Data Protection Statement

ErinoakKids operates as a Health Information Custodian (HIC) under Ontario's *Personal Health Information Protection Act* (PHIPA) and is therefore authorized to collect personal health information in accordance with PHIPA. Our clients entrust us with their personal health information and personal information (together referred to as "protected data"). We are committed to ensuring the security and confidentiality of the protected data in our care. We achieve this through a range of safeguards designed to protect individuals' privacy and to comply with applicable laws and regulations governing the handling of sensitive information.

Here's a general description of the safeguards we implement:

Physical Security Measures: We employ physical security measures to safeguard protected data. This includes secure premises, access controls, surveillance systems, and restricted access to areas where data is stored.

Technical Safeguards: We utilize various technical measures to protect data from unauthorized access, loss, alteration, or disclosure. These include firewalls, encryption, strong authentication mechanisms, regular system updates, and monitoring tools to detect and prevent security breaches.

Confidentiality Agreements: We ensure that all employees, contractors, and partners who have access to protected data sign confidentiality agreements. These agreements hold third parties to the standards of data protection mandated by the ErinoakKids Privacy Policy.

Access Controls: We implement data access controls to ensure that only authorized individuals can access protected data. Access privileges are granted based on the principle of least privilege, meaning that individuals are only given access to the data necessary for performing their job responsibilities.

Employee Training and Awareness: We provide regular training and awareness programs to our employees regarding data security and privacy practices. This includes educating staff about their responsibilities, best practices for data handling, and the potential risks associated with data breaches.

Data Encryption: We use encryption techniques to protect data during transmission and storage. Encryption ensures that even if unauthorized individuals gain access to the data, they cannot decipher its contents without the encryption keys.

Incident Response and Monitoring: We have established incident response procedures to quickly and effectively respond to any security incidents or data breaches. Additionally, we employ monitoring systems to detect and mitigate any potential threats or vulnerabilities proactively.

Data Retention and Disposal: We follow appropriate data retention and disposal policies to ensure that protected data is retained only for the necessary duration and securely disposed of when no longer needed.

Third-Party Vendor Management: When engaging third-party vendors or service providers, we conduct assessments of their security and privacy practices. Contracts or agreements are established to ensure that vendors adhere to appropriate data protection standards.

Regulatory Compliance: We comply with all relevant laws and regulations pertaining to data protection and privacy, such as child and youth, personal information, and personal health information regulations.