Inception Date	02/22/2018
Approved Date	07/17/2023
Last Review Date	07/17/2023

PIMS Privacy Policy

1 Purpose

Strategic Objectives

- This Privacy Policy outlines AllOne Health's compliance with the ISO 27701 and SOC-2, Type 1 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 a 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 is 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 the processing of PII/PHI are retained for a minimum period of 7 years after which they are destroyed.

4.3.2 Return, transfer, or disposal of PII/PHI

- In the event that AllOne Health transfers PII/PHI to a third party acting as a controller, we will do so only if the third party has provided us with contractual assurances that it will:
  - Process the PII/PHI for limited and specified purposes consistent with the consent provided by the Data Subject
  - Provide the same level of protection as is required by ISO 27701 and SOC-2, Type 1 standards or equivalents
  - Notify us if they can no longer meet this obligation
    - If AllOne Health receives such a notice, AllOne Health will take reasonable and appropriate steps to stop and remediate any authorized processing

- AllOne Health may disclose PII/PHI to approved third party data processors retained or contracted by AllOne Health such as business partners and subcontractors, including, without limitation, affiliates, vendors, service providers and suppliers. We may share certain personal information with third parties who conduct marketing studies and data analytics, including those that provide tools or code which facilitates our review and management of our web site and services, such as Google Analytics or similar software products from other providers.

- Except to the extent agreed by the customer, AllOne Health may be required to share personal information as required or permitted by law, regulation, legal process, court order, bankruptcy or other legal requirement, or when we believe in our sole discretion that disclosure is necessary or appropriate, to respond to an emergency or to protect our rights, protect your safety or the safety of others, investigate fraud, comply with a judicial proceeding or subpoenas, court order, law-enforcement or government request, including without limitation to meet national security or law enforcement requirements, or other legal process and to enforce our agreements, policies and terms of use. Other than the aforementioned exceptions, the use and disclosure of all transferred personal information will be subject to this Policy.

- AllOne Health may be required to disclose PII/PHI in response to a lawful request by public authorities, including to meet national security or law enforcement requirements.

- All Data Subjects have the right to access the PII/PHI covered by this policy that AllOne Health holds about them. Additionally, if PII/PHI is inaccurate or has been processed incorrectly, Data Subjects have the right to access their PII/PHI to correct it, amend it or delete it.

- To request access to, or correction, amendment or deletion of, PII/PHI, a Data Subject should contact us at: privacy@allonehealth.com. AllOne Health will cooperate with all reasonable requests to assist Data Subjects to exercise their rights under this policy except when the burden or expense of providing access, correction, amendment, or deletion would be disproportionate to the risks to the Data Subject's privacy, or where the rights of persons other than the Data Subject would be violated.

- AllOne Health may modify this policy from time to time, consistent with changes to the requirements of the ISO 27701 and SOC-2, Type 1 frameworks, or changes within AllOne Health organization. If AllOne Health changes this policy, we will provide Data Subjects appropriate notice regarding such modifications by highlighting the changes on www.allonehealth.com , or by emailing Data Subjects' email addresses of record.

- Should you have any questions or concerns about this Policy or need to update certain personal information, please contact privacy@allonehealth.com.

4.3.3 PII/PHI transmission controls and security

- AllOne Health takes reasonable and appropriate measures to protect PII/PHI covered by this policy from loss, misuse, unauthorized access, disclosure, alteration, and destruction. While AllOne Health cannot guarantee the security of PII/PHI, we are committed to safeguarding all PII/PHI received.

- AllOne Health only collects PII/PHI that is relevant for the purposes of processing. We do not process PII/PHI that is incompatible with the purposes for which it was collected or authorized by the Data Subject. Additionally, AllOne Health takes reasonable steps to ensure that any PII/PHI that is collected is relevant to its intended use, accurate, complete and current.

- AllOne Health retains PII/PHI in a form identifying or making identifiable a Data Subject only for as long as it serves a purpose of processing, which includes the performance of services, obligations to comply with professional standards and legitimate business purposes. We will only request the minimum amount of PII/PHI required to carry out these purposes and will adhere to the ISO 27701 and SOC-2, Type 1 standards for as long as we retain PII/PHI.

- AllOne Health agrees to periodically review and verify our compliance with the ISO 27701 and SOC-2, Type 1 frameworks, and to remedy any nonconformities with that standard.

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 message 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 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.

4.4.5 Legally binding PII/PHI disclosures

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

4.4.6 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.

4.4.7 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.

4.4.8 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.

4.4.9 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 Protection Officer, 100 North Pennsylvania Avenue, Wilkes-Barre PA 18701 or via email message at privacy@allonehealth.com.

5 APPLICABILITY

5.1 ISO/IEC 27001:2013 CONTROLS

- A.5.1.1
- A.6.1.1
- A.6.2.1
- A.7.2.2
- A.8.2.1
- A.8.2.2
- A.8.3.1
- A.8.3.2
- A.8.3.3
- A.9.2.1
- A.9.2.2

- A.9.4.2
- A.10.1.1
- A.11.2.7
- A.11.2.9
- A.12.3.1
- A.12.4.1
- A.12.4.2
- A.13.2.1
- A.13.2.4
- A.14.1.2
- A.14.2.1
- A.14.2.5
- A.14.2.7
- A.14.3.1
- A.15.1.2
- A.16.1.1
- A.16.1.5
- A.18.1.1
- A.18.1.3
- A.18.2.1
- A.18.2.3

5.2 ISO/IEC 27701:2019 CONTROLS

- 8.2.1
- 8.2.2
- 8.2.3
- 8.2.4
- 8.2.5
- 8.2.6
- 8.3.1
- 8.4.1

- 8.4.2
- 8.4.3
- 8.5.1
- 8.5.2
- 8.5.3
- 8.5.4
- 8.5.5
- 8.5.6
- 8.5.7
- 8.5.8

5.3 SOC-2, TYPE 1

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: 07/17/2023

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

6.4 REPORTING

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