Pearwell Privacy Policy

Last Updated: June 20, 2025

Introduction

Pearwell Co., Ltd. ("**Pearwell**," "**we**," "**us**," or "**our**") is a clinic automation partner serving elective care clinics in Thailand. We are committed to protecting the privacy of our clinic clients and their patients. This Privacy Policy explains what personal information we collect, how we use and protect it, and the rights and choices you have in relation to your data – in compliance with Thailand's Personal Data Protection Act B.E. 2562 (2019) ("**PDPA**") [1] [2]. We adhere to applicable privacy laws and general best practices to ensure individuals maintain control over how their personal data is collected, used, and shared [2]. By using Pearwell's website or services, you agree to the practices described in this Policy. This Policy is designed to be adaptable and will be updated as our services and legal requirements evolve.

Information We Collect

We collect personal data from our clinic clients (the clinics we serve) as well as from their end users (patients), and from visitors to our website. We only collect what is necessary for specified purposes and **clearly communicate what data we collect and why** [3]. The types of information we may collect include:

- **Clinic Information:** Contact details of clinic personnel (such as owners or staff), including names, work email addresses, phone numbers, and clinic addresses. We also collect business details needed to set up and support the clinic's account (e.g. clinic name, specialty, operating hours, and service offerings). If a clinic signs up for our services, we may collect login credentials and payment or billing information from the clinic's authorized personnel for account management purposes.

- **Patient Personal Data:** Information about patients that is provided by the clinic or directly by patients through Pearwell's automated systems. This typically includes name, contact information (phone number, email, LINE ID or WhatsApp number), appointment dates and times, and the nature of the appointment or inquiry (e.g. the type of elective procedure or service being booked). It may also include communication history (such as chat transcripts or call recordings) when patients interact with Pearwell's AI assistant or messaging system as part of booking or customer service. If any health-related or medical information is collected (for example, treatment preferences, medical conditions relevant to an appointment, or preliminary medical history questions), we handle it as **sensitive personal data** and obtain explicit consent as required by law [4]. Pearwell does **not** seek to collect extensive medical records; any health data collected is limited to what the clinic needs for scheduling or consultation purposes, and it is processed with heightened protection since health information is classified as sensitive under the PDPA [4].

- **Communications and Support Data:** If you contact Pearwell for support or general inquiries (whether as a clinic or as a patient using our system), we will collect the information you provide in

that communication. This may include your name, contact information, and a record of the correspondence (emails, chat logs, or call notes) to address your inquiry and improve our customer service.

- **Website Usage Data and Cookies:** When you visit our website (pearwell.com), we automatically collect certain technical information via cookies and similar technologies. This includes your device's IP address, browser type, operating system, referring URLs, and browsing behavior on our site (such as pages viewed and actions taken). We use cookies to distinguish you from other users and to remember your preferences. Some cookies are **essential** for site functionality (for example, to keep you logged in on the clinic dashboard), while others are **analytics** cookies that help us understand website traffic and improve our content. We do **not** use cookies for advertising or unrelated third-party marketing. Details on our cookie usage are provided in the *Cookies and Analytics* section of this Policy. You can control or delete cookies through your browser settings at any time. (See *Cookies and Analytics* below for more information.)

Note: Pearwell's services are not directed to individuals under the age of 20 (or the age of majority as defined by local law) without parental consent. We do not knowingly collect personal data from minors. If we discover we have inadvertently received personal data from a minor without proper consent, we will delete it. Clinics using Pearwell should ensure any patient data they input has been collected in compliance with PDPA consent requirements.

How We Use Personal Data

Pearwell uses the collected information to provide and improve our clinic automation services. We limit use of personal data to the purposes for which it was collected, and we ensure there is a lawful basis (such as consent or contractual necessity) for each use [5]. Specifically, we use personal data for the following purposes:

- **Service Delivery and Automation:** We process patient and clinic information to automate front-desk workflows for clinics. For example, we use patient contact details to schedule appointments, send booking confirmations, and deliver appointment reminders via phone call, SMS, LINE, or WhatsApp on behalf of the clinic. Our AI-driven system may use basic information (such as the clinic's FAQs or a patient's appointment reason) to answer patient inquiries or route messages appropriately. All such processing is done to fulfill the services that clinics have contracted for – essentially acting as a 24/7 virtual receptionist for the clinic.

- **Communication:** We use provided contact information to communicate with both clinics and patients as needed. Clinics receive updates about their service (e.g. system alerts, usage reports, or training materials), and patients receive notifications related to their appointments (e.g. reminders, follow-ups or feedback requests) as instructed by the clinic. We ensure messages to patients are relevant to their clinic care and sent in accordance with their preferences and consents. Pearwell does not send promotional or marketing messages to patients on its own behalf. Clinic clients may occasionally receive Pearwell service updates or marketing communications about new features; we will only send such communications to clinic contacts in line with applicable law, and provide an easy opt-out mechanism (for example, an "unsubscribe" link in emails). If a recipient objects to or opts out of marketing communications, we will honor that choice and cease such communications [6].

- **Customer Support and Account Management:** We use data (clinic and patient information, as necessary) to provide support and resolve issues. For clinics, this means we may access account details or relevant patient interaction logs when you reach out with a question or problem, in order to assist you. For example, if a clinic inquires about a missed appointment notification, we might review the related reminder log. For patients who contact us (or whose inquiries are escalated to human support), we use their information to address concerns (e.g. helping with rescheduling or technical issues with the AI system) in coordination with the clinic as needed. All support-related accesses are logged and confidential.

- **Service Improvement and Development:** We may analyze usage data, system logs, and aggregated interactions (which do not identify individuals) to understand how our services are performing and where improvements are needed. For instance, we might review anonymized chat transcripts or call outcomes to refine our AI responses or to identify frequently asked questions that could be better answered. We use analytics (including website analytics and in-service analytics) to fix bugs, optimize user experience, and develop new features. **Important:** When using conversation data to improve our AI, we either remove or pseudonymize personal identifiers so that individuals cannot be readily identified, ensuring the data is used in a privacy-preserving manner. This processing for improvement is based on our legitimate interest in enhancing our services, but we perform it under strict confidentiality and security controls.

- **Data Security and Fraud Prevention:** We may use information as necessary to protect the security of our services, our clients, and their patients. This includes monitoring for and preventing unauthorized access, spam, malware or other security risks. For example, we may log and analyze IP addresses or login attempts to detect suspicious activities and to authenticate users. We also maintain audit trails of system use to trace and prevent any misuse of patient data.

- **Legal Compliance and Enforcement:** Where required, we will use personal data to comply with legal obligations, such as fulfilling lawful requests from authorities or maintaining records required by law. We may also process data as needed to establish or defend legal claims. For example, PDPA and other laws may obligate us to retain certain transaction records or to report certain activities. If we are involved in a dispute or legal process, relevant data may be used to protect our rights or the rights of others. Additionally, if a patient or clinic exercises their data protection rights (such as a request to access or delete data), we will use personal information to verify their identity and fulfill the request as legally required.

We do **not** sell personal data to third parties, and we do not use personal data for purposes incompatible with those described above without obtaining additional consent. If we ever need to process personal data for a new purpose, we will update this Privacy Policy and/or provide notice and obtain consent as required by law. Our goal is to be transparent about why we collect data and how we use it, consistent with PDPA's requirements that businesses clearly communicate what data is collected and why [3].

Third-Party Services and Disclosures

Pearwell may share personal data with third-party service providers and partners strictly to facilitate the purposes described above. Whenever we share data, we do so under confidentiality and security obligations and in accordance with data protection law. Key instances of third-party involvement include:

- **Communication Platforms:** We integrate with external communication services to deliver messages. For example, we may send appointment reminders or chat messages to patients via **LINE**, **WhatsApp**, SMS, email or phone calls. This means that basic contact information (such as phone number or LINE/WhatsApp ID) and message content necessary for the reminder or response will be transmitted to those platforms to reach the user. We use official APIs or business services of these platforms, and personal data is handled according to the platforms' own privacy policies when transmitted (for instance, WhatsApp messages are end-to-end encrypted by design). We encourage users to review the privacy practices of these platforms. Pearwell only shares the minimum data required (e.g. your first name, appointment time and a short message) to achieve the communication. **No sensitive medical details are included in these automated messages** unless absolutely necessary and consented to (for example, a brief reference like "doctor consultation" may be included, but not detailed health information).

- **Cloud Hosting and IT Infrastructure:** Our software and databases are hosted on secure cloud servers (for example, reputable cloud service providers or data centers). Personal data (including patient and clinic information) is stored and processed on these servers. We choose hosting providers that implement strong security standards and, when possible, maintain servers in Thailand or jurisdictions with adequate data protection standards. However, some data may be stored or backed up on servers located in other countries. In such cases, we comply with PDPA's cross-border data transfer requirements by ensuring the recipient country has adequate data protection or by using appropriate safeguards like standard contractual clauses or certifications [7]. All third-party data storage providers are bound by data processing agreements to protect your data and use it only for providing services to us [7].

- **Analytics and Website Tools:** We may use third-party analytics services (such as Google Analytics) on our website to gather information about site traffic and usage patterns. These analytics services may set cookies or collect internet log information and visitor behavior information in an anonymized or pseudonymized form. This helps us analyze metrics like page views, session duration, and referral sources to improve our web presence. The information collected typically does not directly identify individuals (and IP anonymization is enabled where applicable). Nonetheless, you can opt out of analytics cookies as described in the *Cookies and Analytics* section. Analytics providers are not permitted to use the data collected on our behalf for their own purposes.

- **Payment and Administrative Services:** If we use third-party payment processors or invoicing systems to handle clinic subscription payments, we will share necessary billing information (such as clinic name, billing contact, and payment details) with those processors. These entities are authorized to use the information only as needed to process transactions or manage our accounts. All payment transactions are encrypted and handled securely; Pearwell itself does not store full credit card numbers on our systems (such information would be handled by the payment gateway in compliance with payment security standards).

- **Other Trusted Vendors:** In running our business, we may rely on other vendors for functions like email delivery (for sending out newsletters or system emails), customer relationship management (CRM) tools, or IT support services. Such vendors may incidentally process personal data (for example, an email address in a mailing list, or a support ticket containing personal information). We vet all our vendors for strong data protection practices and sign **Data Processing Agreements (DPAs)** with each, contractually requiring them to safeguard personal data and to use it solely for the purposes of providing services to Pearwell [7] . These vendors are not allowed to disclose or sell your data, and they must notify us of any security incidents involving your data. We remain responsible for the protection of your personal data when it is processed by our service providers, and we ensure adequate safeguards are in place.

We do not disclose personal information to any third parties except as described above, or as required by law. We may disclose information if we are compelled by a lawful request (such as a court order, subpoena, or regulatory requirement), but we will verify the legitimacy of such requests and only provide the minimum necessary data. Additionally, in the event of a corporate transaction such as a merger, acquisition, or asset sale, personal data may be transferred to the new owner as part of the business assets. If such a transfer occurs, we will ensure the recipient commits to the same level of privacy protection outlined in this Policy, and we will notify our clients (and obtain consent where required by law). In all cases of data sharing, Pearwell adheres to the principle of **data minimization** – only sharing what is needed – and to PDPA's standards for protecting data throughout its lifecycle [8] .

Data Retention and Deletion

Pearwell retains personal data only for as long as necessary to fulfill the purposes for which it was collected, or as required or permitted by law. We have policies in place to prevent indefinite retention of personal information. In general:

- **Clinic Data:** Information about our clinic clients and their use of the service is retained for the duration of the business relationship and for a reasonable period thereafter. This allows us to maintain service records, comply with financial and legal obligations, and facilitate a smooth restart if a clinic resumes service. For example, billing records and communications may be kept for a certain number of years to comply with accounting laws or PDPA record-keeping requirements.

- **Patient Data:** Patient personal data processed on behalf of our clinic clients is retained as instructed by the clinic (the data controller) and as needed to provide the services. In practice, this means we will keep appointment and communication records for the timeframe that the clinic's account is active, since these records form part of the clinic's operational history (e.g. to track bookings or conversation outcomes). We rely on clinics to determine how long they need to keep their patient data in Pearwell. Clinics may have their own retention policies (for example, many medical service providers retain appointment records for a number of years). Pearwell provides tools or accepts requests to delete or anonymize patient data that is no longer needed. When a patient's personal data is no longer necessary (for instance, if a clinic requests deletion of a particular patient record, or if a patient withdraws consent for us to hold their data and the clinic approves deletion), we will securely erase or anonymize that data from our systems. In any case, once a clinic client relationship ends, we either return the patient data to the clinic and/or purge it from our systems after a defined retention period, except for any information we are legally required to retain.

- **Website Data:** Web analytics data (collected via cookies) is typically retained in aggregate form for analysis, usually for a few months up to a couple of years, depending on the tool, after which it is automatically deleted or anonymized. Cookie data is often ephemeral – for example, some cookies expire after your session or after a set number of days. We do not keep personally identifying web visit logs longer than necessary for security monitoring or analysis.

- **Communications:** Support emails or inquiries we receive are retained as long as needed to resolve your question and for our reference. These records are generally kept for a period (e.g. 1-2 years) in case you have follow-up issues, and to train our support team, unless you request a deletion and we have no overriding need to keep them. Voice call recordings (if any are made for quality assurance when the AI handles calls) are kept only briefly for analysis and then deleted or anonymized, unless they are needed longer to investigate an issue.

When we delete personal data, we ensure it is done securely so that it cannot be reconstructed or read. This may involve permanent erasure from our databases and deletion of any backup copies. In cases where complete deletion is not immediately feasible (for example, data stored in long-term backups), we will isolate and protect the data until deletion is possible. We also may retain data in an anonymized form (stripped of personal identifiers) for statistical or service improvement purposes – in such cases, the data will no longer be associated with any individual and is not considered personal data.

Please note that certain laws (including PDPA and medical regulations) might require us or our clinic clients to retain specific information for a minimum period (for example, for auditing, accounting, or dispute resolution). In such cases, we will retain that data to comply with our legal obligations but will not use it for any other purpose. Once the retention period expires, or if we determine that the data is no longer needed and not legally required, we will proceed with deletion or anonymization.

If you have any specific questions about our data retention practices or would like to request deletion of your data, you can contact us (see the **Contact Us** section). We will respond in accordance with the **Data Subject Rights** section of this Policy and applicable law.

Data Security and Confidentiality

Pearwell takes the security of personal data very seriously. We have implemented a comprehensive set of security measures to prevent unauthorized access, use, alteration, or disclosure of personal information. These measures are designed to meet or exceed industry standards and the requirements of Thai law [9]. Key security practices include:

- **Administrative Safeguards:** We limit access to personal data strictly on a need-to-know basis. Only authorized Pearwell employees and contractors who require access to perform their duties (for example, a support engineer troubleshooting a specific issue) are granted access to client or patient data, and even then, only to the extent necessary. All staff are trained in confidentiality and data protection procedures. They are bound by contractual confidentiality obligations to ensure your information remains private. We conduct background checks where appropriate and ensure that any personnel with access to sensitive data understand their responsibilities under PDPA and our internal policies. Regular training on data privacy and security is provided to keep our team up-to-date on best practices and legal obligations.

- **Technical Safeguards:** We use modern encryption protocols to protect personal data during transmission and storage. For instance, our website and web application utilize HTTPS (TLS encryption) to secure data in transit between your device and our servers. Sensitive data (such as passwords or health-related notes) is encrypted at rest in our databases. We employ firewalls and network security monitoring to guard against external threats. Our systems are regularly updated with security patches to mitigate vulnerabilities. We also implement access controls and authentication mechanisms (such as strong password requirements, two-factor authentication for administrative accounts, and role-based access controls) to ensure that only authorized users can access data. Audit logs are maintained to record access and modifications to personal data, helping us detect and investigate any irregularities.

- **Physical Safeguards:** For any servers or data centers that house personal data, we rely on providers with robust physical security (secure facilities with access control, surveillance, and environmental protections). Server rooms and data centers are accessible only to authorized personnel of the hosting provider and are protected from physical intrusion, damage, or theft. Where we maintain any on-site systems or backups, those are kept in locked, access-controlled environments.

- **Monitoring and Testing:** We continuously monitor our systems for potential security events or anomalies. Our security team (or managed security services) receives alerts for unusual activities, and we have an incident response plan to quickly address and mitigate any security issues. We conduct periodic security assessments and penetration tests through qualified professionals to identify and fix potential weaknesses. If any system or process is found to be insufficient, we promptly strengthen it.

- **Confidentiality by Design:** Our platform is built with privacy in mind. By default, we apply data minimization (only storing data that is needed) and pseudonymization where feasible. For example, internal developers testing system improvements use dummy data rather than real personal data. Any personal data used for training our AI (as mentioned, for improving responses) is anonymized. We also design our AI assistants and features to handle personal information discreetly – for instance, an AI chatbot's logs will refer to users by an ID rather than by full name in most cases, to reduce exposure of identity in our internal analysis tools.

While we strive to protect your personal data with a high level of care, it's important to note that no security system is absolutely foolproof. However, we follow the required standards and continually improve our safeguards in line with the PDPA's security regulations [9] and global best practices. In the unlikely event of a **data breach** (for example, a security incident that results in accidental or unlawful loss, access, or disclosure of personal data), we will promptly take steps to contain and remedy the breach. This includes notifying affected clients and individuals as appropriate and in accordance with PDPA's breach notification rules, and reporting to regulators when required [10]. We document all incidents and responses to learn and prevent future occurrences.

Pearwell also requires our third-party service providers to implement strong security measures. Through our contracts (DPAs), we ensure that any vendor handling personal data on our behalf maintains standards equivalent to our own. We regularly review their compliance where possible (for instance, by reviewing their security certifications or audit reports).

In summary, we maintain administrative, technical, and physical safeguards to protect personal data from unauthorized access or disclosure [9]. We treat all personal data as confidential. If you have any questions about the security of your data, feel free to contact us for more detailed information.

Data Subject Rights and Choices

Pearwell respects the rights of individuals to control their personal data. If you are an individual whose personal data we process (whether you are a clinic client, a patient of a clinic, or a user of our website), you have certain rights under the PDPA (and similar data protection laws) regarding your data. We have established procedures to help you exercise those rights. These rights include:

- **Right to Access:** You have the right to request a copy of the personal data we hold about you, and to receive information about how we have used or disclosed that data. For example, a patient may request to know what information the clinic (via Pearwell) has on file about their appointments, or a clinic staff member may ask for the data associated with their user account. We will provide the requested information, except where we are legally permitted to refuse (for instance, if providing access would infringe on another person's privacy or if a legal investigation is ongoing).

- **Right to Rectification (Correction):** If any personal data we have is inaccurate or incomplete, you have the right to ask us (and/or the clinic, if applicable) to correct it. We encourage clinics to keep their information updated and to update patient records when inaccuracies are discovered. If you notice an error in your data (such as a misspelled name or outdated contact information), you can request a correction and we will work to amend our records promptly.

- **Right to Deletion (Erasure):** You can request that your personal data be deleted or anonymized in certain circumstances. For patients, this might apply if, for example, you no longer want the clinic to keep your contact information in Pearwell's system after your treatment is complete and there is no legal need to retain it. For clinic clients, you might request deletion of certain data when closing your account. We will honor deletion requests to the extent required by law and as practicable. Note that there are exceptions – we might not delete data immediately if it's still needed for the purpose it was collected (e.g. an upcoming appointment), or if we are required by law to keep it for a certain time (e.g. financial records), or if deletion is technically infeasible in backup archives (in which case we will isolate it until deletion is possible). If we cannot fully comply with a deletion request, we will explain why (for example, pointing to the legal requirement to retain it). When we do delete data, we follow secure deletion processes as described in the Data Retention section.

- **Right to Withdraw Consent:** Where we are processing personal data based on your consent, you have the right to withdraw that consent at any time [11]. For instance, if a patient initially consented to receiving automated follow-up messages but later changes their mind, they can withdraw consent to further messages. Similarly, if we rely on consent for any processing of sensitive health information, you can withdraw it. Once we receive notification of consent withdrawal, we will stop the processing that was based on consent (and confirm to you that we have done so), unless we have another lawful basis to continue (for example, if retention is required for legal claims). Withdrawal of consent will not affect the legality of processing done before you withdrew.

- **Right to Object:** You have the right to object to certain processing of your data. For example, you can object to processing that we undertake based on our "legitimate interests," including profiling or

analytics, if you feel it impacts your rights. The most common scenario is objecting to direct marketing – as noted, if we ever send you marketing communications (likely applicable to clinic contacts), you can opt out at any time and we will cease such activities for your data [6]. If you object to any other processing, we will review your request and cease the processing if required by law (or explain our lawful justification for continuing, if applicable).

- **Right to Data Portability:** Under certain conditions, you may have the right to receive your personal data from us in a structured, commonly used and machine-readable format, and to have that data transmitted to another data controller (for example, if you wanted to move your data from Pearwell to another service). This typically applies to data you provided directly and that is processed by automated means. If you require such portable copy of your data (for instance, a clinic might want a CSV export of their patient appointment data, or a patient might request transfer of their records to another clinic), we will accommodate it as much as possible.

- **Right to Restrict Processing:** You can request that we temporarily limit the processing of your personal data in certain situations – for example, while you are contesting the accuracy of the data or if you have objected to processing and we are evaluating your request. During the restriction period, we will not use the data (beyond storing it securely) until the issue is resolved.

- **Right to Be Notified of Data Breach:** PDPA requires that if a data breach occurs that is likely to result in a risk to your rights and freedoms, we must inform the affected individuals and the authorities. While this is our obligation rather than a right you must exercise, we include it here to reassure you that you will be kept informed of any serious issues with your data, should they (unexpectedly) occur.

These rights may be subject to certain conditions or legal exemptions under the PDPA. For example, the PDPA allows organizations to refuse obviously unfounded or excessive requests, or to charge a reasonable fee for repeat requests. However, Pearwell will not charge a fee for a standard rights request and will respond in a timely manner (typically within 30 days of receiving a complete request, as a best practice, unless the law specifies a different timeframe).

Exercising Your Rights: To exercise any of your data subject rights, please contact us using the information in the **Contact Us** section below. Provide sufficient information for us to verify your identity and understand your request (for instance, if you are a patient, let us know which clinic or appointment the request relates to, and provide proof of identity if needed; if you are a clinic representative, we may verify with your registered contact information). We may need to confirm your identity to ensure we do not disclose or delete data at the wrong person's request. If you are a patient of one of our clinic clients, you also have the option to direct your request to the clinic (data controller) you interacted with. The clinic and Pearwell will coordinate to fulfill your request. In fact, clinics have primary responsibility for their patients' data under PDPA, and Pearwell (as a data processor) will assist them in meeting those obligations [8]. So if you feel more comfortable contacting the clinic you visited, you can do so; either way, we will ensure your rights are respected.

Pearwell will address your request as required by law and will inform you of the outcome or any action taken. If we need an extension to deal with complex requests, we will let you know and explain the delay. If we decide we cannot comply with a request, we will provide you with a clear explanation of the reasons

(unless prohibited by law). For example, if you request deletion of data that the clinic must legally keep on record, we may have to refuse but will advise you of that.

Finally, if you believe your data protection rights have been violated, you have the right to lodge a complaint with the Thailand Personal Data Protection Committee (PDPC) or other relevant supervisory authority. We would, however, appreciate the chance to address your concerns first – please contact us with any complaint and we will do our best to resolve it.

Compliance with PDPA and Other Laws

Pearwell's data practices are designed to comply with Thailand's PDPA and to align with international privacy standards. We continuously monitor developments in privacy laws to ensure ongoing compliance. Below are some of the ways we uphold legal and ethical data handling principles:

- **PDPA Compliance:** We treat the PDPA as our primary guiding law for personal data in Thailand. The PDPA grants individuals significant rights and control over their personal information, and imposes duties on us as a service provider to clinics [2]. Pearwell ensures that we have a lawful basis for all personal data processing (for example, obtaining consent from patients where required, or processing under contract with clinics) [5]. We provide clear **privacy notices** (such as this Policy) to inform individuals about the collection, use, and disclosure of their data in accordance with PDPA requirements [8]. We have also instituted measures such as data protection training, incident response plans, and Data Processing Agreements with all our partners, as mandated by PDPA and its subordinate regulations [10]. Because we handle health-related information (scheduling for medical or wellness clinics), we are mindful of PDPA's stricter rules on **sensitive data** and require explicit consent for any processing of health information unless an exemption applies [4]. We also follow any guidelines issued by the Personal Data Protection Committee (PDPC) in Thailand to ensure our practices remain up-to-date. In areas not explicitly detailed by PDPA, we look to globally accepted principles (like those from GDPR) to inform our approach, given that PDPA was influenced by such international standards [2].

- **Best Practices and Global Standards:** In addition to PDPA, we endeavor to meet high privacy and security standards that are recognized globally. This includes applying the concepts of **privacy by design and default** (integrating privacy considerations into our technology from the start), **data minimization** (only collecting what we need for the stated purposes), and **accountability** (keeping records of our data processing activities and regularly assessing compliance). Although our primary market is Thailand, we understand that some clinics might serve international patients or that our services may be accessed from outside Thailand. Therefore, we also consider other relevant laws such as the EU's General Data Protection Regulation (GDPR) and similar frameworks as benchmarks. For instance, our practices around consent, breach notification, and data subject rights are largely consistent with GDPR standards, which are comparable to PDPA in many respects. We want clients and users to have confidence that their data would be protected not just under Thai law but under a broad conception of privacy rights.

- **Cross-Border Data Protections:** As mentioned, if we transfer or store personal data outside of Thailand (which can happen if we use cloud services or communication APIs based in other countries), we will only do so in compliance with PDPA's cross-border data transfer rules. These rules typically require that the destination jurisdiction has adequate data protection standards, or that we

implement appropriate safeguards (such as contractual clauses or certifications) to ensure your data continues to be protected [7]. We keep abreast of PDPC guidance on cross-border transfers and ensure that any such flow of data (e.g., using an AWS server in Singapore, or sending a message via a U.S.-based service) meets the legal criteria. If a particular transfer mechanism becomes invalid or problematic, we will halt or adapt our practices accordingly.

- **Regulatory Cooperation:** We have appointed an internal team member responsible for data protection compliance (a de facto Privacy Officer). If required due to our scale or activities, we will formally appoint a Data Protection Officer ("DPO") according to PDPA criteria. We maintain an open line of communication with legal advisors and, if needed, the regulatory authorities to promptly address any compliance questions. Our advisors (as noted in our company information) include experts in Thai healthcare regulations and technology, helping us stay aligned with both privacy and any sector-specific laws (for example, the Thai healthcare laws regarding patient confidentiality, such as the National Health Act which emphasizes confidentiality of health data [12]).

- **Ongoing Audits and Updates:** Compliance is not a one-time effort. Pearwell commits to regularly reviewing and updating our privacy practices as our business grows or as laws change. We may conduct periodic compliance audits or seek certifications in data protection standards to reinforce our commitment. If we introduce new features or services, we will assess their privacy impact and update this Policy or our internal procedures accordingly to ensure continuous compliance.

In summary, Pearwell complies with the Thai PDPA and follows robust privacy practices to protect personal data. We integrate legal requirements and best practices into every aspect of our service – from how we design our platform to how we train our staff – to maintain trust and confidentiality. Our aim is not just to **meet** the minimum legal requirements, but to **exceed** them where possible, fostering a privacy-first culture that scales as our company grows.

Cookies and Analytics

When you visit Pearwell's website or use our web application, we may use "cookies" and similar tracking technologies to enhance your experience and collect certain information automatically. This section explains our use of cookies and analytics and how you can manage your preferences.

What are Cookies?
Cookies are small text files placed on your device (computer, smartphone, etc.) when you visit a website. They allow the website to recognize your device and store some information about your preferences or past actions. There are different types of cookies:
- *Session cookies* are temporary cookies that remain in your browser's memory only until you close the browser.
- *Persistent cookies* persist for a set period and are used to remember you on subsequent visits.
Cookies can also be categorized by their purpose:
- **Essential Cookies:** These are necessary for the website to function properly. Without them, certain services or features (like logging into the clinic dashboard or remembering your language settings) may not be available.
- **Non-Essential Cookies:** These include cookies used for analytics, performance, and personalization. They help us improve the site but are not strictly required for basic functionality. We **do not use** advertising cookies or tracking cookies for third-party marketing on our site at this time.

How We Use Cookies:
Pearwell uses cookies to provide and improve our web services. For example:
- We set an essential cookie when clinic users log in, to keep them authenticated during their session (so they don't have to re-enter credentials on every page).
- We use cookies to remember certain choices (like a user's chosen interface language or other preferences) to enhance user experience.
- We deploy analytics cookies (such as those from Google Analytics) to collect information about how visitors use our website. This information includes details like which pages are viewed, how long users stay, how they navigate through the site, and what site referred them. The analytics data we collect is aggregated and does not directly identify individual visitors. It helps us understand which content is popular or if there are usability issues on certain pages. This insight is used purely to improve our website design, content, and performance. For instance, if we notice many users dropping off on a certain page, we may investigate and redesign that page.

All cookies used by Pearwell are set in a lawful manner. For cookies that are **not strictly necessary** (such as analytics cookies), we will either:
- Obtain your consent where required (for example, by showing a cookie banner or prompt when you first visit our site, allowing you to accept or reject non-essential cookies), **and/or**
- Provide you with clear information on how to opt out of such cookies.

In practice, because the concept of cookie consent in Thailand is still evolving, we strive to follow international best practices (in line with PDPA's transparency requirements and similar principles under laws like the EU ePrivacy Directive/GDPR). We make it simple for you to choose which cookies you want to allow [13]. If we present a cookie consent banner, you can select to allow all cookies or only certain categories. If you ignore the banner and continue using the site, we will treat that as consent to essential cookies only, and will not set analytics cookies unless you opt in.

Third-Party Cookies:
Aside from our own cookies, certain third-party services we use may set their own cookies on our site. For example, as mentioned, Google Analytics may set cookies (_ga, _gid, etc.) to perform its analysis. Similarly, if we embed content from other platforms (like a YouTube video or a map), those platforms might set cookies. We do not have direct control over third-party cookies, but we ensure that any third-party we allow on our site has robust privacy practices. You have the option to block third-party cookies via your browser settings if you prefer.

Managing and Disabling Cookies:
You have the right to choose whether to accept cookies. Since cookies reside on your device, the easiest way to manage them is through your web browser settings. Most browsers allow you to view, delete, or block cookies (either all cookies or cookies from specific sites). You can usually find these options under the "Settings" or "Preferences" menu of your browser, in the section privacy or security. For example, in Chrome, go to Settings > Privacy and Security > Cookies and other site data. In Safari, go to Preferences > Privacy. You can delete any existing cookies and prevent new ones from being set. However, please note that if you block all cookies, our website's essential features may not work properly (for instance, you might not be able to log in or the site may not remember your preferences). We recommend allowing at least the essential cookies for the best experience.

If you want to opt out of Google Analytics specifically, Google provides a browser add-on for opting out (the "Google Analytics Opt-out Browser Add-on"), which you can install. This instructs Google Analytics not to use your site visit information. Additionally, our analytics cookies (if any) are set to respect global "Do Not Track" signals where possible; if your browser is configured to send a Do Not Track request, our site will honor it by not setting non-essential cookies.

Analytics Data Usage:
Any analytics data collected via cookies is used in accordance with this Privacy Policy. It is only handled by Pearwell or our analytics provider on our behalf, and it is not shared for independent use by any third party. We do not use analytics data to profile individuals or to make decisions about an individual – it's only used in aggregate form for improving our service.

We include cookies and analytics in our Privacy Policy (rather than a separate policy) to provide you with consolidated information [14]. By using our site with cookies enabled, you are deemed to consent to our use of cookies as described here, unless you take steps to disable them. We provide this explanation in line with PDPA's emphasis on clear notification and choice for data subjects regarding any data collection tools [15].

If you have any questions or concerns about our use of cookies and tracking technologies, feel free to contact us. We can provide more details, such as a full list of cookies in use, upon request.

Contact Us

Pearwell welcomes any questions, concerns, or requests you have regarding privacy and data protection. If you need to contact us for any reason related to this Privacy Policy or your personal data, please reach out through one of the following channels:

- **Email:** You can email our data protection team at **privacy@pearwell.com**. This is the fastest way to reach our Privacy Officer or Data Protection Officer (once appointed). Please include in your email your name and contact information, and detail your inquiry or request (for example, if you are requesting data access or deletion, specify the context such as the clinic name or date of interaction). We will respond as promptly as possible, generally within 30 days or earlier if required by law or the urgency of the request.

- **Postal Mail:** If you prefer, you may send written correspondence to our corporate address:

Pearwell Co., Ltd.
1234 Healthcare Innovation Blvd.
Khlong Toei, Bangkok 10110
Thailand

(Note: This is a fictional address for the purpose of this policy. In a real policy, we would list our actual registered office or principal place of business in Thailand.)

Please mark the letter “Attn: Privacy Officer” on the envelope. Keep in mind that postal inquiries may take longer to receive and respond to due to mailing times.

- **Phone:** You may call our office at **(+66) 02-123-4567** during business hours (Monday–Friday, 9:00–18:00 ICT). Please ask for the department handling privacy or data protection. Our staff will either assist you directly or route your call to the appropriate person. Complex requests (like detailed PDPA rights requests) may still need to be put in writing for verification purposes, but we can guide you on the phone about the process.

- **Clinic Clients:** If you are an employee or representative of a clinic using Pearwell, you can also contact your account manager or our client success team with privacy-related questions. They will involve our privacy team as needed.

When contacting us, please avoid sending sensitive personal data (such as identification numbers or medical information) unless it is necessary for your request. We may need to verify your identity especially for rights requests, which might involve a secure process of verification (we will guide you through it).

We are committed to resolving any privacy concerns in a fair and transparent manner. If you have a complaint, we appreciate the opportunity to address it directly. Our goal is to ensure you feel safe and informed in all interactions with Pearwell’s services.

Changes to This Privacy Policy

Pearwell may update this Privacy Policy from time to time to reflect changes in our services, legal obligations, or privacy practices. We encourage you to review this Policy periodically for any updates. When we make significant changes, we will notify our clinic clients and, where appropriate, other users: for example, by posting a prominent notice on our website or sending an email notification to our clients. The “Last Updated” date at the top of this Policy will be revised to the effective date of the changes.

If changes materially affect the way we handle personal data (for instance, if we expand the types of data we collect or introduce new third-party integrations that affect your data), we will endeavor to inform affected individuals in advance and obtain consent if required. Minor changes (such as clarifications or improvements in wording) will be posted with the updated Policy available on our website.

Your continued use of Pearwell’s services after the Privacy Policy changes will be deemed acceptance of those changes, to the extent permitted by law. However, if any change requires your consent under PDPA or other laws, we will ensure to obtain that consent.

We maintain previous versions of this Privacy Policy for reference, and we can provide them upon request to demonstrate our compliance history.

Sources: This Privacy Policy was informed by compliance requirements under Thailand’s Personal Data Protection Act and industry best practices. Key legal guidelines, such as the need to provide clear notice of data collection purposes and individual rights, have been incorporated [1] [8]. We have taken into account the PDPA’s provisions on sensitive health data (which require explicit consent) [4], security measures [9],

and cross-border data safeguards [7], among others. Pearwell's commitment to privacy reflects these standards and the principle that individuals have the right to control their personal data [2].

---

[1] [3] [13] [14] [15] Thailand's Personal Data Protection Act (PDPA) - TermsFeed
https://www.termsfeed.com/blog/thailand-pdpa-personal-data-protection-act/

[2] [6] [11] Data protection laws in Thailand - Data Protection Laws of the World
https://www.dlapiperdataprotection.com/index.html?t=law&c=TH

[4] [5] [7] [8] [9] [10] [12] At a glance: data protection and management of health data in Thailand - Lexology
https://www.lexology.com/library/detail.aspx?g=2b4f2c78-7f9d-4d35-899f-f6f1c6fa13df