System Access Policy

Access to MolecularMatch systems and applications are controlled and limited regardless of user, including but not limited to workforce members, volunteers, business associates, contracted providers, consultants, and any other entity. Access is only given on an as needed basis as approved by the Security Officer. All users are responsible for reporting an incident of unauthorized access of the organization's information systems. These safeguards have been established to address the HIPAA Security regulations including the following:

Applicable Standards from the HITRUST Common Security Framework

- 01.d - User Password Management
- 01.f - Password Use
- 01.r - Password Management System
- 01.a - Access Control Policy
- 01.b - User Registration
- 01.h - Clear Desk and Clear Screen Policy
- 01.j - User Authentication for External Connections
- 01.q - User Identification and Authentication
- 01.v - Information Access Restriction
- 02.i - Removal of Access Rights
- 06.e - Prevention of Misuse of Information Assets

Applicable Standards from the HIPAA Security Rule

- 164.308a4iiC Access Establishment and Modification
- 164.308a3iiB Workforce Clearance Procedures
- 164.308a4iiB Access Authorization
- 164.312d Person or Entity Authentication
- 164.312a2i Unique User Identification
- 164.308a5iiD Password Management
- 164.312a2iii Automatic Logoff
- 164.310b Workstation Use
- 164.310c Workstation Security
- 164.308a3iiC Termination Procedures

Access Establishment and Modification

- Requests for access to a system or applications must be made formally to the Security Officer or whomever such oversight is delegated to (e.g. VP of Engineering).
- Access will only be granted after receipt, review, and approval by the Security Officer;
- All requests for access are retained for at least six years for future reference.
- All access to a system or service is reviewed and updated on an annual basis to assure proper authorizations are in place commiserate with job functions. Please use the linked form to fill out a request. form.
- Any workforce member can request change of access using the same form and making appropriate notifications. The security officer will then approve or deny and make appropriate documentation as a result. form.
- Access to the web application is limited to current users and administrators. Administrators require prior approval and two-factor authentication to gain access. Current users of the system can not access anything outside of their own account.
- For access to where production data is stored, including potential ePHI, approval needs to be requested by the above form. Access to these systems is controlled using centralized user management and authentication as implemented by our third-party, Platform as a Service (PaaS) Subcontractor. All authentication requests utilize either two factor authentication using mobile devices as the second factor or secured SSL certificates stored on approved workstations.
- Temporary accounts are not used unless absolutely necessary for business purposes.
    - Accounts are reviewed every 90 days to assure temporary accounts are not left unnecessarily.
    - Accounts that are inactive for over 90 days are removed.
- In the case of non-personal information, such as generic educational content, identification and authentication may not be required. This is the responsibility of either Security Officer or Privacy Officer to define.
- Privileged users must first access systems using standard, unique user accounts before switching to privileged users and performing privileged tasks.
- All application-to-application communication using service accounts is restricted and not permitted unless absolutely needed. Automated tools are used to limit account access across applications and systems.
- Generic accounts are not allowed on any production environment.
- Access to the production environment where ePHI may reside is granted through encrypted, VPN tunnels.
    - VPN utilizes AES 256 bit encryption.
- In cases of increased risk or known attempted unauthorized access, immediate steps are taken by the Security and Privacy Officer to limit access and reduce risk of unauthorized access. Where these systems are hosted by a third-party, PaaS vendor it is their responsbility.

- Direct system to system, system to application, and application to application authentication and authorization are limited and controlled to restrict access.

Workforce Clearance Procedures

- The level of security assigned to a user to the organization's information systems is based on the minimum necessary amount of data access required to carry out legitimate job responsibilities assigned to a user's job classification and/or to a user needing access to carry out treatment, payment, or healthcare operations.
- All access requests are treated on a "least-access principle".
- We maintain a minimum necessary approach to access to Customer data. As such, most if not all all workforce members and subcontractors do not readily have access to any ePHI.

Access Authorization

- Role based access categories for each system and application must be pre-approved by the Security Officer when used.
- The third-party PaaS Subcontractor utilizes hardware and software firewalls to segment data, prevent unauthorized access, and monitor traffic for denial of service attacks.

Person or Entity Authentication

- Each workforce member has and uses a unique user ID and password that identifies them as the user of the information system. This is true whether it is administrative access to the web application or privledged access to a production system where data is stored
- Each Customer and Subcontractor has and uses a unique user ID and password that identifies them as the user of the information system.

Unique User Identification

- Access to any system or application is controlled by requiring unique User Login ID's and passwords for each individual user and developer.
- Password requirements mandate strong password controls (see below).
- Passwords are not displayed at any time and are not transmitted or stored in plain text.
- Default accounts on all production systems, including root, are disabled.
- Shared accounts are not allowed within any system or network.

Automatic Logoff

- Users are required to make information systems inaccessible by any other individual when unattended by the users (ex. by using a password protected screen saver or logging off the system).
- Information systems automatically log users off the systems after 10 minutes of inactivity.
- The Security Officer pre-approves exceptions to automatic log off requirements.

Employee Equipment Use

- All workstations purchased by the company are the property of the company and are distributed to users by the company.
- Workstations may only be accessed and utilized by authorized workforce members to complete assigned job/contract responsibilities.
- All workforce members are required to monitor workstations and report unauthorized users and/or unauthorized attempts to access systems/applications as per the System Access Policy.
- Transmitted messages may not contain material that criticizes the organization, its providers, its employees, or others.
- Users may not misrepresent, obscure, suppress, or replace another user's identity in transmitted or stored messages.
- Workstation hard drives will be encrypted using Operating System level encryption.
- All workstations have firewalls enabled to prevent unauthorized access unless explicitly granted.
- At onboarding and offboarding, employees workstation is to be configured to system defaults.
- **Workstations may not be used**:
  - to engage in any activity that is illegal or is in violation of the policies.
  - to transmit, retrieve, or store any communications of a discriminatory or harassing nature or materials that are obscene or "X-rated". Harassment of any kind is prohibited. No messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes, sexual preference, or health condition shall be transmitted or maintained. No abusive, hostile, profane, or offensive language is to be transmitted through any of our organization's systems.
  - for any other purpose that is illegal, unethical, or against company policies or contrary to organization's best interests. Messages containing information related to a lawsuit or investigation may not be sent without prior approval.
  - for solicitation of non-company business or any use of the organization's information systems and applications for personal gain is prohibited.
- **Enforcement of Workstation Security Policies**
  - Report violations of this policy to the restricted area's department team leader, supervisor, manager, or director, or the Privacy Officer.

    - Workforce members in violation of this policy are subject to disciplinary action, up to and including termination.
    - Visitors in violation of this policy are subject to loss of vendor privileges and/or termination of services.

Employee Termination Procedures

- The Human Resources Department (or other designated department), users, and their supervisors are required to notify the Security Officer upon completion and/or termination of access needs and facilitating completion of the Termination Checklist.
- The Human Resources Department, users, and supervisors are required to notify the IS Help Desk to terminate a user's access rights if there is evidence or reason to believe the following (these incidents are also reported on an incident report and is filed with the Privacy Officer):
    - The user has been using their access rights inappropriately;
    - A user's password has been compromised (a new password may be provided to the user if the user is not identified as the individual compromising the original password);
    - An unauthorized individual is utilizing a user's User Login ID and password (a new password may be provided to the user if the user is not identified as providing the unauthorized individual with the User Login ID and password).
- The Security Officer will terminate users' access rights immediately upon notification.
- The Security Officer audits and may terminate access of users that have not logged into organization's information systems/applications for at least three months.
- Workstation will be reset to system default with all appropriate security setup performed.

Paper Records

We do not use paper records for any sensitive information. Use of paper for recording and storing sensitive data is against our policies. Paper records that are kept as part of an archiving process for various requests and record keeping do not contain sensitive information.

Password Management

- User IDs and passwords are used to control access to all systems and may not be disclosed to anyone for any reason.
- Users may not allow anyone, for any reason, to have access to any information system using another user's unique user Login ID and password.
- On all production systems and applications in our environment, password configurations are set to require that passwords are a minimum of 8 character length, 90 day password expiration, account lockout after 5 invalid attempts, password history of last 4 passwords remembered, and account lockout after 15 minutes of inactivity.

- All system and application passwords are hashed by concatenating the user's password and a random 256-bit salt value, generated on a per-user basis, and then applying SHA-256 to the value to create a password hash. The password hash and the salt are then stored in the backend database and are used for password validation on future user authentication attempts.
- Each information system automatically requires users to change passwords at a pre-determined interval as determined by the organization, based on the criticality and sensitivity of the ePHI contained within the network, system, application, and/or database.
- Passwords are inactivated immediately upon an employee’s termination (refer to the termination procedures in this policy).
- All default system, application, and Partner passwords are changed before deployment to production.
- All passwords used in configuration scripts are secured and encrypted.
- If a user believes their user ID has been compromised, they are required to immediately report the incident to the Security Office.

PaaS Access to Systems

Access to the PaaS hosted secure system is via VPN connections. This access is only to our specific systems. These connections are setup upon initial engagement with the PaaS Subcontractor. These connections are secured and encrypted and the only method to connect to the vendor's PaaS hosted systems.

In the case of data migration, PaaS Subcontractor does, on a case by case basis, support importing/exporting data. In these cases SCP is used to assure all data is secured and encrypted in transit.

In the case of an investigation, PaaS Subcontractor will assist as needed including with law enforcement in forensics.