Data Management Policy

MolecularMatch has procedures to create and maintain retrievable exact copies of electronic protected health information (ePHI). This policy, and associated procedures for testing and restoring from backup data, has been subcontracted to a third-party, HIPAA compliant vendor (PaaS Subcontractor). We have verified that their policies and procedures meet or exceed our standards and those of HIPAA and the HITRUST Common Security Framework. As such, we have assurances that that complete, accurate, retrievable, and tested backups are available for all systems hosted by the PaaS Subcontractor.

Proof of such due diligence is kept by the Security Officer.

To protect the confidentiality, integrity, and availability of ePHI, both for ourselves and by our PaaS Subcontractor, our PaaS Subcontractor executes daily backups to assure that data remains available when needed and in case of disaster recovery.

Violation of this policy and its procedures by workforce members may result in corrective disciplinary action, up to and including termination of employment. Violation of this policy by our PaaS Subcontractor will result in legal and punatitive action.

Applicable Standards from the HITRUST Common Security Framework

- 01.v - Information Access Restriction

Applicable Standards from the HIPAA Security Rule

- 164.308(a)(7)(ii)(A) - Data Backup Plan
- 164.310(d)(2)(iii) - Accountability
- 164.310(d)(2)(iv) - Data Backup and Storage

Backup Policy and Procedures

1. PaaS Subcontractor will perform daily snapshot backups of all systems that process, store, or transmit ePHI.
2. PaaS Subcontractor's Dev Ops Team is designated to be in charge of backups. Our Security Officer or delegated internal workforce member shall make monthly verifications that such backups exist and retain their original integrity.

3. The PaaS Subcontractor's Dev Ops Team members are trained and assigned to complete backups and manage the backup media.
4. Backups are documented as follows:
    - Name of the system
    - Date & time of backup
    - Where backup is stored (or to whom it was provided)
5. Backups are always securely encrypted in a manner that protects them from loss or environmental damage.
6. Backups are tested and documented that files have been completely and accurately restored from the backup media.