HIPAA Policy and Procedure Manual

Revised December 12, 2023

1. Introduction

1.1. Introduction

Arammu is committed to protecting the privacy, security, confidentiality, integrity, and availability of Individually Identifiable Health Information (PHI) in compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and their associated regulations. All individuals representing Arammu will take responsibility for safeguarding PHI to which they have access. Violation of provisions set forth in these policies and procedures may result in disciplinary action, which may include termination of employment

1.2 Purpose

This document outlines the policies and procedures implemented by Arammu to ensure compliance with the Health Insurance Portability and Accountability Act (HIPAA) and to protect the confidentiality, integrity, and availability of Protected Health Information (PHI).

In the event of any conflict between a provision of these policies and more stringent State laws or requirements, the more stringent law or requirement shall control.

1.3 Scope

This policy applies to all employees, contractors, and third-party service providers who have access to PHI at Arammu.

1.4. Questions Concerning HIPAA Compliance

If any member of Arammu's Workforce has a question concerning Arammu's privacy or breach notification policies, the HIPAA Privacy or Breach Notification Rules, or their application to any situation, they shall contact the Privacy Officer for guidance.

1.5 Disclaimer

It is the intention of Arammu that these Privacy and Security Policies be used by its employees, and other members of its Workforce, in meeting their responsibilities to Arammu. Violation of a policy can be the basis for discipline or termination of employment; however, because these Privacy and Security Policies relate to the establishment and maintenance of high standards of performance, under no circumstances shall any policy or procedure be interpreted or construed as establishing a minimum standard, or any evidence of a minimum standard, of the safety, due care, or any other obligation which may be owed by Arammu, its employees, or its agents to another person.

2. Definitions

Access
The ability or the means necessary to read, write, modify or communicate data/information or otherwise use any system resource.

Business Associates
Entities that perform functions or activities on behalf of a Covered Entity that involves the use or disclosure of PHI.

Breach
The unauthorized acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule, which compromises the security or privacy of PHI.

Covered Entities
Entities that transmit health information electronically, such as healthcare providers, health plans, and healthcare clearinghouses.

Encryption
The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

Healthcare Insurance Portability and Accountability Act (HIPAA)
Developed in 1996, the acronym HIPAA stands for Healthcare Insurance Portability and Accountability Act. Initially created to help the public with insurance portability, HHS eventually built administrative simplifications that involved electronic, medical record technology and other components. In addition, HHS built a series of privacy tools to protect healthcare data.

Privacy Rule
The part of the HIPAA rule that addresses the saving, accessing and sharing of medical and personal information of an individual, including a patient's own right to access.

Protected Health Information (PHI)
Protected Health Information (PHI) refers to any individually identifiable health information that is transmitted or maintained in any form or medium, including electronic, oral, or paper. PHI means any health information, including demographic information, HIPAA Privacy and Security Policies and Procedures, including demographic information collected from an individual, that:

1. Is created or received by a health-care provider, health plan, employer or health-care clearinghouse; and,

2. Relates to the past, present or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present or future payment for the provision of healthcare to an individual; and,
    a. That identifies the individual; or,
    b. There is a reasonable basis to believe the information can be used to identify the individual.

Security Rule
The part of the HIPAA rule that outlines national security standards intended to protect health data created, received, maintained or transmitted electronically.

Arammu has made a significant effort to limit PHI collected. The primary PHI collected consists of individuals name and email address. No other demographic or identifiable health information is collected on Arammu's platform.

3. Responsibilities

3.1 Designated Privacy Officer

Arammu designates Matt Rubin as the Privacy Officer responsible for the development and implementation of privacy policies and procedures.

The Privacy Officer of Arammu shall:
1. Oversee the development, implementation, maintenance, and revision of policies and procedures to protect confidential health information in accordance with Federal and State regulations. The Privacy Officer notifies the Executive Team of any policies, procedures, or implementation issues that need their review;
2. Perform periodic Privacy Rule focused risk assessments to identify issues that need attention;
3. Develop staff training on HIPAA policies, procedures, and practices;
4. Monitor and ensure that all Arammu employees receive HIPAA training;
5. Maintain an updated Notice of Privacy Practices that is distributed in accordance with these procedures;
6. Manage disclosures of information;
7. Investigate potential breaches and determine whether there has been a breach of unsecured PHI; notify appropriate parties as outlined in the Breach Notification Procedure.
8. Respond to Requests for Amendments of PHI;
9. Investigate and respond to complaints regarding the confidentiality of information;
10. Provide additional information about matters covered by the Notice of Privacy Practices;
11. Update privacy forms and coordinate the placement of these forms throughout Arammu.

3.2 Workforce Training

All employees must undergo training on HIPAA policies and procedures upon hire and regularly thereafter. Training will cover the importance of safeguarding PHI and the consequences of non-compliance.

All members of Arammu shall be trained annually on Arammu's privacy and breach notification policies and procedures with respect to PHI as necessary and appropriate for the members of the Workforce to carry out their functions within Arammu. Additional training will also occur in response to any risk assessment identifying the need for additional training.

The Privacy Officer will ensure the documentation of each training session and the names of Arammu employees who completed the training. The supervisors of interns and volunteers will document their HIPAA training when it occurs.

4. Safeguards for PHI

4.1 Background

In compliance with the Privacy Rule of the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) covered entities and business associates must have in place implemented policies and procedures to safeguard patients' PHI (§164.524).

All Arammu employees, subcontractors, Business Associates, interns, and volunteers are responsible for the privacy and security of PHI of persons receiving services. The Privacy Officer shall implement appropriate administrative, technical and physical safeguards to protect the privacy of PHI and to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure. They are responsible for periodically monitoring to ensure that uses and disclosure of PHI complies with applicable Federal, State and/or local law or regulation, and these policies and procedures.

4.2 Policy

It is the policy of Arammu to honor a patient's right of access to inspect and obtain a copy of their protected health information (PHI) in Arammu's designated record set, for as long as the PHI is maintained in compliance with HIPAA and Arammu's retention policy.

4.3 Limited Data Collection

Arammu will only collect the minimum necessary PHI required to perform business functions.

4.4 Access Controls

Access to PHI will be restricted to authorized personnel based on their job responsibilities. User accounts will be monitored and terminated promptly upon termination of employment.

4.5 Transmission Security

PHI transmitted electronically will be encrypted to ensure the confidentiality and integrity of the information.

See Arammu System Security Plan for more details.

4.6. Vulnerability Testing

Arammu will hire an external third-party company to perform vulnerability testing on an annual basis.

5. Privacy Notice

5.1 Notice of Privacy Practices

Arammu will provide a Notice of Privacy Practices to individuals whose PHI is collected, outlining their rights and how their information will be used and disclosed.

The Notice of Privacy Practices shall comply with HIPAA rules and regulations. The Notice of Privacy Practices communicates:

1. The uses and disclosures of PHI that may be made by Arammu
2. The rights of a person with respect to their PHI; and,
3. Arammu duties in safeguarding such PHI.

The Notice shall be written in plain language and shall be made available in languages understood by a substantial number of individuals served by Arammu. Arammu shall make certain the Notice in Spanish translation is available.

5.2 Changes to Privacy Practices Not Stated in Notice of Privacy Practices

Arammu may change, at any time, a privacy practice that does not materially affect the content of its Notice of Privacy Practices, provided:

1. The policy or procedure involved, as revised, complies with the HIPAA Privacy and Breach Notification Rules; and,
2. Prior to the effective date of the change, the policy or practice, as revised, is documented by the Privacy Officer in written or electronic form for six (6) years from the date of its creation or the date when it last was in effect, whichever is later.

6. Minimum Necessary Use and Disclosures of PHI

When using or disclosing PHI, members of Arammu Workforce shall make reasonable efforts to limit the amount of PHI used or disclosed to the minimum necessary. The following standards (the "Minimum Necessary Standard") apply to the use and disclosure of PHI:

1. Arammu Workforce members shall only have access to the amount and type of PHI necessary to carry out their job duties, functions and responsibilities.
2. Arammu limits access to, and use of, the PHI of persons served in accordance with its business associate agreements with vendors and subcontractors.
3. Arammu Workforce members shall restrict their use, access and disclosure of PHI to the minimum necessary to achieve the purpose of the disclosure.

This Minimum Necessary Standard does not apply in the following situations:

1. When the PHI is for use by, or a disclosure to, a healthcare provider for purposes of providing treatment to the patient;
2. When the disclosure is to the person served, their parent (if a minor), legal guardian or legally authorized personal representative;
3. When the disclosure is pursuant to a valid Authorization requested through the person served or their parent (if a minor), legal guardian or legally authorized personal representative, in which case the disclosure shall be limited to the PHI specified in the Authorization;
4. When the disclosure is to the Secretary of the U.S. Department of Health and Human Services (Federal government);
5. When the law requires the disclosure; only PHI required to be disclosed by law shall be disclosed.

Minimum Necessary Standard When Requesting PHI

When requesting PHI from another entity, Arammu shall limit its request for PHI to the amount reasonably necessary to accomplish the purpose for which the request is made. For requests that are not on a routine or recurring basis, Arammu shall evaluate the request to determine if the requirements of the Privacy Rule have been satisfied.

7. Reporting and Response to Breaches

7.1 Determining Whether a Breach of PHI Occurred

This section addresses Arammu's Breach Notification Rule Requirements. An acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule is presumed to be a breach unless the Privacy Officer or Business Associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the PHI or to whom the disclosure was made;
3. Whether the PHI was actually acquired or viewed; and,
4. The extent to which the risk to the PHI has been mitigated.

The risk assessment will also examine the three exceptions of a definition of a breach:

1. Unintentional acquisition, access, or use of PHI by a Workforce member or person acting under the authority of Arammu or Arammu business associate and such acquisition, access, or use was made in good faith and within the scope of authority;
2. Inadvertent disclosure of PHI by a person authorized to access PHI to another person authorized to access PHI at Arammu, a member of the OHCDS, or an Arammu business associate;
3. Arammu or Arammu's business associate has a good faith belief that the unauthorized person to whom the impermissible disclosure was made would not have been able to retain the information.

7.2 Procedures for Breach Notification

Arammu maintains an open-door policy regarding compliance with HIPAA. Employees, subcontractors, interns and volunteers are encouraged to speak with the Privacy Officer or other appropriate individual regarding any concerns they may have with Arammu's HIPAA policies and procedures or initiatives designed to maintain and enhance privacy and security controls. There shall be no retaliation against employees, subcontractors, interns or volunteers who, in good faith, report any activities he or she believes is a breach of HIPAA. Although not guaranteed (depending on the circumstances) anonymity shall be maintained whenever possible. Arammu may impose lesser sanctions, when it determines it is appropriate, when a Workforce member is responsible for a breach, and reports the breach; and/or that more severe sanctions may be imposed for a Workforce member who is responsible for a breach, but fails to report it, under appropriate circumstances.

Employees, subcontractors, interns or volunteers who believe that unauthorized access, use or disclosure of PHI has occurred shall immediately report the circumstances of the suspected breach to their supervisor and the Privacy Officer

within forty-eight (48) hours after knowledge of the incident. The report of a potential breach shall include the following information, to the extent available:

1. A brief description of what happened, including the date of the potential breach and the date the potential breach was discovered;
2. Who used the PHI without appropriate permission or Authorization and/or to whom the information was disclosed without permission or Authorization;
3. A description of the types of and amount of unsecured PHI involved in the breach;
4. Whether the PHI was secured by encryption, destruction, or other means;
5. Whether any intermediate steps were taken to mitigate an impermissible use or disclosure;
6. Whether the PHI that was disclosed was returned prior to being accessed for an improper purpose; and,
7. If the PHI was provided to Arammu under a Business Associate Agreement.

Following a report of a concern of impermissible use or disclosure of PHI, the Privacy Officer, or their designee, will complete a risk assessment to determine the probability level that the PHI has been compromised by the impermissible use or disclosure. The conclusion of the risk assessment will be documented, along with any actions needed, such as a notification letter, in the Arammu HIPAA Incident Log. It is expected that members of Arammu's Workforce will cooperate in the investigation and assessment.

Failure to report a suspected breach to the Privacy or Security Officer may result in disciplinary action against employees, subcontractors, interns or volunteers.

7.3 Timeline of Notification

HIPAA's breach notification rule requires notification to affected individuals, the Secretary of USHHS, and in certain cases, the media, without unreasonable delay and within sixty (60) calendar days following the discovery of a breach under Federal and or State HIPAA rule guidelines. The discovery of a breach includes the first date it shall have been known by exercising reasonable diligence.

7.4 Content of Notification

The Privacy Officer will be responsible for writing and sending the Breach Notification letters to affected individuals. The notification shall be written in plain language and include to the extent possible:

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
2. A description of the types of unsecured PHI that were involved in the breach (name, email address);
3. Any steps individuals shall take to protect themselves from potential harm resulting from the breach;

4. A brief description of what Arammu is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and,
5. Contract procedures for individuals to ask questions or learn additional information, which shall include a phone number, an e-mail address, Web site, or postal address.

Reasonable steps shall be taken to have the notification translated into languages that are frequently encountered by Arammu and as may be necessary to ensure effective communication with individuals with disabilities.

8. Documentation and Record Retention

8.1 Documenting Policies and Procedures

All policies and procedures related to HIPAA compliance will be documented and maintained.

8.1.1 Policy Development Process:
- Arammu will establish a systematic process for developing, reviewing, and approving policies and procedures related to HIPAA compliance.
- The process will involve input from relevant stakeholders, including the Privacy Officer, legal counsel, and department heads.
- Policies and procedures will be reviewed at least annually or more frequently if there are changes in the business environment, technology, or regulations.

8.1.2 Policy Ownership and Accountability:
- Each HIPAA-related policy will have a designated owner who is responsible for its maintenance, updates, and compliance.
- Owners will ensure that policies are aligned with the current legal and regulatory landscape and communicate any changes to affected parties promptly.

8.1.3 Accessibility of Policies:
- All HIPAA policies and procedures will be maintained in a centralized repository accessible to all employees.
- The repository will include the most recent versions of policies, along with a version control mechanism to track changes.

8.1.4 Employee Acknowledgment:
- Employees will be required to acknowledge their understanding and agreement to comply with HIPAA policies and procedures.
- Acknowledgments will be documented and retained as part of the employee's personnel file.

8.1.5 Policy Training:

- Arammu will provide regular training sessions to employees regarding HIPAA policies and procedures.
- Training sessions will cover policy updates, best practices, and case studies to enhance understanding and application.

8.2 Record Retention

8.2.1 Retention Period:

- Arammu will establish and maintain a record retention schedule for all documents containing PHI.
- The retention period will comply with HIPAA regulations and any applicable state laws, taking into account the nature of the information and business needs.

8.2.2 Secure Storage:

- PHI and related records will be stored securely, whether in physical or electronic form, to prevent unauthorized access, disclosure, or tampering.
- Physical records will be stored in locked cabinets, and electronic records will be stored on secure servers with access controls.

8.2.3 Record Disposal:

- Arammu will implement secure procedures for the disposal of PHI and related records.
- Procedures will ensure the permanent and irretrievable destruction of PHI to prevent unauthorized access.

8.2.4 Documentation of Record Disposal:

- Arammu will maintain documentation of the disposal process, including dates, methods, and responsible parties.
- Documentation will be retained in accordance with the record retention schedule.

By implementing these detailed documentation and record retention practices, Arammu aims to ensure the ongoing effectiveness and compliance of its HIPAA policies and procedures. Regular reviews, updates, and training will contribute to a culture of awareness and responsibility surrounding the handling of PHI within the organization.

9. Enforcement and Penalties

9.1 Disciplinary Actions

9.1.1 Non-Compliance Investigations:

- Any suspected or reported instances of non-compliance with HIPAA policies and procedures will be thoroughly investigated by the Privacy Officer or designated personnel.

- Investigations may involve interviews, document reviews, and other relevant actions to determine the extent of the non-compliance.

9.1.2 Disciplinary Actions Process:
- Disciplinary actions will be taken in a fair and consistent manner, following a documented process.
- The severity of the disciplinary action will be commensurate with the nature and recurrence of the violation, ranging from verbal counseling to termination of employment.

9.1.3 Employee Reporting Obligations:
- Employees are obligated to report any known or suspected non-compliance with HIPAA policies and procedures promptly.
- Failure to report violations may result in disciplinary action.

9.1.4 Record of Disciplinary Actions:
- Arammu will maintain a confidential record of all disciplinary actions related to HIPAA non-compliance.
- Records will include details of the violation, actions taken, and any remedial measures implemented.

9.2.1 Civil Penalties:
- Violations of HIPAA may result in civil penalties imposed by the Office for Civil Rights (OCR).
- Civil penalties may include fines, with amounts varying based on the level of negligence, the nature of the violation, and the number of affected individuals.

9.2.2 Criminal Penalties:
- Intentional or willful violations of HIPAA may result in criminal charges, leading to fines and imprisonment.
- Criminal charges may be pursued when there is evidence of deliberate disregard for patient privacy or when PHI is used for malicious purposes.

10. Review and Revision

10.1 Periodic Review

10.1.1 Scheduled Reviews:
- Arammu is committed to conducting scheduled reviews of all HIPAA policies and procedures on an annual basis.
- The Privacy Officer, in collaboration with relevant stakeholders, will initiate and oversee the review process.

10.1.2 Review Committee:

- A designated committee, including the Privacy Officer, legal counsel, and representatives from relevant departments, will be responsible for conducting the periodic reviews.
- The committee will assess the effectiveness and appropriateness of existing policies, considering changes in the regulatory environment, technology, and business practices.

10.1.3 Documentation of Reviews:
- Each review will be thoroughly documented, capturing any identified deficiencies, recommended changes, and actions taken.
- Documentation will include the date of the review, participants, and a summary of findings.

10.2 Policy Update Process

10.2.1 Change Management Process:
- Arammu will implement a change management process to facilitate updates to HIPAA policies and procedures.
- Proposed changes will be documented, reviewed by the designated committee, and approved by the Privacy Officer before implementation.

10.2.2 Communication of Changes:
- Employees will be promptly informed of any updates or changes to HIPAA policies and procedures.
- Communication methods may include email notifications or training sessions.

10.2.3 Acknowledgment of Policy Changes:
- Employees will be required to acknowledge and confirm their understanding of any updated HIPAA policies within a specified timeframe.
- Acknowledgments will be documented and retained as part of the employee's personnel file.

10.3 Continuous Monitoring

10.3.1 Ongoing Compliance Monitoring:
- Arammu will establish continuous monitoring mechanisms to assess ongoing compliance with HIPAA policies and procedures.
- Monitoring activities may include regular audits, risk assessments, and internal reporting mechanisms.

10.3.2 Incident Reporting and Analysis:
- Employees will be encouraged to report any incidents, near misses, or concerns related to HIPAA compliance promptly.
- Reported incidents will be thoroughly investigated, and findings will be used to inform updates to policies and procedures as necessary.

10.4 Documentation of Changes

10.4.1 Version Control:

- A version control system will be maintained for all HIPAA policies and procedures, clearly indicating the most recent versions.
- Version control will assist in tracking changes over time and ensuring that employees are working with the latest policies.

10.4.2 **Archiving Previous Versions:**

- Previous versions of policies and procedures will be archived for a specified period, as required by record retention policies.
- Archived versions will be maintained for reference and auditing purposes.

By establishing a comprehensive review and revision process, Arammu aims to ensure that HIPAA policies and procedures remain current, effective, and aligned with regulatory requirements. Regular reviews, effective communication of changes, and continuous monitoring contribute to the ongoing success of the organization's HIPAA compliance efforts.

11. Contact Information

11.1 Privacy Officer Contact

Individuals may contact Matt Rubin, the Privacy Officer, at matt@arammu.com, (781) 223- 3997 with any questions or concerns regarding the company's HIPAA policies and procedures.

By implementing and adhering to these policies and procedures, Arammu aims to protect the privacy and security of PHI in compliance with HIPAA regulations. Employees are responsible for familiarizing themselves with these policies and procedures and following them diligently. Non-compliance may result in disciplinary action, legal consequences, and damage to Arammu's reputation.

In conclusion, Arammu is committed to upholding the highest standards of privacy and security in the handling of Protected Health Information (PHI). This HIPAA policy serves as a testament to our dedication to compliance with regulatory requirements and the safeguarding of individuals' sensitive health information. As we navigate the dynamic landscape of healthcare and technology, we recognize the importance of continuous improvement. Through periodic reviews, diligent enforcement, and a culture of responsibility, we strive to not only meet but exceed the expectations set forth by the Health Insurance Portability and Accountability Act. By embracing these principles, we ensure that PHI is handled with the utmost care, integrity, and confidentiality, thereby fostering trust among our patients, partners, and the community we serve. Thank you for your commitment to maintaining the highest standards of ethical and legal conduct in all aspects of our operations.

Appendix A:

Arammu's Notice of Privacy Policy

Notice of Privacy Practices
Effective Date: December 15, 2023

Introduction:
Arammu is dedicated to protecting the privacy and confidentiality of your health information. This Notice of Privacy Practices explains how we use and disclose your Protected Health Information (PHI) and your rights regarding this information. PHI is information about you, including demographic information, that may identify you and relates to your past, present, or future physical or mental health or condition, the provision of healthcare services, or the payment for healthcare services.

Uses and Disclosures of PHI:
Arammu may use or disclose your PHI for purposes of treatment, payment, or healthcare operations. However, as a company that collects minimal PHI, our use and disclosure of this information are limited to what is necessary for the purposes of providing services to you.

1. **Treatment:** We may use your PHI to provide you with healthcare services. For example, information obtained by a healthcare provider will be recorded in your record and used to determine the course of counseling that should work best for you.
2. **Payment:** We may use and disclose your PHI to obtain payment for the services we provide. For example, we may use your health information to prepare a bill for services rendered.
3. **Healthcare Operations:** We may use and disclose your PHI for healthcare operations, which include activities necessary to run our business. For example, we may use your PHI to evaluate the quality of services provided or to conduct audits.

Your Rights Regarding PHI:

You have the following rights concerning your PHI:
1. **Right to Inspect and Copy:** You have the right to inspect and obtain a copy of your PHI.
2. **Right to Amend:** If you feel that the PHI we have about you is incorrect or incomplete, you may request an amendment.
3. **Right to an Accounting of Disclosures:** You have the right to request an accounting of certain disclosures of your PHI made by us.
4. **Right to Request Restrictions:** You have the right to request restrictions on certain uses and disclosures of your PHI.

5. **Right to Request Confidential Communication:** You have the right to request that we communicate with you about your health information in a certain way or at a certain location.
6. **Right to a Paper Copy of this Notice:** You have the right to receive a paper copy of this Notice.

Our Responsibilities:
Arammu is required by law to maintain the privacy of your PHI and to provide you with notice of our legal duties and privacy practices. We are committed to protecting the privacy of your PHI and will abide by the terms of this Notice.

Security:
The Site has significant security measures in place to protect against the loss, misuse or alteration of information under Arammu's control.

Compliance with COPPA:
The Site is not directed at children under the age of 13. Arammu complies with the Children's Online Privacy Protection Act and does not knowingly permit submission of Personal Information by anyone under 13 years of age.

Correct/Update Procedure:
If you want to delete or modify your Personal Information Arammu's records, you may do so by:

- Email: info@arammu.com

Changes to this Notice:
We reserve the right to change this Notice. Any changes will be effective for all PHI that we maintain. An updated Notice will be available upon request and will be posted on our website.

Contact Information:
If you have any questions or concerns regarding this Notice, please contact:
Matt Rubin, Privacy Officer, at matt@arammu.com, (781) 223- 3997.

We are dedicated to protecting your privacy and providing you with the highest level of service.

Tatiana Gray, Ph.D.
Chief Operating Officer

Date: December 15, 2023