HIPAA Compliance Policy

1. Purpose

This HIPAA Compliance Policy is designed to ensure that The Merlin Group World adheres to the requirements of the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and the subsequent amendments, including the Health Information Technology for Economic and Clinical Health (HITECH) Act. It aims to protect the privacy and security of Protected Health Information (PHI) and ensure compliance with all relevant federal regulations.

2. Scope

This policy applies to all employees, contractors, and business associates of The Merlin Group World with access to PHI or Personal Health Records (PHR) within our system. This includes all administrative, clinical, and support staff.

This includes any business associates such as CarePatron and AboveBoard, or others contracted by The Merlin Group World to store, process, or access PHI. All business associates must sign a Business Associate Agreement (BAA) prior to handling any PHI.

3. Definitions

Protected Health Information (PHI): Any information, whether oral or recorded in any form, that relates to the health, provision of health care, or payment for health care that can be linked to an individual.

Electronic Protected Health Information (ePHI): PHI transmitted by electronic media or maintained in electronic media.

Business Associate: A person or entity, not a workforce member, who performs functions or activities on behalf of or provides certain services to a covered entity that involves the use or disclosure of PHI.

4. Privacy practices

HIPAA Compliance Policy

The Merlin Group World is committed to maintaining the privacy of PHI. This involves providing notice of our legal duties and privacy practices concerning PHI, including:

- Use and disclosure of PHI for treatment, payment, and health care operations.
- Individuals have the right to understand and control how their PHI is used.
- Obligations to protect the privacy of PHI.

5. Security measures

To protect ePHI,The Merlin Group World implements the following security measures:
- Security Controls
  - Encryption

Administrative safeguards: Policies and procedures designed to clearly show how the entity will comply with the act. These include:

- Administrative Safeguards: Staff training on HIPAA rules; internal access controls to limit PHI access; signed confidentiality agreements.

- Physical Safeguards: Secure workstations; restricted physical access to data storage devices; locked offices when unattended.

- Technical Safeguards: Use of HIPAA-compliant platforms such as CarePatron; AES-256 encryption of data in transit and at rest; strong password policies and multi-factor authentication.

- Security Controls: Routine access logging and audits; system alerts for unauthorized access attempts; regular vulnerability assessments.

7. Breach notification

In a breach involving unsecured PHI, The Merlin Group World will notify affected individuals, the Secretary of Health and Human Services, and, if the breach involves more than 500 individuals, the media, following HIPAA regulations.

HIPAA Compliance Policy

Organization's breach response plan:

7.1 Breach Identification and Reporting

- All employees, contractors, and vendors are required to immediately report any known or suspected breach of PHI to the HIPAA Security Officer.
- Reports must include: what was accessed, when it occurred, how it was discovered, and any known individuals affected.
- Initial reports may be submitted verbally, but must be documented in writing within 24 hours of discovery.

7.2 Investigation and Risk Assessment

The HIPAA Security Officer will initiate an internal investigation and risk assessment within 48 hours of breach discovery, including:

- The nature and extent of the PHI involved
- The identity of the unauthorized person who accessed or disclosed the PHI
- Whether the PHI was actually viewed or acquired
- The extent to which the risk has been mitigated

If it is determined that there is a significant risk of harm to individuals, the event is classified as a breach requiring notification.

7.3 Notification Requirements

HIPAA Compliance Policy

If a breach is confirmed, The Merlin Group World will provide notification as follows:

- **Affected Individuals:** Written notice by first-class mail (or email, if consent is given) within **60 calendar days** of breach discovery.
- **Secretary of Health and Human Services (HHS):**
    - For breaches involving **fewer than 500 individuals**, notification is submitted **annually** through the HHS portal.
    - For breaches involving **500 or more individuals**, notification must be submitted **within 60 calendar days**.
- **Media Notification:** If 500 or more individuals in a single state or jurisdiction are affected, a press release will be issued to prominent media outlets serving the area.

All notifications will include:

- A description of the breach
- Types of information involved
- Steps affected individuals should take to protect themselves
- Actions taken by The Merlin Group World to investigate, mitigate, and prevent further breaches
- Contact information for further questions

7.4 Documentation

All breach investigations and actions taken will be documented and retained for a minimum of **six years**.

Documentation will include:

- Initial breach report
- Investigation notes
- Risk assessment findings
- Notifications sent
- Corrective actions implemented

7.5 Mitigation and Corrective Action

Following a breach, The Merlin Group World will:

- Contain and mitigate any ongoing risks
- Implement corrective actions to address gaps in security
- Provide additional staff training if appropriate
- Review and update relevant HIPAA policies and procedures

8. Training and awareness

HIPAA Compliance Policy

All staff members of The Merlin Group World will receive training on HIPAA policies and procedures, with additional training provided as rules and regulations evolve. This training includes but is not limited to privacy practices, security measures, and breach notification procedures.

9. Compliance and enforcement

The Merlin Group World will regularly review and update HIPAA compliance efforts to ensure ongoing adherence to all relevant regulations. Violations of this policy may result in disciplinary action, including termination of employment.

10. Designation of HIPAA Security Officer

To ensure compliance with the HIPAA Security Rule, The Merlin Group World has designated the following individual to serve as the HIPAA Security Officer:

Name: Samuel Juan Salgado

Title: HIPAA Security Officer

Organization: The Merlin Group World

Email: themerlingroupworld@gmail.com

The HIPAA Security Officer is responsible for overseeing the implementation and management of all technical, physical, and administrative safeguards necessary to protect electronic Protected Health Information (ePHI). Responsibilities include, but are not limited to:

Ensuring access to ePHI is restricted and role-based

Implementing and managing encryption and authentication protocols

Monitoring and auditing system access and security logs

Developing incident response plans and breach protocols

HIPAA Compliance Policy

Reviewing and updating security practices regularly

Coordinating with any third-party service providers (e.g., CarePatron, AboveBoard) to ensure their platforms meet HIPAA security requirements

The Security Officer will conduct or oversee periodic risk assessments and ensure compliance with evolving regulatory standards.

11. Designation of HIPAA Privacy Officer

Name: Samuel Juan Salgado

Title: HIPAA Privacy Officer

Email: themerlingroupworld@gmail.com

The Privacy Officer is responsible for ensuring proper handling of PHI in accordance with HIPAA's Privacy Rule. This includes managing how PHI is used and disclosed, addressing patient rights (such as access and correction), and investigating privacy-related complaints or incidents.

12. Policy review and modification

This policy will be reviewed annually and modified as necessary to ensure compliance with HIPAA regulations and to reflect changes in federal law, state law, and The Merlin Group World's operations.

13. Contact information

For any questions or concerns regarding this policy or HIPAA compliance, please contact:

themerlingroupworld@gmail.com or +18137664900.

14. Business Associate Agreements (BAAs)

HIPAA Compliance Policy

All vendors or third parties that have access to PHI (e.g., calendar systems, hosting providers, communication platforms) must have a signed Business Associate Agreement with The Merlin Group World, ensuring their compliance with HIPAA. BAAs are required before any data is shared or access is granted.