**Genomic Privacy and Data Protection Policy (GPDP Policy)**

**Version: 1.0**

**Effective Date: 10/22/2025**

**Approved By: Executive Compliance Officer Name Keitavius Alexander**

**Policy Owner: Chief Compliance & Privacy Officer**

**Last Reviewed: 10/22/2025**

**Table of Contents**

**1. Executive Summary**

**2. Purpose**

**3. Scope**

**4. Key Terms**

**5. Roles and Responsibilities**

**6. Collection and Consent**

**7. Data Classification**

**8. Access Control Framework**

**9. Security and Technical Controls**

**10. Data Sharing and Cross-Border Transfers**

**11. Incident Response**

**12. Audit and Monitoring**

**13. Training and Awareness**

**14. Retention and Disposal**

**15. Policy Review and Updates**

**16. Regulatory and Framework Alignment**

**17. Enforcement**

**1. Executive Summary**

The Genomic Privacy and Data Protection Policy (GPDP) establishes the framework for the ethical, secure, and compliant handling of human specimens and genomic data. It governs how biological samples and their derived genetic information are collected, processed, and stored in accordance with HIPAA, GDPR, NIST 800-53, NIST Privacy Framework, and ISO 27001/27701.

This policy embodies the principles of Zero Trust Architecture, Least Privilege Access, and Data Minimization while ensuring transparency and informed consent. The GPDP safeguards individual privacy, ensures research integrity, and upholds global compliance standards.

**2. Purpose**

The purpose of this policy is to ensure that all genomic and biological specimens, and any data derived from them, are handled in an ethical, secure, and compliant manner. This includes the prevention of unauthorized access, misuse, or disclosure of genomic data, and the promotion of accountability and privacy throughout the data lifecycle.

**3. Scope**

This policy applies to:

• All employees, researchers, contractors, vendors, and affiliated facilities engaged in the collection, analysis, or storage of biological or genomic data.

• Third-party data processors and external collaborators handling genomic data on behalf of the organization.

• All systems, networks, laboratories, databases, and cloud environments where genomic data or specimens are processed or stored.

• Cross-border transfers and international research partnerships that involve genetic or biological materials.

**4. Key Terms**

• Specimen: Biological material derived from a human (e.g., tissue, saliva, blood, or hair) used for testing, sequencing, or research.

• Genetic Data: Information obtained from DNA, RNA, or other biological samples that can reveal hereditary or health-related details.

• PII (Personally Identifiable Information): Any information that can directly or indirectly identify an individual (e.g., name, ID number, genetic sequence).

• Chain of Custody: The documented and verifiable process of tracking a specimen from collection to disposal, ensuring integrity and traceability.

• Zero Trust: A cybersecurity principle requiring continuous verification of user identity and access requests regardless of network location.

• Least Privilege: Granting users only the minimal access required to perform their job functions.

• De-identification: The removal or alteration of identifying information from genomic data to prevent re-identification of the subject.

**5. Roles and Responsibilities**

• Chief Compliance & Privacy Officer (CCPO): Oversees implementation, ensures legal adherence, and reviews audit outcomes.

• Data Protection Officer (DPO): Manages HIPAA, GDPR, and Privacy Impact Assessment (PIA) compliance.

• Lab Managers and Researchers: Maintain specimen integrity, chain of custody, and enforce data handling standards.

• IT and Security Teams: Implement encryption, access control, and monitoring in alignment with NIST and ISO frameworks.

• Third-Party Vendors: Must demonstrate compliance with equivalent privacy and security controls before engaging in data handling.

6. Collection and Consent

• Informed consent must be obtained and recorded prior to any collection or use of human specimens.

• Participants must be clearly informed about the purpose, duration, and intended use of their data.

• Opt-out mechanisms shall be provided for non-essential or secondary data use.

• Consent must meet requirements set forth by HIPAA, GDPR, and 45 CFR 46 (Common Rule).

7. Data Classification

Genomic data will be classified into three sensitivity tiers:

• Tier 1 – Restricted: Identifiable genomic or medical data linked to personal identifiers.

• Tier 2 – Confidential: De-identified or pseudonymized genomic data used internally.

• Tier 3 – Public: Fully anonymized and aggregated data approved for publication or research dissemination.

Each tier has corresponding access, storage, and retention requirements, enforced by the Compliance Office.

**8. Access Control Framework**

• Based on Zero Trust Architecture (ZTA) and Role-Based Access Control (RBAC) principles.

• All users are governed under Least Privilege protocols.

• Multi-Factor Authentication (MFA) required for all genomic data access points.

• Access logs must be maintained, reviewed monthly, and stored securely.

• Quarterly access reviews are mandatory for all privileged accounts.

**9. Security and Technical Controls**

• Encryption:

• Genomic and specimen data must be encrypted both in transit (TLS 1.3) and at rest (AES-256).

• Physical Security:

• Laboratories must employ restricted access zones and temperature-controlled environments.

• Specimens must be stored in tamper-proof containers and transported securely.

• Chain of Custody:

• All specimens are to be labeled with barcodes or RFID tags for traceability.

• Network and Endpoint Security:

• Firewalls, continuous monitoring, and vulnerability assessments required.

• Data Loss Prevention (DLP):

• Automated systems will detect and block unauthorized data transfer or sharing.

**10. Data Sharing and Cross-Border Transfers**

• Cross-border transfers require explicit DPO approval and GDPR-compliant safeguards (Standard Contractual Clauses).

• All external data sharing requires a signed Business Associate Agreement (BAA) or equivalent data-sharing contract.

• De-identified datasets must be used wherever possible for research collaboration.

• Recipients must maintain protection measures equivalent to the originating organization’s standards.

**11. Incident Response**

• All security or privacy incidents must be reported within 24 hours to the CCPO and DPO.

• Notifications shall follow HIPAA Breach Notification Rules (45 CFR §§164.400-414) and GDPR Article 33.

• A root cause analysis (RCA) must be conducted within 72 hours.

• Corrective actions and retraining procedures must follow every confirmed incident.

**12. Audit and Monitoring**

• Internal audits conducted quarterly; third-party compliance audits annually.

• Continuous monitoring systems will track data access, environmental conditions, and security events.

• Non-compliance triggers corrective action, including access revocation or disciplinary measures.

**13. Training and Awareness**

• Annual training on data privacy, ethical research, and genomic data handling is mandatory.

• Specialized sessions for lab personnel on bioethics and specimen security.

• New hires must complete training prior to obtaining access credentials.

**14. Retention and Disposal**

• Retention periods must align with research and legal requirements.

• Upon expiration or consent withdrawal, data and specimens must be securely destroyed or anonymized.

• Chain-of-custody and destruction records retained for at least seven years post-disposal.

**15. Policy Review and Updates**

• This policy is reviewed annually or following any major legal or technological developments.

• Updates require approval from the Compliance Committee and notification to all stakeholders.

• Revision logs will be maintained to track policy evolution and accountability.

**16. Regulatory and Framework Alignment**

This policy aligns with the following international frameworks and regulations:

• HIPAA (45 CFR Parts 160 & 164): Ensures privacy and security of identifiable genomic data.

• GDPR (Articles 9, 32–34): Classifies genetic data as a sensitive category and mandates strict protection.

• NIST 800-53 Rev. 5: Defines access, privacy, and accountability controls for sensitive data systems.

• NIST Privacy Framework (2020): Integrates privacy risk management with organizational controls.

• ISO 27001 / 27701: Establishes standards for information security and privacy management systems.

• OECD Guidelines on Human Biobanks and Genetic Research Databases: Promotes transparency, governance, and ethical consent mechanisms.

• 21 CFR Part 11 (FDA): Regulates the use of electronic records and digital specimen documentation in clinical research.

**17. Enforcement**

Violations of this policy will result in:

• Disciplinary action, including suspension or termination.

• Revocation of data or system access rights.

• Potential legal or financial penalties based on jurisdictional law.

The organization reserves the right to investigate any suspected breach of this policy and to cooperate with regulatory authorities as required