# TUNASYS

## Privacy Policy

Governing the Collection, Use, and Protection of Personal Data
Across Tuno and Related Tunasys Services

Effective Date: April 19, 2026
Last Updated: April 19, 2026
Version 2.0

## Table of Contents

## 1. Introduction

TUNASYS COMPANY LIMITED, a company limited incorporated under the laws of Thailand with Business Registration Number 0105569064159 and head office at 1 Empire Tower, 47th Floor, Unit 4703, Sathon Tai Road, Yan Nawa, Sathon, Bangkok, Thailand ("we", "us", "our", or "Tunasys"), is committed to protecting the privacy and
personal data of our customers, their end users, and all individuals who interact with our products and services. This Privacy Policy ("Policy") explains how we collect, use, disclose, store, and protect your personal data when you access or use our services, including Tuno and all related software platforms, websites, APIs, mobile applications, and documentation (collectively, the "Services"). Tuno is a product of Tunasys.

Tunasys is incorporated in Thailand and may provide the Services in Thailand and such other jurisdictions as Tunasys may expand into from time to time. This Policy is designed to comply with the Personal Data Protection Act B.E. 2562 (2019) of Thailand ("Thailand PDPA") and any other applicable data protection laws in jurisdictions where we operate.

By accessing or using our Services, you acknowledge that you have read, understood, and agree to the practices described in this Policy. If you are using the Services on behalf of an organization, you represent that you are authorized to agree to this Policy on behalf of that organization.

This Policy should be read in conjunction with our Terms of Service, which governs your use of the Services. In the event of a conflict between this Policy and the Terms of Service regarding data protection matters, this Policy shall prevail. This Policy is governed by and construed in accordance with the laws of Thailand.

## 2. Definitions

**"Customer"** means the business entity (such as a clinic, franchise, or healthcare provider) that has subscribed to or registered for the Services.

**"Customer Data"** means all data uploaded, submitted, or generated by the Customer or its Authorized Users through the Services, including patient records, appointment data, transaction records, consent forms, and any other information processed through the platform.

"Data Controller" means the entity that determines the purposes and means of processing personal data under the Thailand PDPA. Depending on the context, this may be Tunasys or the Customer.
"Data Processor" means the entity that processes personal data on behalf of the Data Controller under the Thailand PDPA. When Tunasys processes Customer Data on behalf of a Customer and in accordance with the Customer's instructions, Tunasys acts as a Data Processor. Where Tunasys independently determines the purposes and essential means of processing, Tunasys acts as a Data Controller. Hosting, maintaining, securing, backing up, monitoring, or administering Supabase, application databases, storage systems, servers, logs, or support tools does not by itself determine controller status; the applicable role depends on who determines the purposes and essential means of the relevant processing.

**"Data Subject"** means any identified or identifiable natural person whose personal data is processed through the Services.

**"End User"** means the patients, clients, or consumers of the Customer whose personal data may be processed through the Services.

**"Personal Data"** means any information relating to an identified or identifiable natural person, directly or indirectly, including but not limited to names, identification numbers, location data, online identifiers, and factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.

**"Sensitive Personal Data"** means personal data that requires heightened protection under applicable law, including but not limited to health data, biometric data, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, sexual orientation, criminal records, and disability information.

"OPDPC" means the Office of the Personal Data Protection Committee of Thailand, the supervisory authority for the Thailand PDPA.

## 3. Information We Collect

### 3.1 Account and Identity Information

Information you provide when registering for or using the Services, including business name, contact person name, email address, phone number, job title, business address, and login credentials.

### 3.2 Financial and Billing Information

Payment details, billing addresses, bank account information, tax identification numbers, VAT/GST registration details, transaction histories, and invoice records required for subscription management and payment processing.

### 3.3 Customer Data (Processed on Behalf of Customers)

When Customers use the Services, they may input data about their own clients and patients. This may include patient names, contact details, medical or treatment records, appointment histories, consent forms, photographs (before/after treatment images), health-related information, and other data relevant to the Customer's operations. With respect to this Customer Data, the Customer generally acts as the Data Controller and Tunasys generally acts as the Data Processor where Tunasys processes such data on the Customer's instructions and in accordance with our Terms of Service and any applicable Data Processing Agreement. Tunasys may act as Data Controller for processing activities for which Tunasys independently determines the purposes and essential means, including account administration, billing, security, service analytics, legal compliance, abuse prevention, and product improvement.

### 3.4 Technical and Usage Information

Information collected automatically when you interact with the Services, including IP addresses, browser type and version, device identifiers, operating system, screen resolution, language settings, time zone, access times, pages viewed, features used, clickstream data, error logs, and referring/exit pages.

### 3.5 Communication Records

Records of communications between you and TunaSys, including support tickets, chat transcripts, emails, phone call records (if recorded with notice), survey responses, feedback, and training session interactions.

### 3.6 Location Information

Approximate geographic location derived from IP address, and where provided by the Customer, the physical address of clinic or business locations for use in features such as clinic finder functionality.

### 3.7 Sensitive Personal Data

In general, TunaSys does not directly collect Sensitive Personal Data. However, Customers may input health-related data or other sensitive information into the Services in the course of managing their clinic operations. Where TunaSys processes Sensitive Personal Data as a Data Processor on behalf of a Customer, TunaSys will:

- Process Sensitive Personal Data only on the documented, written instructions of the Customer and for no other purpose;
- Implement technical and organizational measures appropriate to the heightened risk associated with Sensitive Personal Data, including encryption at rest and in transit, strict role-based access controls, and comprehensive audit logging;
- Promptly notify the Customer if TunaSys believes any instruction infringes applicable data protection law;
- Ensure that any personnel or sub-processors authorized to process Sensitive Personal Data are bound by appropriate confidentiality obligations.

The Customer, as Data Controller, remains responsible for ensuring that it has a lawful basis for collecting and processing Sensitive Personal Data and that all necessary consents or other legal grounds have been established prior to inputting such data into the Services.

## 4. How We Collect Information

### 4.1 Directly from You

When you register for an account, subscribe to the Services, fill out forms, contact our support or sales teams, participate in demos or training sessions, or otherwise provide information to us.

### 4.2 Automatically Through the Services

Through cookies, server logs, analytics tools, and similar technologies when you use or interact with the Services. See Section 12 for more details on cookies and tracking technologies.

### 4.3 From Third Parties

From payment processors, business partners, referral programs, publicly available sources, and third-party platforms you connect to the Services (such as accounting software integrations or payment gateway providers).

### 4.4 From Customers (as Data Processor)

Customer Data is provided to TunaSys by the Customer through the normal use of the Services. TunaSys does not independently collect this data but processes it on behalf of and under the instructions of the Customer.

## 5. Legal Bases for Processing

We process personal data only when we have a lawful basis to do so under applicable data protection law. The applicable legal bases vary by jurisdiction as follows:

### 5.1 Contractual Necessity

Processing is necessary for the performance of a contract to which you are a party, or to take steps at your request prior to entering into a contract. This includes providing the Services, managing subscriptions, processing payments, delivering support, and onboarding new Customers.

### 5.2 Consent

Where we rely on your consent, we will obtain it in a manner that is clear, specific, informed, and freely given. You have the right to withdraw consent at any time, though withdrawal will not affect the lawfulness of processing carried out prior to withdrawal. We rely on consent for activities such as sending marketing communications, processing Sensitive Personal Data where applicable, and enabling optional analytics or personalization features.

### 5.3 Legitimate Interests

Processing is necessary for our legitimate business interests or those of a third party, provided that such interests are not overridden by your rights and freedoms. Our legitimate interests include improving and securing the Services, fraud prevention, internal analytics, and enforcing our Terms of Service, subject to applicable law.

### 5.4 Legal Obligation

Processing is necessary for compliance with a legal obligation to which Tunasys is subject, including tax and accounting requirements, regulatory reporting, responding to lawful requests from public authorities, and compliance with applicable data protection laws in Thailand and any other applicable jurisdiction.

### 5.5 Vital Interests

In rare circumstances, processing may be necessary to protect the vital interests of a Data Subject or another person.

### 5.6 Public Interest

Processing may be necessary for the performance of a task carried out in the public interest or in the exercise of official authority, where applicable.

5.7 Business Improvement and Service Analytics

Where permitted by applicable law, Tunasys may use personal data for developing or improving our products and services, provided such use is necessary, proportionate, subject to appropriate safeguards, and does not unlawfully override the rights and freedoms of Data Subjects.

## 6. How We Use Your Information

### 6.1 Providing and Operating the Services

To create and manage your account, provide the subscribed features, process transactions, deliver customer support, conduct onboarding and training, and maintain the overall functionality and performance of the Services. Where Customers operate clinics in Thailand, health and treatment data is processed under Sections 24(5) and 26 of the Thailand PDPA as necessary for medical care and treatment. Where a clinic operates multiple branches under the same legal entity, authorised staff across all branches may access a patient's records for the purpose of providing continuous care. This access is limited to staff with a legitimate clinical or administrative need and does not constitute sharing with a third party.

### 6.2 Billing and Payment Processing

To process subscription fees, generate invoices, manage billing records, facilitate refunds, reconcile payments, and comply with tax obligations in Thailand and any other applicable jurisdiction.

### 6.3 Communication

To send you service-related notices, updates, security alerts, and administrative messages. With your consent, we may also send marketing and promotional communications about our products and services. All marketing communications include an unsubscribe mechanism as required by applicable law.

### 6.4 Improvement and Development

To analyze usage patterns, conduct research, identify trends, improve the user experience, develop new features, troubleshoot issues, and optimize the performance and security of the Services.

### 6.5 Security and Fraud Prevention

To detect, investigate, and prevent fraudulent, unauthorized, or illegal activity, and to protect the rights, property, and safety of TunaSys, our Customers, and the public.

### 6.6 Compliance and Legal Obligations

To comply with applicable laws, regulations, and governmental orders, including the Thailand PDPA, OCPB regulations, Thai tax and accounting laws, and other regulatory requirements in the jurisdictions in which we operate.

### 6.7 Regulatory Compliance Assistance

To facilitate Customers' compliance with applicable regulations through features such as consent management, digital signature capture, audit trail generation, and data retention management. The Customer remains solely responsible for its own regulatory compliance.

### 6.8 Aggregated and Anonymized Analysis

To produce aggregated, anonymized, or de-identified data that does not identify any individual, for purposes including benchmarking, product improvement, industry analysis, and research. Such data is not considered personal data under applicable law.

## 7. How We Share Your Information

We do not sell personal data to third parties. We may share personal data in the following circumstances:

### 7.1 Service Providers and Sub-Processors

We engage trusted third-party service providers to assist in operating the Services, including cloud hosting providers, payment processors, email delivery services, analytics providers, customer support tools, and security services. These providers are contractually obligated to process personal data only on our instructions and in accordance with applicable data protection law. See Section 19 for our sub-processor disclosure policy.

### 7.2 Business Partners

We may share data with business partners who provide complementary services, such as hardware vendors, software integrations, or consulting services, but only to the extent necessary to deliver the Services and with appropriate contractual safeguards in place.

### 7.3 Legal and Regulatory Requirements

We may disclose personal data if required to do so by law, regulation, legal process, or governmental request, including requests from the OPDPC in Thailand, tax authorities, law enforcement agencies, or courts of competent jurisdiction.

### 7.4 Protection of Rights

We may disclose personal data where we reasonably believe it is necessary to detect, prevent, or address fraud, security issues, or technical problems, or to protect the rights, property, or safety of TunaSys, our Customers, or the public.

### 7.5 Business Transfers

In the event of a merger, acquisition, reorganization, bankruptcy, or sale of all or substantially all of TUNASYS COMPANY LIMITED's assets, personal data may be transferred as part of such transaction. We will notify affected parties of any such transfer and any changes to applicable privacy practices.

### 7.6 With Consent

We may share personal data with third parties when you have given your explicit consent to such sharing.

### 7.7 Aggregated and Anonymized Data

We may share aggregated, anonymized, or de-identified data with third parties for research, industry analysis, or other purposes. Such data cannot be used to identify any individual.

## 8. International Data Transfers

As a Thailand-incorporated company, Tunasys may transfer personal data between Thailand and countries in which our sub-processors operate. All international transfers are conducted in accordance with applicable law.

8.1 Transfers from Thailand

For transfers of personal data originating from Thailand, Tunasys complies with Sections 28 and 29 of the Thailand PDPA and any supplementary guidance or notifications issued by the OPDPC. We will not transfer personal data from Thailand unless the destination country has adequate data protection standards as determined by the OPDPC, or we have implemented appropriate safeguards, including Standard Contractual Clauses in a form consistent with OPDPC guidance where applicable.

8.2 General Safeguards

Across all jurisdictions, TunaSys relies on one or more of the following mechanisms for international transfers:

- Adequacy determination by the relevant supervisory authority;
? Contractual protections (Standard Contractual Clauses or equivalent);
- Binding Corporate Rules where applicable;
- Explicit informed consent of the Data Subject, where no other mechanism is available.

## 9. Data Retention

We retain personal data only for as long as necessary to fulfill the purposes for which it was collected, including to satisfy legal, accounting, or regulatory requirements under Thai law and any other applicable law. When determining retention periods, we consider the nature and sensitivity of the data, the potential risk of harm from unauthorized use or disclosure, the purposes for which we process the data, and applicable legal requirements.

### 9.1 Account Data

Account information is retained for the duration of your subscription and for a period of five (5) years following termination or expiration, or longer if required by applicable statute of limitations or regulatory requirements.

### 9.2 Customer Data

Customer Data is retained for the duration of the Customer's subscription. Upon termination, TunaSys will make Customer Data available for export for thirty (30) days, after which it may be securely deleted in accordance with our data deletion procedures, unless retention is required by applicable law.

### 9.3 Financial Records

Financial and billing records are retained for a minimum of five (5) years, or longer as required by Thai tax, accounting, company record, or equivalent laws in the applicable jurisdiction.

### 9.4 Audit Logs

System audit logs, including access logs, consent records, and compliance-related logs, are retained for a minimum of three (3) years or as required by applicable regulatory requirements, including requirements under the Thailand PDPA and any applicable OCPB regulations.

### 9.5 Communication Records

Support tickets, correspondence, and feedback are retained for up to three (3) years following resolution or last activity, after which they are securely deleted or anonymized.

### 9.6 Anonymized Data

Data that has been fully anonymized such that it no longer constitutes personal data may be retained indefinitely for research, analytics, and improvement purposes.

## 10. Data Security

Tunasys implements appropriate technical and organizational measures to protect personal data against unauthorized or unlawful processing, accidental loss, destruction, alteration, or damage, in accordance with the Thailand PDPA and any equivalent obligations under applicable law. Our security measures include, but are not limited to:

- Encryption of data in transit using TLS/SSL protocols and encryption of data at rest using industry-standard algorithms
- Role-based access controls ensuring that personal data is accessible only to authorized personnel on a need-to-know basis
- Comprehensive audit logging that records all access to and modifications of personal data, creating tamper-evident records
- Regular security assessments, vulnerability testing, and code reviews
- Secure software development practices, including input validation, parameterized queries, and protection against common vulnerabilities
- Incident response procedures for detecting, reporting, and responding to data breaches in a timely manner
- Regular backups of Customer Data with secure storage
- Employee and contractor training on data protection and information security best practices

While we implement robust security measures, no method of electronic transmission or storage is completely secure. We cannot guarantee absolute security, but we commit to promptly addressing any security incidents in accordance with applicable breach notification requirements.

### 10.1 Breach Notification

In the event of a personal data breach, Tunasys will act in accordance with applicable breach notification obligations. Where required under the Thailand PDPA, we will notify the OPDPC within seventy-two (72) hours of becoming aware of a qualifying breach, and will notify affected Data Subjects without undue delay where the breach is likely to result in high risk to their rights and freedoms. For Customers affected by a breach of Customer Data, we will notify the Customer promptly so that the Customer can fulfill its own notification obligations as Data Controller.

## 11. Your Rights as a Data Subject

Under applicable data protection laws, including the Thailand PDPA, you may have the following rights with respect to your personal data. The availability of these rights may vary depending on the applicable jurisdiction and the legal basis for processing:

### 11.1 Right of Access

You have the right to request confirmation as to whether we process your personal data and, if so, to obtain access to such data and information about how it is processed.

### 11.2 Right to Rectification / Correction

You have the right to request that we correct any inaccurate personal data and complete any incomplete personal data concerning you, subject to applicable law.

### 11.3 Right to Erasure / Withdrawal

You have the right to request the deletion or destruction of your personal data, or the anonymization thereof, where the data is no longer necessary for the purposes for which it was collected, where you withdraw consent (and no other legal basis applies), or where processing is unlawful. This right is subject to legal retention obligations and other applicable exceptions.

### 11.4 Right to Restrict Processing

You have the right to request that we restrict or suspend the processing of your personal data in certain circumstances, such as where you contest the accuracy of the data or where processing is unlawful but you do not want the data deleted.

### 11.5 Right to Data Portability

You have the right to receive your personal data in a structured, commonly used, and machine-readable format, and to transmit such data to another controller, where technically feasible and required by applicable law.

### 11.6 Right to Object

You have the right to object to the processing of your personal data where processing is based on legitimate interests or is for direct marketing purposes. Upon objection, we will cease processing unless we demonstrate compelling legitimate grounds that override your interests, rights, and freedoms.

### 11.7 Right to Withdraw Consent

Where processing is based on your consent, you have the right to withdraw consent at any time. Withdrawal of consent does not affect the lawfulness of processing carried out prior to the withdrawal. See Appendix A for details on how to withdraw consent.

### 11.8 Right to Lodge a Complaint

You have the right to lodge a complaint with the competent supervisory authority in your jurisdiction, including the OPDPC in Thailand, if you believe that the processing of your personal data violates applicable data protection law.

### 11.9 Exercising Your Rights

To exercise any of the above rights, please contact us using the details provided in Section 16. We will respond to your request within thirty (30) days (or such shorter period as required by applicable law). We may require you to verify your identity before processing your request. If we are unable to fulfill your request, we will provide you with an explanation of the reasons.

### 11.10 Rights of End Users

If you are an End User whose personal data is processed through the Services by a Customer, please note that the Customer is the Data Controller for your data. You should direct any requests to exercise your data subject rights to the relevant Customer in the first instance. TunaSys will assist the Customer in responding to such requests in accordance with our contractual obligations.

## 12. Cookies and Tracking Technologies

Our websites and applications may use cookies and similar tracking technologies (such as pixels, beacons, and local storage) to enhance functionality, analyze usage, and improve the user experience.

### 12.1 Types of Cookies

- Strictly Necessary Cookies: Essential for the operation of the Services, such as session management and authentication. These cannot be disabled.
- Functional Cookies: Remember your preferences and settings to enhance your experience.
- Analytics Cookies: Help us understand how visitors interact with our Services, enabling us to improve functionality and content.
- Marketing Cookies: Used to deliver relevant advertisements and measure the effectiveness of marketing campaigns (used only with your consent).

### 12.2 Cookie Management

You can manage your cookie preferences through your browser settings or through any cookie consent mechanism we make available on our website. Disabling certain cookies may affect the functionality of the Services.

## 13. Third-Party Services and Infrastructure

The Services rely on third-party infrastructure and service providers, including cloud hosting platforms, database services, payment processors, email services, and analytics tools. While we carefully select and contractually bind our service providers to appropriate data protection obligations, we cannot be held liable for outages, data incidents, or service disruptions caused by third-party infrastructure providers that are beyond our reasonable control.

A current list of our material sub-processors is maintained and published in accordance with Section 19. The Services may contain links to third-party websites or integrate with third-party applications. This Policy does not apply to any third-party services. We encourage you to review the privacy policies of any third-party services you access through our platform.

## 14. Children's Privacy

The Services are designed for use by businesses and are not directed at children or minors.

14.1 Thailand
Under the Thailand PDPA and the Civil and Commercial Code of Thailand, a minor is a person who has not yet reached twenty (20) years of age and has not been legally emancipated. Tunasys will not knowingly process personal data of minors under 20 without the consent of a parent or legal guardian, except where processing is permitted under Section 24 of the Thailand PDPA without consent, including where necessary for direct medical treatment of the minor. Customers who input data about patients under 20 in Thailand are responsible for ensuring that parental or guardian consent has been obtained where required.

14.2 General
If Tunasys becomes aware that it has inadvertently processed personal data of a minor without appropriate consent, it will take prompt steps to delete or anonymize such data. The age threshold applicable to any particular processing activity will be determined by the law of the jurisdiction in which the Data Subject is located.

## 15. Changes to This Privacy Policy

We may update this Policy from time to time to reflect changes in our practices, the Services, or applicable law. When we make material changes, we will provide notice through the Services, by email, or through other appropriate means at least thirty (30) days before the changes take effect. The "Last Updated" date at the top of this Policy indicates when the most recent revision was made.

Your continued use of the Services after any changes to this Policy constitutes your acceptance of the updated Policy. If you do not agree to any changes, you should discontinue use of the Services and contact us to request deletion of your personal data.

## 16. Contact Information

If you have any questions, concerns, or requests regarding this Policy or our data protection practices, or if you wish to exercise any of your rights as a Data Subject, please contact us at:

TUNASYS COMPANY LIMITED
Business Registration Number: 0105569064159
Head Office: 1 Empire Tower, 47th Floor, Unit 4703, Sathon Tai Road, Yan Nawa, Sathon, Bangkok, Thailand
Data Protection Contact: Harvey Liu, Director
Email: harvey@tunasys.com
Website: https://tunasys.com

We will endeavor to respond to all legitimate requests within thirty (30) days. In complex cases, we may extend this period by an additional thirty (30) days, in which case we will inform you of the extension and the reasons for the delay.

## 17. Jurisdiction-Specific Provisions

17.1 Thailand (Personal Data Protection Act B.E. 2562)
For Data Subjects in Thailand, this Policy is issued in compliance with the Thailand PDPA. In addition to the rights described in Section 11, Data Subjects in Thailand may exercise the right to request disclosure of how personal data was acquired without their consent (Section 30 of the Thailand PDPA). Consent obtained under the Thailand PDPA will be presented in a manner that is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language. We will not make the provision of the Services conditional on consent to processing that is not necessary for the performance of the contract. Sensitive Personal Data as defined under Section 26 of the Thailand PDPA will only be collected with explicit consent or where another lawful basis under the Thailand PDPA applies. Cross-border transfers of personal data from Thailand will comply with Sections 28 and 29 of the Thailand PDPA.

17.2 Other Jurisdictions

As Tunasys expands to additional markets, jurisdiction-specific provisions will be added to this Policy to ensure compliance with local data protection requirements. If you are located in a jurisdiction not specifically addressed above, the general terms of this Policy apply.

## 18. Data Protection Contact

### 18.1 Designation

Tunasys has designated Harvey Liu, Director, as its Data Protection Contact for privacy and data protection matters. Tunasys will evaluate whether a dedicated independent Data Protection Officer appointment is required under any applicable jurisdiction as the volume and sensitivity of personal data processed through the Services increases.

### 18.2 Responsibilities

The Data Protection Contact is responsible for:
- Informing and advising Tunasys and its personnel of their obligations under applicable data protection laws, including the Thailand PDPA;
- Monitoring compliance with data protection laws and Tunasys internal data protection policies and procedures;
- Providing advice on data protection impact assessments and monitoring their performance;
- Acting as the primary point of contact for the OPDPC on matters relating to personal data processing;
- Acting as the point of contact for Data Subjects seeking to exercise their rights under this Policy.

### 18.3 Contact

Data Subjects and supervisory authorities may contact the Data Protection Contact directly at: harvey@tunasys.com. All communications are handled in accordance with applicable data protection and confidentiality obligations.

## 19. Sub-Processor Transparency

TUNASYS COMPANY LIMITED engages the following categories of sub-processors to assist in delivering the Services. All sub-processors are bound by data processing agreements that require them to protect personal data to standards at least equivalent to those set out in this Policy and applicable law.

| Category | Function | Data Types Processed | Location |
|---|---|---|---|
| Cloud Database & Hosting | Database, storage, authentication | All Customer Data, account data | Global (EU/US) |
| Payment Processing | Subscription billing, invoicing | Financial & billing information | Regional |
| Email Delivery | Transactional and system emails | Email addresses, notification content | Global |
| Analytics | Usage analytics, performance monitoring | Technical & usage data (anonymized) | Global |
| Customer Support | Support ticketing and communications | Communication records | Regional |
| Security & Monitoring | Threat detection, uptime monitoring | Technical logs, access data | Global |

A current list of named sub-processors (including entity names, registered addresses, and applicable data transfer mechanisms) is published at https://tunasys.com/legal/sub-processors and is updated within thirty (30) days of any material change. Customers will be notified of any addition or replacement of a sub-processor that processes Customer Data, and will have the right to object to such changes in accordance with their Data Processing Agreement with TunaSys.

## Appendix A: Consent Withdrawal Procedure

Where TunaSys or a Customer relies on your consent as the lawful basis for processing your personal data, you have the right to withdraw that consent at any time. Withdrawal of consent does not affect the lawfulness of any processing carried out before the withdrawal. This Appendix describes how consent withdrawal works in practice.

### A.1 Who Can Withdraw Consent

Any Data Subject whose personal data is processed on the basis of consent — whether as a TunaSys customer, end user, or patient of a clinic using TunaSys — may withdraw consent. For minors, the parent or legal guardian who granted consent may withdraw it on the minor's behalf.

### A.2 How to Withdraw Consent

Consent may be withdrawn through any of the following mechanisms:

- In-platform: End users (patients) may withdraw consent directly via the patient-facing portal or consent management screen within TunaSys, where available. Withdrawal takes effect immediately upon confirmation.
- Via the clinic: End users may request consent withdrawal from the clinic that collected their data. As Data Controller, the clinic is responsible for processing the withdrawal and instructing TunaSys accordingly.

- Direct request to Tunasys: For data processed directly by Tunasys (e.g., account data, marketing communications), withdrawal requests may be submitted to harvey@tunasys.com or via the unsubscribe mechanism in any marketing email.

- Written request: A written withdrawal request may be submitted to TUNASYS COMPANY LIMITED at the contact details in Section 16.

### A.3 Effect of Withdrawal

Upon receipt of a valid withdrawal request, TunaSys or the relevant Customer (as applicable) will cease processing based on consent within a reasonable time, not to exceed thirty (30) days. Note that:

- Withdrawal of consent for treatment-related data processing does not prevent the clinic from processing data on alternative lawful grounds (e.g., Section 24(5) Thailand PDPA — necessity for medical treatment);
- Withdrawal of consent for branch profile sharing will result in your patient profile no longer being accessible to other branches in the clinic network, taking effect at the next system sync, not to exceed 24 hours;

- Withdrawal does not require deletion of data where Tunasys or the Customer has another lawful basis for retention (e.g., legal obligation, contractual necessity, or applicable retention requirement).

### A.4 Record of Withdrawal

TunaSys maintains an audit log of all consent grants and withdrawals, timestamped and tamper-evident, in accordance with Section 9.4 of this Policy. Customers may access consent records for their own patients via the TunaSys platform.