Roles Policy

MolecularMatch has a Security Officer [164.308(a)(2)] and Privacy Officer [164.308(a)(2)] appointed to assist in maintaining and enforcing safeguards towards compliance. The responsibilities associated with these roles are outlined below.

Applicable Standards from the HITRUST Common Security Framework

- 06.d - Data Protection and Privacy of Covered Information
- 06.g - Compliance with Security Policies and Standards

Applicable Standards from the HIPAA Security Rule

- 164.308(a)(2) - Assigned Security Responsibility
- 164.308(a)(5)(i) - Security Awareness and Training

Privacy Officer

The Privacy Officer is responsible for assisting with compliance and security training for workforce members, assuring the organization remains in compliance with evolving compliance rules, and helping the Security Officer in his responsibilities. Additionally, the Privacy Officer is the liason and oversight around compliance when dealing with external parties.

1. Provide annual training to all workforce members of established policies and procedures as necessary to carry out their job functions, and document the training provided.
2. Assist in the administration and oversight of business associate agreements.
3. Manage relationships with customers and partners as those relationships affect security and compliance of ePHI.
4. Maintain a program promoting workforce members to report non-compliance with policies and procedures.
    1. Promptly, properly, and consistently investigate and address reported violations and takes steps to prevent recurrence.
    2. Apply consistent and appropriate sanctions against workforce members who fail to comply with security policies and procedures.
    3. Mitigate, with assistance from the Security Officer to the extent practicable, any harmful effect known to the company of a use or disclosure of ePHI in violation of

the policies and procedures, even if effect is the result of actions of our business associates, customers, and/or partners.

5. Assist Security Officer as outlined in policies.

The current Privacy Officer is Collin Brack (cbrack@molecularmatch.com).

Workforce Training Responsibilities

1. The Privacy Officer facilitates the training of all workforce members as follows:
    1. New workforce members within their first month of employment;
    2. Existing workforce members annually;
    3. Existing workforce members whose functions are affected by a material change in the policies and procedures, within a month after the material change becomes effective;
    4. Existing workforce members as needed due to changes in security and risk posture.
2. The Security Officer or designee maintains documentation of the training session materials and attendees for a minimum of six years.
3. The training session focuses on, but is not limited to, the following subjects defined in our security policies and procedures:
    1. HIPAA Privacy, Security, and Breach notification rules;
    2. HITRUST Common Security Framework;
    3. NIST Security Rules;
    4. Risk Management procedures and documentation;
    5. Auditing. All users should expect their access and activities to be monitored;
    6. Workstations may only be used to perform assigned job responsibilities;
    7. Users may not download software onto company workstations and/or systems without prior approval from the Security Officer;
    8. Users are required to report malicious software to the Security Officer immediately;
    9. Users are required to report unauthorized attempts, uses of, and theft of any system and/or workstation;
    10. Users are required to report unauthorized access to facilities;
    11. Users are required to report noted log-in discrepancies (i.e. application states users last log-in was on a date user was on vacation;
    12. Users may not alter ePHI maintained in a database, unless authorized to do so by a valid customer with permission of the Security Officer;
    13. Users are required to understand their role in the contingency plan;
    14. Users may not share their user names nor passwords with anyone;
    15. The requirements for users to create and change passwords;
    16. Users must set all applications that contain or transmit ePHI to automatically log

off after “X” minutes of inactivity;
17. Supervisors are required to report terminations of workforce members and other outside users;
18. Supervisors are required to report a change in a users title, role, department, and/or location;
19. Procedures to backup ePHI;
20. Procedures to move and record movement of hardware and electronic media containing ePHI;
21. Procedures to dispose of discs, CDs, hard drives, and other media containing ePHI;
22. Procedures to re-use electronic media containing ePHI;
23. SSH key and sensitive document encryption procedures.

Security Officer

The Security Officer is responsible for facilitating the training and supervision of all workforce members [164.308(a)(3)(ii)(A) and 164.308(a)(5)(ii)(A)], investigation and sanctioning of any workforce member that is in violation of any security policy and non-compliance with the security regulations [164.308(a)(1)(ii)(c)], and writing, implementing, and maintaining all polices, procedures, and documentation related to efforts toward security and compliance [164.316(a-b)].

The current Security Officer is Nick Tackes (ntackes@molecularmatch.com).

Organizational Responsibilities

The Security Officer, in collaboration with the Privacy Officer, is responsible for facilitating the development, implementation, and oversight of all activities pertaining to company efforts to be compliant with the HIPAA Security Regulations, HITRUST CSF, and any other security and compliance frameworks. The intent of the Security Officer Responsibilities is to maintain the confidentiality, integrity, and availability of ePHI. These organizational responsibilities include, but are not limited to the following:

1. Oversee and enforce all activities necessary to maintain compliance and verify the activities are in alignment with the requirements.
2. Help to establish and maintain written policies and procedures to comply with the Security rule. Maintain them for six years from the date of creation or date it was last in effect, whichever is later. (See **Policy Management Policy**)
3. Update policies and procedures as necessary and appropriate to maintain compliance. Maintain changes made for six years from the date of creation or date it was last in effect, whichever is later. (See **Policy Management Policy**)
4. Facilitate audits to validate compliance efforts throughout the organization including Risk

Assements. (See **Risk Management Policy** and **Auditing Policy**.

5. Document all activities and assessments completed to maintain compliance and maintains documentation for six years from the date of creation or date it was last in effect, whichever is later.
6. Provide copies of the policies and procedures to management, customers, and partners, and has them available to review by all other workforce members to which they apply. (See **Introduction**)
7. Annually, and as necessary, review and update documentation to respond to changes affecting the security and risk posture of ePHI stored, transmitted, or processed within the platform.
8. Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it may be accessed.
9. Reports security efforts and incidents to administration immediately upon discovery. Responsibilities in the case of a known ePHI breach are documented in the Our Breach Policy.
10. The Security Officer facilitates the communication of security updates and reminders to all workforce members to which it pertains. Examples of security updates and reminders include, but are not limited to:
    1. Latest malicious software or virus alerts;
    2. Requirement to report unauthorized attempts to access ePHI;
    3. Changes in creating or changing passwords;
    4. Additional security-focused training is provided to all workforce members by the Security Officer. This training includes, but is not limited to:
    5. Data backup plans;
    6. System auditing procedures;
    7. Redundancy procedures;
    8. Contingency plans;
    9. Virus protection;
    10. Patch management;
    11. Media Disposal and/or Re-use;
    12. Documentation requirements.

Supervision of Workforce Responsibilities

Although the Security Officer is responsible for implementing and overseeing all activities related to maintaining internal compliance, it is the responsibility of all workforce members (i.e. team leaders, supervisors, managers, directors, co-workers, etc.) to supervise all workforce members and any other user of our systems, applications, servers, workstations, etc. that contain ePHI.

1. Monitor workstations and applications for unauthorized use, tampering, theft, or violations. Report non-compliance according to the **Incident Response policy**.
2. Assist the Security and Privacy Officers to ensure appropriate role-based access is provided to all users.
3. Take all reasonable steps to hire, retain, and promote workforce members and provide access to users who comply with the security regulation and our security policies and procedures.

Sanctions of Workforce Responsibilities

All workforce members should report non-compliance of our policies and procedures to the Privacy Officer or other individual as assigned by the Privacy Officer. Individuals that report violations in good faith will not be subject to intimidation, threats, coercion, discrimination, or any other retaliatory action as a consequence.

1. The Privacy Officer shall promptly facilitate a thorough investigation of all reported violations of our security policies and procedures. The Privacy Officer may request assistance from others as needed. The Privacy Officer will:
    1. Complete an audit trail/log to identify and verify the violation and sequence of events.
    2. Interview any individual that may be aware of or involved in the incident.
    3. All individuals are required to cooperate with the investigation process and provide factual information to those conducting the investigation.
    4. Provide individuals suspected of non-compliance of the Security rule and/or our policies and procedures the opportunity to explain their actions.
    5. Thoroughly document the investigation as the investigation occurs.
2. Violation of any security policy or procedure by workforce members may result in corrective disciplinary action, up to and including termination of employment. Violation of this policy and procedures by others, including business associates, customers, and partners may result in termination of the relationship and/or associated privileges. Violation may also result in civil and criminal penalties as determined by federal and state laws and regulations.
    1. A violation resulting in a breach of confidentiality (i.e. release of PHI to an unauthorized individual), change of the integrity of any ePHI, or inability to access any ePHI by other users, requires immediate termination of the workforce member.
3. The Security Officer shall facilitate taking appropriate steps to prevent recurrence of the violation (when possible and feasible).
4. In the case of an insider threat, the Security Officer and Privacy Officer shall setup a team to investigate and mitigate the risk of insider malicious activity. Workforce members are encouraged to come forward with information about insider threats and can do so

anonymously.

5. The Privacy Officer shall maintain all documentation of the investigation, sanctions provided, and actions taken to prevent reoccurrence for a minimum of six years after the conclusion of the investigation.