Privacy Notice

Organization Name	Document Name	Document owner
AIRS Medical	Privacy Notice	Yunmyeong Kim, CPO
Effective Date	**Version**	**Document approvers**
September 1, 2023.	1.1	Hyeseong Lee, CEO Jingu Lee, CEO

To protect the freedom and rights of information subjects providing its products and services including SwiftMR, AIRS Medical(hereinafter referred to as the "Organization") legally processes and safely manages personal information in accordance with the Personal Information Protection Act, the Health Insurance Portability and Accountability Act, the General Data Protection Regulation, and related laws and regulations. In accordance with Article 30 of the Personal Information Protection Act, the following privacy notice is established and disclosed in order to guide information subjects of the procedures and standards for processing personal information and to promptly and smoothly handle grievances related thereto.

Key labels for privacy notices

For more information, please check the privacy notice below.

				
Collection of general personal information	Purpose of processing personal information	Retention period of personal information	Consignment of processing	Grievance Department

AIRS MEDICAL

Table of Contents

1. Purpose, item collected, and retention period of processing personal information, items collected, and period of retention and use
2. Consignment of Personal Data Processing
3. Destruction of Personal Information and Procedures
4. Measures to Destroy Personal Information of Unused Users
5. Rights and Obligations of Information Subjects and Legal Representatives and Method of Exercising
6. Measures to ensure the safety of personal information
7. Installation, operation, and rejection of automatic personal information collection devices
8. Collection, Use, and Rejection of Behavioral Information
9. Handling pseudonymized information
10. Privacy Officers and Personal Information Access Requests
11. Violation Remedies

1. Purpose, items collected, and retention period of processing personal information

1.1. The items, purpose, and retention period of the personal information processed by the organization are as follows.

Category	Purpose	Items collected	Retention period
Managing requests for free trial	Providing answers to free trial requests Providing free trial of products and services Managing history of free trial requests	Required: Name, Email, Phone number, Institution, Job title, Country, Address	3 years from the date of submission
Managing inquiries from Contact Us	Providing answers to inquiries Managing history of inquiries	Required: Name, Email, Country, Facility/Company name, Job title Optional: Phone number, City	3 years from the date of submission
Managing attendees list of product presentation	Writing physician financial transparency reports	Required: Name, Job title, Specialty	Until withdrawal of consent
(PC browser access)	Building a service experience that users can feel confident about in terms of	Required: Device information, IP address, Operating system, accessed	3 months from date of access

Information automatically collected while using Internet services	security, privacy and safety	browser information, service usage history	
(Mobile access) Information automatically collected while using Internet services	Building a service experience that users can feel confident about in terms of security, privacy and safety	Required: Mobile device information, mobile device IP address, mobile operating system, accessed mobile browser information, service usage history	3 months from date of access
Managing job application, recruiting, and government grants	Guidance on the hiring process Handling complaints and notification of outcomes for employment-related inquiries	Required: Name, Contact, Email Optional: Education, Work Experience	(Employee) 1 year from date of departure (Unhired) 1 month from completion of hiring process
Offering products and services	Analyzing service usage history and access frequency Statistics about service usage Maintenance of products and service	Required: Email, MRI image (automatically de-identified as soon as uploaded to a webpage or cloud server)	1 year from the date of termination
Improving products and services	Conducting studies on MRI acceleration and image quality improvement	Required: Patient number, Name, Date of birth, Date of examination, MRI image Optional: Height, weight, Past medical histories	Until the purpose is accomplished 3 years from end date of study
Improving products and services	Developing algorithms for detecting anatomical structures on ultrasound	Required: Patient number, Name, Date of birth, Date of examination, Ultrasound image Optional: Height, Weight, Past medical histories	Until the purpose is accomplished 3 years from end date of study

1.2. The personal information processed will not be used for any purpose other than the above, and if the purpose of processing changes, the organization will take necessary measures such as obtaining separate consent in accordance with Article 18 of the Personal Information Protection Act.

1.3. The organization shall process and retain personal information within the period of retention and use of personal information in accordance with the laws and regulations or the period of retention and use of personal information agreed upon when collecting personal information

from the information subject. However, in the case of the following reasons, the organization shall process and retain personal information until the end of the relevant reasons.

1.3.1. If there is an ongoing investigation or inquiry into a violation of applicable laws or regulations, until the investigation or inquiry is concluded.

1.3.2. If a debt or liability remains due to the use of the products and services, until the debt or liability relationship is settled.

1.3.3. If there is a mandatory retention period under applicable law, until the end of that period.

- Telecommunications Secrecy Act: Telecommunications verification data such as website visit history (3 months)
- Electronic Commerce Act: Records on contract or subscription withdrawal (5 years)
- E-commerce Act: Records on payment and supply of goods (5 years)
- E-commerce Act: Records on handling of consumer complaints or disputes (3 years)
- E-Commerce Act: Records on display and advertising (6 months)
- Information and Communications Network Act: Records on identity verification (6 months)
- Location Information Protection Act: Records on personal location information (6 months)

2. Consignment of Personal Data Processing

2.1. The organization entrusts the processing of personal information as follows for the smooth processing of personal information.

Consignee	**Consignment work**
Imweb Inc.	Developing and operating the website
INNO Consulting Inc.	Applying for employment-related grants and response to inspections
Medical Standard Co., Ltd.	Providing product-related information and experiences
Flex Inc.	Managing human resources information
Hunet Inc.	Law court essential training and job Training
Daou Technology Inc.	Sending KakaoTalk notifications
Salesforce, Inc.	Managing customer information

Automattic, Inc.	Developing and operating the website
Gusto, Inc.	Managing human resources information

2.2. The organization entrusts the processing of personal information overseas as follows.

Consignee	**Location (country)**	**Location (address)**	**Date and Method**	**Items**	**Retention period**	**Contact for the administrator**
Salesforce, Inc.	USA	Salesforce Tower, 415 Mission Street, 3rd Floor, San Francisco, CA 94105, United States	Send over the network when forming customer relations	Name, Email, Phone number, Affiliation, Job title	Until the end of the consignment agreement	privacy@salesforce.com
Automattic, Inc.	USA	60 29th Street #343 San Francisco, CA 94110	Send over network when submitting information on the website	Name, Email, Phone number, Affiliation, Job title, Country, Address	Until the end of the consignment agreement	privacypolicyupdates@automattic.com
Gusto, Inc.	USA	525 20th Street San Francisco, CA 94107	Sent over the network when joining the company	Name, Contact, Address, Education, Salary	Until the end of the consignment agreement	privacy@gusto.com

2.3. When concluding a consignment contract, the organization specifies the prohibition of processing personal information other than for the purpose of performing entrusted tasks, technical and administrative protection measures, restrictions on re-consignment, management and supervision of the trustee, and responsibilities such as compensation for damages in documents such as contracts in accordance with Article 26 of the Personal Information Protection Act, and supervises whether the trustee processes personal information safely .

2.4. If the contents of the consignment work or the trustee change, we will disclose it through this privacy notice without delay.

3. Destruction of Personal Information and Procedures

3.1. The Organization shall destroy personal information without delay when it becomes unnecessary, such as the expiration of the personal information retention period or the achievement of the purpose of processing.

3.2. If the personal information retention period agreed to by the information subject has expired or the purpose of processing has been achieved, but the personal information must still be retained in accordance with other laws and regulations, the personal information shall be transferred to a separate database (DB) or preserved in a different storage location.

3.3. The process and methods for destroying personal information are as follows

- Destruction Procedure: Select the personal information for which the reason for destruction has occurred and destroy the personal information with the approval of the person in charge of personal information protection.
- Destruction method: Personal information recorded and stored in the form of electronic files is destroyed so that the records cannot be reproduced, and personal information recorded and stored in paper documents is destroyed by shredding or incineration.

4. Measures to Destroy Personal Information of Unused Users

4.1. The organization converts users who have not used the service for one year into dormant accounts and keeps their personal information separately. The separated personal information is stored for one year and then destroyed without delay.

4.2. At least 30 days prior to the dormancy transition, the organization will notify prospective members of the dormancy, the date of the transition, and the items of personal information that will be kept in segregated storage in a manner that is notifiable to the user, such as by email or text.

4.3. If you do not wish to be converted to a dormant account, you can sign in to the service prior to being converted to a dormant account. If you sign in even though you have been converted to a dormant account, the organization will restore your dormant account and allow you to use the service as normal, subject to your consent.

5. Rights and Obligations of Information Subjects and Legal Representatives and Method of Exercising

5.1. The information subject can exercise the right to view, correct, delete, or request suspension of processing of personal information at any time against the organization.

5.2. The exercise of rights pursuant to Paragraph 1 can be made in writing, by e-mail, or by facsimile transmission (FAX) in accordance with Article 41, Paragraph 1 of the Enforcement Decree of the Personal Information Protection Act, and the organization will take action without delay.

5.3. The exercise of rights pursuant to Paragraph 1 can be made through a representative, such as the legal representative of the information subject or a person authorized to do so. In this case, you must submit a power of attorney in the form of Attachment No. 11 to the "Notification on the Method of Processing Personal Information (No. 2020-7)".

5.4. The rights of the information subject to access personal information and request suspension of processing may be restricted under Article 35, Paragraph 4, and Article 37, Paragraph 2 of the Personal Information Protection Act.

5.5. A request for the correction or deletion of personal information cannot be made if the personal information is specified as the subject of collection under another law.

5.6. The Organization shall verify that the person making the request is the individual or a legitimate representative when requesting access, correction, deletion, or suspension of processing in accordance with the rights of the information subject.

6. Measures to ensure the safety of personal information

6.1. The organization takes the following measures to ensure the safety of personal information.

6.1.1. Administrative measures: establishing and implementing an internal management plan, operating a dedicated organization, and regularly training employees.

6.1.2. Technical measures: management of access rights to personal information processing systems, installation of access control systems, encryption of personal information, and installation and renewal of security programs

6.1.3. Physical measures: access control to computer labs, server rooms, data storage rooms, etc.

6.2. In order to ensure the safety of personal information, the Organization implements the following activities in addition to those stipulated by laws and regulations.

6.2.1. Obtain domestic and international privacy certifications

- HIPPA compliance (Thoropass)
- GDPR compliance(Thoropass)

7. Installation, operation, and rejection of automatic personal information collection devices

7.1. We use "cookies" for the following purposes. A cookie is a small amount of information sent to a user's computer browser or mobile application by the server (HTTP) used to operate a website and stored on the user's computer's internal hard disk or mobile device.

7.1.1. Purpose of use of cookies: to maintain user's preferences, maintain login status, provide service convenience features, improve services by analyzing user's service usage statistics, provide customized services, target marketing by analyzing interests, and understand the extent of participation in various events.

7.1.2. Disadvantages of refusing to save cookies: You may have difficulty using some services that require a login; You may be restricted from receiving rewards; You may have difficulty providing services and information optimized for you; You may have difficulty using customized services.

7.1.3. Installing, operating, and rejecting cookies: Depending on the type of browser or app, you can reject the storage of cookies in the following ways.

- If you're using Chrome, see how to set cookies
- If you use Microsoft Edge, see how to set cookies
- If you use Safari, see how to set cookies
- If you use the Safari app, see how to set cookies
- If you're using the Chrome app, see how to set cookies

- If you're using the Naver App, to set cookies: Settings > Browsing data > Clear cookies
- Android: Settings > Applications > Select a service > Storage > Clear cache
- iOS: Settings > Privacy > Tracking > Disable Service Apps

7.2. In order to provide users with a better experience, the Organization uses "web log analysis tools" that automatically collect and analyze information about your visit history and access method when you access the website/app. In some cases, the Organization outsources web log analysis to third parties, and information collected in the process may be transferred overseas. You can read more about this in the "Outsourcing of Personal Information Processing" section.

7.2.1. Purpose of using web log analysis tools: To improve the service through statistical analysis of users' use of the service, to provide customized services and benefits, and to provide customized advertisements.

7.2.2. Deny-Block Methods for Web Analytics Tools :

- [Google Analytics] view

7.2.3. Penalty for refusal: There is no penalty for using the service, but it may affect statistical analysis to improve the service.

8. Collection, Use, and Rejection of Behavioral Information

8.1. The organization do not collect, use, or provide behavioral information for online personalized advertising.

9. Processing of pseudonymized information

9.1. The organization pseudonymize personal information collected for statistical purposes, scientific research, public record keeping, etc. to make it unrecognizable to a specific individual and process it as follows.

Category	Processing Purpose	Item Collected	Retention Period

Category	Processing Purpose	Item Collected	Retention Period
Improving products and services	Conducting studies on MRI acceleration and image quality improvement	Patient number, Name, Date of birth, Date of examination, MRI image, Height, weight, Past medical histories	Until the purpose is accomplished or 3 years after the end of the IRB study
Improving products and services	Developing algorithms for detecting anatomical structures on ultrasound	Patient number, Name, Date of birth, Date of examination, Ultrasound image, Height, Weight, Past medical histories	Until the purpose is accomplished or 3 years after the end of the IRB study

9.2. In addition, in accordance with Article 28(4) of the Act (Obligation to take safety measures for pseudonymous information, etc.), the organization take administrative, technical, and physical protection measures necessary to ensure the safety of pseudonymous information, such as storing and managing pseudonymous information separately so that it cannot be re-identified, and creating and keeping records of the processing of pseudonymous information.

9.2.1. Administrative measures: establishment and implementation of internal management plans, regular employee training, etc.

9.2.2. Technical measures: management of access rights to personal information processing systems, installation of access control systems, encryption of unique identification information, and installation of security programs

9.2.3. Physical measures: Access control to computer labs, server rooms, data storage rooms, etc

10. Privacy officer and access to personal information requests

10.1. The organization designates a person in charge of personal information protection as follows to take overall responsibility for the processing of personal information, and to handle complaints and remedy damages from information subjects related to the processing of personal information.

10.2. The information subject may request access to personal information pursuant to Article 35 of the Personal Information Protection Act to the contact information below. The Organization will

endeavor to promptly process the information subject's request for access to personal information.

Category	Representative	Contact
Chief Privacy Officer	Title/Position: Chief Privacy Officer, Data Protection Officer Contact Name: Yunmyeong Kim	kim.theo@airsmed.com
Privacy Department	Department Name: Information Security	airsinfra@airsmed.com
Requesting access to personal information	Department Name: Information Security Representative Name: Deokgeun Nam	nam.deokgeun@airsmed.com

10.3. The information subject may contact the privacy officer and the department in charge for all personal information protection-related inquiries, complaints, damage relief, etc. that occurred while using the organization's products or services. The organization will respond to and handle inquiries from information subjects without delay.

11. Remedies for Infringement of Rights

11.1. The organization guarantees the right of the information subject to self-determine personal information, and strives to provide counseling and damage relief due to personal information infringement, and if you need to report or consult, please contact the department in charge.

11.2. The information subject may apply for dispute resolution or consultation to the Personal Information Dispute Mediation Committee or the Personal Information Infringement Report Center of the Korea Internet & Security Agency to obtain relief from personal information infringement. In addition, please contact the following organizations for reporting and counseling on other personal information infringements.

- Personal Information Dispute Mediation Committee: +82 1833-6972 (without area code) (www.kopico.go.kr)
- Personal Information Infringement Report Center : +82 118 (privacy.kisa.or.kr)

- Supreme Prosecutor's Office Republic of Korea: +82 1301 (www.spo.go.kr)
- Korean International Police Agency: +82 182 (ecrm.cyber.go.kr)

11.3. A person whose rights or interests have been infringed by a disposition or omission made by the head of a public institution in response to a request pursuant to the provisions of Articles 35 (Access to Personal Information), 36 (Correction and Deletion of Personal Information), and 37 (Suspension of Processing of Personal Information) of the Personal Information Protection Act may file an administrative appeal in accordance with the Administrative Appeals Act.

- Central Administrative Appeals Commission: +82 110 (www.simpan.go.kr)

12. Changes of the Privacy Notice

12.1. This privacy notice is effective from September 1, 2023.

12.2. Previous privacy notices can be found below.

- 2022.07.01~2023.08.31.
- 2022.04.22~2023.06.30.
- 2021.08.02~2022.04.21.

Announcement Date: August 25, 2023

Effective Date: September 1, 2023