Data Integrity Policy

MolecularMatch takes data integrity very seriously. As stewards of our Customers data, we strive to assure data is protected from unauthorized access and that it is available when needed. The following policy drives many of our procedures and technical settings in support of this aim.

This policy, and associated procedures for Data Integrity, has been subcontracted in part to a third-party, Platform as a Service, 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 proper Data Integrity tools and policies to proactively track and retroactively investigate any violation of data integrity are used.

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

Applicable Standards from the HITRUST Common Security Framework

- 10.b - Input Data Validation

Applicable Standards from the HIPAA Security Rule

- 164.308(a)(8) - Evaluation

Data integrity Policy

Production Systems that create, receive, store, or transmit customer data (hereafter "Production Systems") must follow the following guidelines.

Disabling non-essential services

PaaS Subcontractor is responsible for:

- Disabling all non-essential and unrequired softward and services that are not vital to the business purpose or function of Production Systems.

Monitoring Log-in Attempts

See Auditing Policy

Prevention of malware on Production Systems

We are responsible for:

- Using Production Systems only for business needs.

PaaS Subcontractor is responsible for:

- Scanning all Production Systems with OSSEC every 2 hours and at reboot to ensure no malware is present.
- Evaluating and removing all detected malware.
- Using Production Systems only for business needs.

Patch Management

We are responsible for:

- Making sure application code and associated systems are kept up to date at all times (e.g. web server and database).
- Testing all new versions to ensure they do not violate any policy including this one.
- Subscribing to appropriate resources to ensure responsible workforce members (administractors and development operations) remain up-to-date on all responsible software on Production Systems.

PaaS Subcontractor is responsible for:

- Making sure patches to application and OS system versions are kept up to date at all times.
- Testing all new versions to ensure they do not violate any policy including this one.
- Subscribing to appropriate resources to ensure responsible workforce members (administractors and development operations) remain up-to-date on all responsible software on Production Systems.

Intrusion Detection and Vulnerability Scanning

- *See the Intrusion Detection Policy.*
- *See the Vulnerability Scanning Policy.*

Production System Security

We are responsible for:

- Managing and maintaing the application and associated products, including related security.
- Keeping the software and related systems up to date, including production system architecture diagrams.
- Controlling access to appropriate indviduals and role-based access to the system. Administractive access to the system must be controlled using two-factor authentication.

PaaS Subcontractor is responsible for:

- Managing and maintaing the servers environments, network, and related security.
- Keeping up-to-date system lists and architecture diagrams for all Production environments.
- Controlling access to Production Systems using centralized tools and two-factor authentication.

Production Data Security

Both parties must work to reduce the risk of compromise to Production Data.

We are responsible for:

- Reviewing controls designed to protect Production Data from improper alteration or destruction.

PaaS Subcontractor is responsible for:

- Implementing and reviewing controls designed to protect Production Data from improper alteration or destruction.
- Ensuring that Production Data is stored in a manner that supports user access logs and automated monitoring for potential security incidents.
- Ensure Production Data is segmented and only accessible to the appropriate authorized customer.
- Encrypting all Production Data at rest by using encrypted volumes.

Transmission Security

We are responsible for:

- Encrypting all data in transmission from end-to-end.
- Protecting encryption keys and machines that generate keys from unauthorized access.
- Providing a mechanism to assure person or system sending or receiving data is authorized to send and save data.

PaaS Subcontractor is responsible for:

- Encrypting all data in transmission from end-to-end. Encryption is not terminated at the network end point but is carried through to the application.
- Protecting encryption keys and machines that generate keys from unauthorized access.
- Limiting duration of use of encryption keys to one year before they must be regenerated.
- Providing a mechanism to assure person or system sending or receiving data is authorized to send and save data.
- Logging all transmissions of Production Data access. These logs must be available for audit.