GENOMIC LIFE

Security & Privacy. It's in our DNA.

At Genomic Life, security, privacy, consent, and robust safeguards are at the core of everything we do; they are foundational elements of who we are and how we operate — truly a part of our corporate DNA.

INTEGRITY

We Do Not Sell Data

Integrity is very important in everything we do. While we should all acknowledge that no one in today's world can guarantee perfect security against data theft, our team of professionals work diligently each and every day to keep your information safe and secure. Rest assured, **we do not sell client or member data.**

SAFEGUARDS

3rd Party Risk Management

We are strongly dedicated to protecting the security and privacy of our clients and members. Genomic Life rigorously monitors, reviews, and manages third-party relationships and risks, ensuring that our partners adhere to the highest standards of data protection and compliance. **We believe no one should be able to share your data without your consent.**

GOVERNANCE

Compliance with HIPAA Security & Privacy Regulations

Our HIPAA-compliant platform strictly follows security and privacy regulations and has additional safeguards to protect your data, ensuring trust and transparency for our clients and members.

Those measures include maintaining certifications (HITRUST, NIST CSF, SOC 2), performing frequent audits, and actively monitoring third-party relationships to prioritize security and privacy in our operations.

CLINICAL STANDARDS

Medical-grade Partner Network

We carefully select our medical-grade partners from the clinical and healthcare service sectors who are HIPAA-covered entities, and we negotiate BAAs. This ensures that you not only gain access to industry-leading medical-grade offerings, but also have access to organizations who uphold stringent security and privacy standards.

TRANSPARENCY

Trust & Verify

We are committed to transparency and open communication. If you have questions, please contact us; we are happy to demonstrate our integrity and dedication to our clients and members.

Helpful definitions of terms and acronyms can be found on the following page.

Have questions? Visit genomiclife.com/contact or call (844) 694-3666

GENOMIC LIFE

Helpful Definitions

We gathered helpful definitions about concepts on the previous page. We hope these insights support you as you navigate through the material.

BA (Business Associate): A BA is a vendor serving a HIPAA Covered Entity and during the provision of services, the BA will receive individually identifiable health information (like enrollment information from a health plan). Since HITECH amended HIPAA, Business Associates are subject to certain provisions of HIPAA by law.

BAA (Business Associate Agreement): A Business Associate Agreement (BAA) is a legally binding contract that defines the responsibilities and safeguards that a business associate must maintain when handling protected health information (PHI) on behalf of a covered entity.

HIPAA (Health Insurance Portability and Accountability Act): The Health Insurance Portability and Accountability Act (HIPAA) is a U.S. federal law enacted in 1996 aimed at safeguarding the privacy and security of individuals' health information. HIPAA sets standards for the protection of electronic health information and ensures that organizations maintain the confidentiality, integrity, and availability of sensitive health data.

HIPAA Covered Entity: A HIPAA covered entity includes healthcare providers, health plans, and healthcare clearinghouses that electronically create, receive, maintain, or transmit protected health information (PHI). These entities are required to comply with HIPAA regulations to protect the privacy and security of patient medical records. Compliance with HIPAA enhances trust and supports partnerships by ensuring that sensitive health information is managed responsibly and in accordance with legal standards.

HITRUST r2 Certification: The HITRUST r2 Certification is a comprehensive framework designed to assess and certify the effectiveness of an organization's data protection and cybersecurity practices. It provides a standardized approach for demonstrating compliance with industry regulations, frameworks, and best practices, ensuring that organizations effectively safeguard sensitive information.

NIST Cybersecurity Framework (CSF): The NIST Cybersecurity Framework (CSF) is a voluntary framework that provides guidelines and best practices for organizations to manage and reduce cybersecurity risks. It emphasizes enhancing organizational resilience through effective risk management strategies, enabling entities to better protect their information systems and respond to incidents.

SOC 2 Type II Compliance: SOC 2 Type II is an auditing standard that evaluates an organization's controls related to security, availability, processing integrity, confidentiality, and privacy over a specified period. SOC 2 Type II compliance indicates that the organization has consistently adhered to its stated controls and practices related to these critical areas, signifying a strong commitment to maintaining high standards of data security and privacy.