# HIPAA BUSINESS ASSOCIATE PRIVACY POLICY

We take privacy very seriously. We share a commitment with Covered Entities to protect the privacy and confidentiality of Protected Health Information (PHI) that we obtain subject to the terms of a Business Associate Agreement.

This policy is provided to help you better understand how we use, disclose, and protect PHI in accordance with the terms of Business Associate Agreements.

## Definitions

- *Business Associate Agreement (BA Agreement).* A formal written contract between iMerit and a Covered Entity that requires iMerit to comply with specific requirements related to PHI.
- *Covered Entity.* A health plan, healthcare provider, or healthcare clearinghouse that must comply with the HIPAA Privacy Rule.
- *Protected Health Information (PHI).* PHI includes all "individually identifiable health information" that is transmitted or maintained in any form or medium by a Covered Entity. Individually identifiable health information is any information that can be used to identify an individual and that was created, used, or disclosed in (a) the course of providing a health care service such as diagnosis or treatment, or (b) in relation to the payment for the provision of health care services.

## Use and Disclosure of PHI

We may use PHI for our management, administration, data aggregation, analytics and legal obligations to the extent such use of PHI is permitted or required by the BA Agreement and not prohibited by law. We may use or disclose PHI on behalf of, or to provide services to, Covered Entities for purposes of fulfilling our service obligations to them, if such use or disclosure of PHI is permitted or required by the BA Agreement and would not violate the HIPAA Privacy Rule.

We use third party cloud service provider. HIPAA compliant region provided by cloud service provider is used for hosting and processing PHI shared by Covered Entity. In the event that PHI must be disclosed to any other subcontractors or agents, we ensure that those subcontractors or agents agrees to abide by the same restrictions and conditions that apply to us under the BA Agreement with respect to PHI, including the implementation of reasonable and appropriate safeguards.

We may also use PHI to report violations of law to appropriate federal and state authorities.

**Safeguards**

We use appropriate safeguards to prevent the use or disclosure of PHI other than as provided for in the BA Agreement. We have implemented administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that we create, receive, maintain, or transmit on behalf of a Covered Entity. Such safeguards include:

- Maintaining appropriate clearance procedures and providing supervision to assure that our workforce follows appropriate security procedures;
- Providing appropriate training for our staff to assure that our staff complies with our security policies;
- Making use of appropriate encryption when transmitting PHI over the Internet;
- Utilizing appropriate storage, backup, disposal and reuse procedures to protect PHI;
- Utilizing appropriate authentication and access controls to safeguard PHI;
- Utilizing appropriate security incident procedures and providing training to our staff sufficient to detect and analyze security incidents; and
- Maintaining a current contingency plan and emergency access plan in case of an emergency to assure that the PHI we hold on behalf of a Covered Entity is available when needed.

**Mitigation of Harm**

In the event of a use or disclosure of PHI that is in violation of the requirements of the BA agreement, we will mitigate, to the extent practicable, any harmful effect resulting from the violation. Such mitigation will include:

- Reporting any use or disclosure of PHI not provided for by the BA Agreement and any security incident of which we become aware to the Covered Entity; and
- Documenting such disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request for an accounting of disclosure of PHI in accordance with HIPAA.

**Access to PHI**

As provided in the BA Agreement, we will make available to Covered Entities, information necessary for Covered Entity to give individuals their rights of access, amendment, and accounting in accordance with HIPAA regulations.

Upon request, we will make our internal practices, and records including policies and procedures, relating to the use and disclosure of PHI received from, or created or received

by the BA on behalf of a Covered Entity available to the Covered Entity or the Secretary of the U.S. Department of Health and Human Services for the purpose of determining compliance with the terms of the BA Agreement and HIPAA regulations.