.1. All staff receive training on appropriate communication practices, including how to handle requests for information by phone, email and in person

9.4.1.2. The privacy officer periodically reviews communication processes to ensure compliance and identify areas for improvement.

9.4.1.3. Any incidents involving misdirected communication, privacy concerns or breaches will be documented and managed under the practice's Breach Response Policy.

9.5. Patients are informed of the practice's communication policies at the time of registration and may indicate their preferred methods of communication. Patients reserve the right to restrict or modify communication preferences at any time. The clinic will document and abide by these preferences when deemed possible, while ensuring the continuity of care.

9.5.1. To support patient transparency and awareness, WE Kidz Pediatrics ensures that the privacy information is clearly communicated to patients and visitors. Our privacy policies are accessible on the WE Kidz Pediatrics website which can be located at https://wekidzpediatrics.com/policies/

9.5.2. Patients are informed of their right to request a copy of the full privacy policy or to inquire about how their information is collected, used and safeguarded.

10. **Record Retention**

10.1. WE Kidz Pediatrics retains patients' medical records in accordance with Ontario law, the Personal Health Information Protection Act (PHIPA), and professional guidelines set out by the College of Physicians and Surgeons of Ontario (CPSO). The purpose of record retention is to ensure continuity of care, satisfy legal and professional obligations and to maintain documentation of each patients' healthcare history.

10.1.1. Adult Patient Records: The medical records of adult patients must be retained for a minimum of ten (10) years from the last date of service recorded. This period ensures

that documentation is available for medical, legal or insurance related inquiries that may arise after the last date of service.

10.1.2. Records of Minors: The medical records of patients who are under the age of 18 must be retained until 10 years after the date on which the patient reach (or would have reached) the age of majority. This requirement ensures continuity of information as minors transition into adult care and provides an appropriate time frame for medical, legal or insurance related inquiries.

10.1.3. In some instances, records may be retained longer when clinically, legally or administratively appropriate. The CPSO recommends maintaining medical records for a minimum of fifteen (15) years when feasible, to accommodate ongoing or complex care histories, legal matters or chronic conditions.

10.2. The CMPA (Canadian Medical Protective Association) advises that physicians retain medical records for at least ten (10) years from the date of last entry or for minors, ten (10) years after reaching the age of majority (18 or 19 depending on jurisdiction). This practice aligns with risk-management principles and provides sufficient documentation in the event of a future complaint, audit or legal inquiry.

11. **Secure Disposal and Destruction of Personal Health Information**:

11.1. When medical records are no longer required to be retained under legal, professional, or clinical obligations, WE Kidz Pediatrics ensures that they are securely and permanently destroyed. The goal is to prevent unauthorized access, reconstruction, or misuse of personal health information (PHI) once its retention period has expired. All destruction activities are carried out in accordance with PHIPA, CPSO guidelines and professional best practices.

11.1.1. Paper medical records are destroyed using cross-cut shredding or by a certified document destruction company that meets PHIPA and CPSO security standards.

11.1.2. Electronic data is destroyed through digital wiping, degaussing or physical destruction of storage media ensuring no data remains recoverable. This includes but is not limited to computers, servers, USB drives and backup media. Devices that are reused within the clinic are wiped and re-encrypted before being redeployed in the practice.

11.2. Oversight and Documentation:

11.2.1. WE Kidz Pediatrics seeks to obtain expert technical advice to ensure proper destruction methods are used for modern data formats and ever evolving technologies.

11.2.2. A disposal log is kept maintaining accountability recording:

11.2.2.1. The patient's name or file number

11.2.2.2. The retention period covered by the destroyed record

11.2.2.3. The method of destruction

11.2.2.4. The date of destruction

11.2.2.5. The name and role of person (or company) who supervised and/ or performed the destruction.

11.2.3. This documentation is retained permanently as proof of compliance with privacy and retention standards. All destructions are carried out under the supervision of the privacy officer or designated custodian, who then confirms that the destruction meets the legal and professional requirements. If an external vendor is sourced, a Confidentiality and Data-Destruction Agreement must be signed before the destruction is performed.

11.3. Security and Risk Mitigation:

11.3.1. Destruction processes are scheduled routinely and performed in a secured and controlled environment. Access to materials awaiting destruction is strictly limited to authorized personnel. Any suspected loss, theft or mishandling during destruction is immediately reported and investigated as a potential privacy breach.

11.3.2. The practice periodically reviews its destruction and disposal protocols to ensure compliance with evolving privacy standards, new data technologies and IPC, PHIPA and CPSO requirements. Staff involved in record management are IT maintenance receive ongoing training to ensure consistent application of these safeguards.

12. **Access to Health Information**:

12.1. Patients reserve the right to access their medical records in a timely and organized manner.

12.2. Requests for access should be directed to the privacy officer for review and coordination.

12.3. Should a patient request a copy of their medical record, it will be provided at a reasonable cost in accordance with the Ontario Medical Association (OMA) fee schedule.

12.4. Access will only be granted following the approval by the physician or authorized custodian to ensure accuracy, completeness, and compliance with privacy regulations.

12.5. If a patient wishes to review their original record on-site, a staff member must be present during the review. A reasonable fee may apply for this service.

12.6. Requests for information may be made verbally or in writing. Written requests are preferred to ensure clarity and proper documentation

12.7. WE Kidz Pediatrics follows strict guidelines and procedures to respond to health information access requests.

12.7.1. We acknowledge receipt of the request.

12.7.2. We respond to the request for access within 30 days of the receipt of the request.

12.7.3. If replying to the request within 30 days is deemed unreasonable or impractical, an extension of 30 days may be granted. Notice of such extension must be provided in writing to the requestor.

13. **Limitations on Access**:

13.1. Patients may be denied access to their medical records only where such denial is permitted or required by law.

13.2. Legal exceptions to the right to access include, but are not limited to the following circumstances:

13.2.1. Granting access could reasonably be expected to result in serious harm to the patient or the public.

13.2.2. Providing access would reveal personal information about another person who has not provided consent to disclose the information.

13.2.3. The record contains raw data from standardized psychological test or assessments that, if released, could compromise the validity or interpretation of those assessments.

13.2.4. The information in the record was collected for the purpose of an inspection, investigation or similar proceeding that is authorized by law and is still ongoing or incomplete.

13.2.5. The request for access is determined to be frivolous, vexatious or made in bad faith.

13.3. If only a portion of the record is subject to a legal exception, WE Kidz Pediatrics will make every reasonable effort to separate and withhold the exempted information and provide access to the remainder of the record to be lawfully disclosed.

14. **Accuracy of Information**:

14.1. WE Kidz Pediatrics makes every reasonable effort to ensure that all patient information is accurate, complete and up to date at the time it is collected, used and disclosed.

14.2. Should a patient identify an inaccuracy in their record, they may request that a correction or clarification be made. All such requests will be documented in the patient's medical record as well as the outcome of the review.

14.3. Any amendment or notation to a medical record must receive the approval or authorization of the physician or designated health information custodian prior to being added.

14.4. If the physician or custodian determine that a correction cannot be made, the patient will be informed of the reason and a statement of disagreement may be added to the record upon the patient's request, in accordance with PHIPA.

15. **Privacy Education and Training**:

15.1. WE Kidz Pediatrics conducts mandatory updated annual privacy training to ensure that all individuals who provide care or assist within the practice are aware of their obligations under this policy and PHIPA as well as the consequences of breaching the agreements.

15.2. Our training includes, but is not limited to:

15.2.1. The purpose for which employees and others affiliated with WE Kidz Pediatrics are permitted to collect, use, and disclose personal health information.

15.2.2. The updated limitations, conditions and/ or restrictions governing the collection, use and disclosure of personal health information.

15.2.3. The current privacy policies and procedures implemented and followed by WE Kidz Pediatrics.

15.2.4. WE Kidz Pediatrics obligations under PHIPA.

15.2.5. The duty to notify the privacy officer at the first reasonable opportunity if personal health information is stolen, lost or accessed by unauthorized persons.

15.2.6. Quarterly audits, reviews and ongoing monitoring of the collection, use, and disclosure of personal health information.

15.2.7. The consequences of a breach of this policy or the obligations imposed by PHIPA.

15.2.8. Overview the administrative, technical and physical safeguards implemented to protect personal health information.

16. **Employee Exit Protocol**:

16.1. The purpose of this protocol is to ensure that when an employee, volunteer student, or contractor dissolves a relationship with WE Kidz Pediatrics, whether voluntary or involuntary, all access to personal health information, clinical systems, and organizational property is securely terminated to protect the privacy, security, and integrity of both patient and business information.

16.2. This protocol extends to all staff members, including clinical, administrative, and technical personnel, as well as temporary or contract workers with success to WE Kidz Pediatrics information systems, facilities or confidential information.

16.3. The privacy officer is responsible for overseeing the employee exit process and ensuring all steps are completed prior or on the final day of employment.

16.4. The procedure process is as follows:

16.4.1. Revoking all electronic access, including EMR, email, scheduling systems, shared drives and other secure messaging platforms. All usernames, passwords and two-factor authorization token are immediately disabled upon termination or notice period completion. The departing employee's access to internal communication systems (fax servers, patient portals and telehealth accounts) are immediately revoked. Ensure that any staff directories or role-based access lists are updated to reflect the departure of the employee.

16.4.2. All keys, keycards, identification badges, fobs and office access devices will be collected. Any equipment issued by the clinic, such as laptops, tablets, USB drives, phones and/ or storage devices are retrieved prior to dismissal. We confirm that no patient information, paper files, or digital copies remain in the employee's possession. This can include emails accounts, home devices or cloud storage.

16.4.3. Conduct an exit meeting to review confidentiality obligations, including ongoing compliance with PHIPA and clinical privacy policies even after employment ends. Update audit trails and password management logs to reflect the removal of access. Report any potential security breaches to the privacy officer immediately.

16.4.4. Departing employees remain legally and ethically bound by confidentiality obligations under PHIPA and WE Kidz Pediatrics' privacy policies. Disclosure or misuse

of personal health information after employment may be subject to legal and regulatory actions.

17. **Privacy Complaints**:
    17.1. We Kidz Pediatrics is committed to ensuring that our privacy policies and practices effectively address patient concerns and respond to patient needs.
    17.2. A patient who believes that WE Kidz Pediatrics has not appropriately responded to their access request or has mishandled their personal health information is encouraged to first discuss the concern with their physician.
        17.2.1. Patient complaints may be made verbally or in writing.
        17.2.2. WE Kidz Pediatrics follows specific, clearly defined procedures for receiving, reviewing, and resolving privacy complaints.
            17.2.2.1. Our complaint process is designed to be easily accessible, transparent, and simple to use.
            17.2.2.2. Patients are informed of the available complaint mechanisms and are provided with guidance on how to file a complaint.
            17.2.2.3. The privacy officer will acknowledge receipt of the complaint, investigate the concern, and provide a written summary of findings and corrective actions taken.
        17.2.3. If patients wish to pursue the matter further after receiving a response from, WE Kidz Pediatrics, they may direct their complaints to one of the following authorities:
            17.2.3.1. The appropriate regulatory college, if the concerns relate to a regulated healthcare provider.
            17.2.3.2. The Information and Privacy Commissioner of Ontario (IPC), who oversees compliance with PHIPA.
    17.3. All privacy complaints, investigations, and resolutions are documented and retained in accordance with the organization's record retention schedule. Information obtained through the complaint process is maintained confidential and used solely for the purpose of resolution and improvement of privacy practices.

18. **Breach of Privacy Policy**:
    18.1. Purpose: To outline the potential consequences and accountability measures associated with a breach of WE Kidz Pediatrics privacy policy or the Personal Health Information Protection Act. This section ensures all staff and associates of WE Kidz Pediatrics understand the seriousness of privacy obligations and the implications of non-compliance.
    18.2. Definition: A breach occurs when personal health information is collected, used, disclosed, retained, or disposed of in a manner that contravenes PHIPA or WE Kidz Pediatrics' established privacy policies and procedures. Breaches may be intentional or accidental.
    18.3. Examples of privacy breaches include, but are not limited to:
        18.3.1. Unauthorized access to a patient's record by an employee.

18.3.2. Loss or theft of paper or electronic records which contain personal health information.

18.3.3. Sending patient information to the wrong recipient via fax, email or mail.

18.3.4. Discussing patient information in public areas or with unauthorized individuals.

18.3.5. Failure to secure electronic devices, files or passwords containing personal health information.

18.4. Breaches of this policy or PHIPA may result in a disciplinary, legal, or regulatory action, which can include but not limited to:

18.4.1. Internal disciplinary action including suspension or termination of employment or contract with WE Kidz Pediatrics.

18.4.2. Disciplinary measures by the appropriate regulatory college or licensed health professionals.

18.4.3. Legal and financial penalties:

18.4.3.1. Under PHIPA, individuals may be subject to fines up to $200,000, and organizations up to $1,000,000.

18.4.3.2. Civil legal action may also be taken by individuals affected by a privacy breach. Criminal proceedings in cases of wilful or malicious breaches. The Information and Privacy Commissioner of Ontario (IPC) may issue binding orders, require corrective measures and make findings public

18.5. WE Kidz Pediatrics takes all privacy breaches seriously and will respond promptly to identify root causes, contain the incident, and to prevent recurrence. All breaches are revied by the privacy officer and when required, are reported to the IPC and affected individuals in accordance with PHIPA reporting obligations.

18.6. All employees, staff, students and contractors are required to immediately report any suspected or actual breaches, Delayed or unreported breaches may be subject to additional disciplinary action.

19. **Privacy Breach Response Protocol**:

19.1. The purpose of this protocol is to establish clear steps for identifying, containing, reporting and remediating any privacy breach involving personal health information at WE Kidz Pediatrics. All breaches will be handled promptly and in accordance with PHIPA and governing organizational policy to minimize harm and prevent recurrence.

19.2. Upon learning of a possible or confirmed privacy breach, WE Kidz Pediatrics will immediately take steps to contain the incident to the best of our ability, including:

19.2.1. Retrieving hard copies of personal health information that may have been disclosed or misplaced.

19.2.2. Ensuring that no copies, backups or screenshots remain accessible to unauthorized personnel.

19.2.3. Taking technical steps to prevent further unauthorized access to electronic information, such as, but not limited to:

19.2.3.1. Changing system passwords and user access credentials.

19.2.3.2. Restricting or suspending system access.

19.2.3.3. Temporarily shutting down affected systems or accounts, if necessary.

19.2.3.4. Securing the area and equipment involved in the breach and preserving relevant audit logs for investigation.

19.2.4. In accordance with PHIPA, affected individuals and appropriate authorities will be notified promptly when a suspected or confirmed breach of personal health information occurs. These notifications will contain sufficient detail to explain the incident, which information has been affected and what actions are being taken.

19.3. The privacy officer will lead a full investigation to determine the cause and scope of the breach. This includes, but is not limited to:

19.3.1. Conducting an internal review of the incident, systems and staff actions involved.

19.3.2. Determining what steps should be taken to prevent similar breaches in the future.

19.3.3. Implementing the incident and response in the privacy breach log, including dates, actions taken and outcomes.

19.4. All details related to the breach will be heavily documented including date of the occurrence, nature of the breach, persons notified, corrective measures taken and follow up activities. The records will be retained in accordance with WE Kidz Pediatrics' record retention schedule and made available to regulatory authorities upon request.

19.5. Following the resolution of each breach, the privacy officer will conduct a post-incident review to assess the effectiveness of the response and identify opportunities for improvement. Recommendations from this review will be implemented promptly and incorporated into ongoing staff training and policy updates.

20. **Challenging Compliance**:

20.1. This section outlines how patients, parents or substitute decision-makers can challenge WE Kidz Pediatrics' compliance with our privacy policies and the Personal Health Information Protection Act (PHIPA). It ensures patients are educated on how to raise concerns, receive a timely response, and escalate their complaint should they remain unsatisfied.

20.2. WE Kidz Pediatrics is committed to maintaining transparency, accountability and trust will all patients and families. We encourage open communication about how personal health information is collected, used, disclosed, or stored. Concerns about privacy policies will be addressed respectfully, promptly and without fear of reprisal.

20.3. Patients may contact the privacy officer in person, by phone, or in writing to express concerns about the WE Kidz Pediatrics' practices and compliances with PHIPA. The privacy officer will acknowledge receipt of the concern within a reasonable timeframe and initiate a review. The review may involve gathering details, interviewing relevant staff, and reviewing policies, logs and audit records to determine whether a privacy breach or non-compliance occurred. Findings and corrective measures, if applicable, will be communicated in writing. All outcomes are documented in the privacy compliance log, which is reviewed quarterly to identify patterns or areas requiring policy improvement.

20.4. If a patient or their representative believes their concern has not been adequately addressed by, WE Kidz Pediatrics, they have the right to escalate the matter to:

20.4.1. The appropriate regulatory college (example, CPSO, College of Physicians and Surgeons of Ontario) if the concern involved a regulated health professional.

20.4.2. The Information and Privacy Commissioner of Ontario (IPC), who oversees compliance with PHIPA and has authority to investigate privacy complaints independently.

20.5. In most cases, an issue can be resolved by simply discussing it with us. You can reach us at:

210-2055 Huron Church Rd
Windsor, Ontario N9C 2L6
Phone: (519) 915-1207
Email: admin@wekidzpediatrics.com

If after contacting us, you feel that your concerns have not been addressed to your satisfaction, you have the right to complain to the Information and Privacy Commissioner of Ontario (IPC). The commissioner can be reached at:

1400-2 Bloor St E
Toronto, Ontario M4W 1A8
Telephone: (416) 326-3333 Toll-Free: 1 (800) 387-0073
Fax: (416) 325-9195
Website: www.ipc.on.ca

All complaints and challenges received under this section are recorded in the privacy compliance log along with their resolutions. The privacy officer reviews all logged items quarterly to ensure corrective actions are completed and recurring issues are addressed. Trends that have been identified may lead to staff retraining, procedural updates or revisions to current privacy policies to improve over all compliance.