Inception Date	02/22/2018
Approved Date	10/10/2025
Last Review Date	06/25/2026

PIMS Privacy Policy

1 Purpose

Strategic Objectives

- This Privacy Policy outlines AllOne Health's compliance with the ISO 27701 and SOC-2, Type 2 privacy frameworks regarding the collection, use, and retention of Personally Identifiable Information ("PII") and Protected Health Information ("PHI") that is processed by AllOne Health.
- Ensuring PII/PHI is protected, and privacy concerns are addressed.

2 Responsibilities

All employees of AllOne Health that have access to PII/PHI are responsible for conducting themselves in accordance with this policy. PII/PHI shall not be collected, used, or disclosed in a manner contrary to this policy without proper written permission from AllOne Health's legal department.

3 Scope and Audience

- AllOne Health Platform: The AllOne Health platform (the "platform") includes the software, hardware, communications capabilities, and other technology infrastructure supporting the functions.
- AllOne Health Data: AllOne Health Data ("data") includes customer and other data used, stored, accessed, and/or processed on the platform.
- Personally Identifiable Information (PII): Information that identifies or can be used to identify specific individuals, also referred to as PII in this document.
- Protected Health Information (PHI): Information that includes the personal health information of individuals, also referred to as PHI in this document.
- Company: Refers to AllOne Health and all its legal entities and subsidiaries.
- Data subject: An identifiable natural person who can be identified, directly or indirectly, by PII/PHI supplied to AllOne Health.
- Sensitive PII/PHI: Any PII/PHI regarding a Data Subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, physical or mental health, or sexual life.

- Data Protection Officer (DPO): Representative of the company responsible for ensuring that their organization processes the personal data of relevant data subjects) in compliance with this policy. The DPO is assigned in the Information Security and Privacy Policy.

4 POLICY

4.1 CONDITIONS FOR COLLECTION AND PROCESSING

4.1.1 Customer Agreement

- Customers agree to the terms of service provided when first accessing [application].
- In the conduct of AllOne Health's business operations, we may share PII with attorneys, consultants, human resources providers, payroll providers, and other service providers contracted to provide services for the activities, delivery, and management of AllOne Health products and services.

4.1.2 Purposes of PII/PHI collection

- AllOne Health collects only necessary information to provide services. PII/PHI processing is done only for necessary application functions and is not processed for any other reason.

4.1.3 Marketing and advertising use

- Data subjects will be contacted prior to any use of their PII/PHI for marketing or advertising purposes, and such use will not be done without the data subjects' consent. Consent to the use of PII/PHI for marketing or advertising by AllOne Health is not required to use AllOne Health services.

4.1.4 Infringing instruction

- AllOne Health will make its best effort to inform customers of any potential processing instructions received that violate applicable legislation or regulations in the opinion of AllOne Health's legal counsel.

4.1.5 Customer obligations

- Where applicable, customer obligations are outlined within the customer services agreement or other contracting documents for AllOne Health application.

4.1.6 Records related to processing PII/PHI

- All PII/PHI are considered strictly confidential by AllOne Health and records containing PII/PHI are maintained for a minimum of five years and no more than 7 years unless a different retention period is defined in contractual language with the customer.

4.2 OBLIGATIONS TO PII/PHI PRINCIPLES

4.2.1 Obligations to PII/PHI principles

- Where applicable, the terms of service for AllOne Health application detail customer obligations to PII/PHI principles such as the timely correction or deletion of PII/PHI within AllOne Health application.

4.3 PRIVACY BY DESIGN AND PRIVACY BY DEFAULT

4.3.1 Temporary Files

- Temporary files created during processing do not persist beyond the operation that created them and are not subject to extended retention. Volumes that may hold temporary files are encrypted at rest, protecting any residual data while present and supporting secure decommissioning of media.

4.3.2 Return, transfer, or disposal of PII/PHI

AllOne Health ensures that the return, transfer, or disposal of PII/PHI is performed in a secure, controlled, and compliant manner consistent with contractual, legal, and regulatory requirements.

Return of PII/PHI

- Upon termination or expiration of a contract, or where a customer is contractually entitled to request return, AllOne Health returns the applicable PII/PHI to the customer in a secure, mutually agreed format within the timeframe specified in the governing agreement. Where return or destruction is infeasible, AllOne Health notifies the customer, extends the protections of the agreement to retained data, and limits further use or disclosure to the purposes that make return or destruction infeasible.

Transfer of PII/PHI

- Where PII/PHI is transferred to customers, third parties, or authorized processors:
  - Transfers shall be limited to defined and lawful purposes
  - Appropriate safeguards, including contractual, technical, and organizational controls, shall be implemented to protect the data
  - Transfers shall comply with applicable data protection laws and contractual obligations

Disposal of PII/PHI

- When PII/PHI is no longer required for the purposes for which it was collected or retained:
  - Data shall be securely deleted or destroyed using approved methods
  - Disposal shall be performed in accordance with the AllOne Health data retention schedule and applicable legal or contractual requirements
  - Records of disposal activities shall be maintained where required

Retention Exception

- PII/PHI may be retained beyond contract termination where:
  - Required by applicable law or regulatory requirements
  - Necessary to support legal claims, audits, or business obligations

All return, transfer, and disposal activities are subject to oversight by AllOne Health's Information Security and Privacy program to ensure compliance with ISO 27701 and SOC 2 requirements.

4.3.3 PII/PHI transmission controls and security

AllOne Health implements technical and organizational controls to protect PII/PHI from unauthorized access, disclosure, alteration, and destruction, with a specific focus on secure transmission and handling of sensitive data.

Secure Transmission

- PII/PHI transmitted over public or untrusted networks is encrypted using industry-standard protocols (e.g., TLS or equivalent)

- Highly sensitive information requires additional safeguards such as file-level encryption or approved secure file transfer methods
- Transmission of PII/PHI via unsecured channels (e.g., SMS or unauthorized communication platforms) is strictly prohibited

Data Protection Controls

- PII/PHI is protected using layered security controls designed to prevent loss, misuse, and unauthorized access
- Systems enforce authentication and access controls (e.g., SSO, MFA) prior to permitting access to PII/PHI
- Access is restricted based on role and business need in accordance with least privilege principles

Data Accuracy and Integrity

- Controls are implemented to ensure that PII/PHI remains accurate, complete, and protected from unauthorized alteration during transmission and processing
- Validation and integrity checks are performed where appropriate to maintain data quality

Data Minimization in Transmission

- Only the minimum necessary PII/PHI is transmitted to fulfill defined business purposes
- Data transfers are limited to authorized recipients and approved use cases

Monitoring and Review

- Transmission and access activities involving PII/PHI are logged and monitored to detect unauthorized or suspicious activity
- Controls related to PII/PHI security are periodically reviewed and updated as part of the ISMS/PIMS continuous improvement process

- .

4.4 PII/PHI SHARING, TRANSFER, AND DISCLOSURE

4.4.1 Basis for PII/PHI transfer between jurisdictions

- Where legal counsel determines a transfer between jurisdictions will occur, AllOne Health will inform data subjects at least two weeks prior to the transfer and allow the data subject to accept such changes or terminate their contract with AllOne Health by contacting the DPO:
    - AllOne Health, ATTN: Data Protection Officer, 100 North Pennsylvania Avenue, Wilkes-Barre PA 18701 or via email at privacy@allonehealth.com.

4.4.2 Countries and international organizations to which PII/PHI can be transferred

- AllOne Health may from time to time, and as it deems appropriate, transfer PII/PHI within or between the following entities:
    - Countries:
        - The United States of America
        - Canada
    - Organizations:
        - Microsoft
        - Amazon

- Google

4.4.3 Records of PII/PHI disclosure to third parties

- The Registry of Processing Activities (ROPA) maintains a record of all PII/PHI disclosures to third parties. Data subjects may request information about their personal data by contacting the DPO.

4.4.4 SMS

- AllOne Health does not share SMS opt-in data with any third parties. Under no circumstances will personally identifiable information (PII) or protected health information (PHI) be transmitted or disclosed via SMS. This policy is strictly enforced in accordance with AllOne Health's data protection and privacy standards.

4.4.5 Notification of PII/PHI disclosure requests

- Where legally permissible, AllOne Health shall inform data subjects of requests of relevant PII/PHI made by government organizations or State entities.

4.4.6 Legally binding PII/PHI disclosures

- AllOne Health will, with the opinion of legal counsel, reject any request for PII/PHI disclosure where legally permissible.

4.4.7 Disclosure of subcontractors used to process PII/PHI

- Data subjects will be contacted by the DPO and informed of any pending disclosures of relevant PII/PHI to subcontractors prior to use.

4.4.8 Engagement of a subcontractor to process PII/PHI

- AllOne Health will only engage with subcontractors to process PII within the bounds of the data subject's contract.

4.4.9 Change of subcontractor to process PII/PHI

- AllOne Health shall inform customers, acting as controllers, and data subjects of any intended changes concerning the addition or replacement of subcontractors to process relevant PII/PHI and provide the customer, acting as controller, and data subject opportunity to object to such changes by contacting the DPO.

4.4.10 Requests, Questions or Concerns

- For any requests, questions or concerns regarding privacy, please contact the AllOne Health Data Protection Officer at:
    - AllOne Health, ATTN: Data Privacy Officer, 100 North Pennsylvania Avenue, Wilkes-Barre PA 18701 or via email at privacy@allonehealth.com.

5 Applicability

5.1 ISO/IEC 27001:2022 Controls

5.2 ISO/IEC 27701:2019 Objectives

5.3 SOC-2, Type 2

6 Document Control and Approval

6.1 Distribution

Name	Role
InfoSecurity SharePoint site, AllOne Health website	All Users

6.2 Approval

Prepared by: James Pettigrew
Title: System Administrator, Data and Communications Manager

Approved by: Gwen Mueller
Title: Director of IT
Date of Approval: 06/26/2026

6.3 Version History

Version History	Description of Change(s)	Updated By	Approved By	Date
1.0	Established privacy statement	Kylie LaFontaine		02/22/2018
2.0	Added ISO 27701 and SOC-2, Type 1 standards, added PHI	James Pettigrew		06/28/2022
2.1	Added cross reference for DPO to the Information Security and Privacy Policy, added DPO contact information, updated contact email to privacy@allonehealth.com	James Pettigrew		08/23/2022
2.2	Renamed document to PIMS Privacy Policy	James Pettigrew		08/23/2022
2.3	Added customer as controller for 4.4.8	James Pettigrew		08/25/2022
2.4	Updated policy approver	James Pettigrew	Gwen Mueller	07/17/2023
2.5	Grammar corrections, added type 2 to SOC reference, added ISO reference to 2022 standard	James Pettigrew	Gwen Mueller	07/24/2024
2.6	Added SMS statement to section 4.4.3	James Pettigrew	Gwen Mueller	10/10/2025

2.7	Updated Privacy by design and privacy by default, changed protection to privacy for DPO	James Pettigrew		06/25/2026

6.4 REPORTING

Use the standard statement of, “Any deviation from this policy shall be escalated to the AllOne Health ISMS/PIMS Steering Committee.”