Third Party Policy

MolecularMatch makes every effort to assure all thirdy party organizations are compliant and do not compromise the integrity, security, and privacy of our company or production data. Third Parties include Customers, Partners, Subcontractors, and Contracted Developers.

Applicable Standards from the HITRUST Common Security Framework

- 05.i - Identification of Risks Related to External Parties
- 05.k - Addressing Security in Third Party Agreements
- 09.e - Service Delivery
- 09.f - Monitoring and Review of Third Party Services
- 09.g - Managing Changes to Third Party Services
- 10.1 - Outsourced Software Development

Applicable Standards from the HIPAA Security Rule

- 164.314(a)(1)(i) - Business Associate Contracts or Other Arrangements

Policies to Assure 3rd Parties Remain Compliant

1. The following steps are required before third parties are granted access to any systems:
    - Due diligence with the 3rd party;
    - Controls implemented to maintain compliance;
    - Written agreements, with appropriate security requirements, are executed.
2. All connections and data in transit between our Platform and 3rd parties are encrypted end-to-end.
3. Access granted to external parties is limited to the minimum necessary and granted only for the duration required.
4. A standard business associate agreement with Customers and Partners is defined and includes the required security controls in accordance with the organization’s security policies. Additionally, responsibility is assigned in these agreements.
5. Service Level Agreements (SLAs) are put in place with Subcontractors with an agreed service arrangement addressing liability, service definitions, security controls, and aspects of services management.

    - Monitoring tools are used to regularly evaluate Subcontractors against relevant SLAs.

6. Third parties are unable to make changes to any infrastructure piece without explicit permission. Additionally, no Customer or Partner has access outside of their own environment, meaning they cannot access, modify, or delete anything related to other 3rd parties.
7. Whenever outsourced development is utilized, all changes to production systems will be approved and implemented by workforce members only. All outsourced development requires a formal contract.
8. All current Partners and Subcontractors are maintained and annually reviewed.
9. All current Partners and Subcontractors are assessed for security and compliance considerations.
10. Regular review is conducted as required by SLAs to assure security and compliance. These reviews include reports, audit trails, security events, operational issues, failures and disruptions, and identified issues. Anything found is investigated and resolved in a reasonable and timely manner.
11. Any changes to Partner and Subcontractor services and systems are reviewed before implementation.