Data Management & Security

- HMIS Security Standards
- HIPAA Compliance

This policy establishes the overarching principles for managing and securing data at Anything Helps. It sets out the procedures for protecting all types of sensitive data, ensuring compliance with internal data management protocols. This policy aims to safeguard the confidentiality, integrity, and availability of data, while supporting operational needs. This policy applies to all employees, contractors, and volunteers who handle data within the organization. It ensures that data is appropriately managed throughout its lifecycle, from collection and storage to sharing and disposal.

Data Protection

Anything Helps will ensure the confidentiality, integrity, and availability of sensitive information through the following practices:

1. All physical and electronic data must be encrypted and stored securely.
2. Access to sensitive information will be limited to authorized personnel.
3. Secure systems will be used for data entry, storage, retrieval, and transmission to preserve data integrity.
4. Role-based access control (RBAC) will be implemented to assign access privileges based on user responsibilities.

Incident Response and Breach Notification

Incident Reporting: Employees, contractors, and business associates must immediately report any suspected or actual PHI breach to the designated Privacy Officer.

Initial Investigation: Within 24 hours of discovery, the Privacy Officer shall:

1. Investigate the cause of the breach;
2. Determine the type and scope of PHI involved;
3. Assess whether the breach has been contained;
4. Evaluate the potential impact, including:
    - The nature and sensitivity of the PHI;
    - The potential harm to affected individuals;
    - Whether unauthorized individuals accessed the PHI.

Breach Notification Requirements:

- If fewer than 500 individuals are affected, notify the individuals and the U.S. Department of Health and Human Services (HHS) within 60 days of the end of the calendar year.
- If 500 or more individuals are affected, notify affected individuals, HHS, and the media (if appropriate) within 60 days of breach discovery.

Containment and Prevention measures may include:

- Immediate actions to contain the breach;
- Updating or revising security protocols;
- Staff retraining on data protection practices;
- Implementation of new technical safeguards, such as stronger encryption or access controls.

Documentation: The Privacy Officer shall compile a written report that includes:

1. A description of how the breach occurred;
2. Details on containment and mitigation actions;
3. The process and timeline used to notify all required parties.

Monitoring and Compliance

To support ongoing data protection:

- Regular audits will be conducted to ensure adherence to this policy and related protocols.
- All staff will participate in annual training on data security and incident response.
- Any suspected breach will be promptly evaluated and managed under the procedures outlined in this policy.

> **References:**

Previous: Systemization Standards **Next:** Service Provision