# Risk Management Policy

This policy establishes the scope, objectives, and procedures of MolecularMatch's information security risk management process. The risk management process is intended to support and protect the organization and its ability to fulfill its mission.

## Applicable Standards from the HITRUST Common Security Framework

- 03.a - Risk Management Program Development
- 03.b - Performing Risk Assessments
- 03.c - Risk Mitigation

## Applicable Standards from the HIPAA Security Rule

- 164.308(a)(1)(ii)(A) – HIPAA Security Rule Risk Analysis
- 164.308(a)(1)(ii)(B) – HIPAA Security Rule Risk Management
- 164.308(a)(8) – HIPAA Security Rule Evaluation

## Risk Management Policies

1. It is our policy to conduct thorough and timely risk assessments of the potential threats and vulnerabilities to the confidentiality, integrity, and availability of all important electronic information including electronic protected health information (ePHI) as well as other confidential and proprietary electronic information. Collectively this information is stored, transmitted, and processed on behalf of direct and indirect customers. To that end, we develop strategies to efficiently and effectively mitigate the risks identified in the assessment process as an integral part of our information security program.
2. Risk analysis and risk management are recognized as important components of our corporate compliance program and information security program in accordance with the Risk Analysis and Risk Management implementation specifications within the Security Management standard and the evaluation standards set forth in the HIPAA Security Rule, 45 CFR 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(1)(i), and 164.308(a)(8).
3. Risk assessments are done throughout each product life cycle:
    1. Before the integration of major updates to the system and before changes are made to physical safeguards or hosting environments. *Note: These changes do*

    *not include routine updates to existing systems, deployments of new systems created based on previously configured systems, or new code developed for routine operations and management of the system.*
    2. While making changes to the system that introduce new, untested configurations.
    3. In response to environmental or operational changes affecting the security of ePHI.
4. We implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to:
    1. Ensure the confidentiality, integrity, and availability of all ePHI received, maintained, processed, and/or transmitted for its Customers;
    2. Protect against any reasonably anticipated threats or hazards to the security or integrity of received ePHI;
    3. Protect against any reasonably anticipated uses or disclosures of ePHI that are not permitted or required; and
    4. Ensure compliance by all workforce members.
5. Any risk remaining (residual) after other risk controls have been applied, requires sign off by the Senior Management and the Security Officer.
6. All workforce members are expected to fully cooperate with all persons charged with doing risk management work, including contractors and audit personnel. Any workforce member that violates this policy will be subject to disciplinary action based on the severity of the violation according to our policies, which is outlined in the **Roles Policy**.
7. The implementation, execution, and maintenance of the information security risk analysis and risk management process is the responsibility of the Security Officer (or other designated employee), and the identified Risk Management Team.
8. All risk management efforts, including decisions made on what controls to put in place as well as those to not put into place, are documented and the documentation is maintained for six years.

# Risk Management Procedures

**Risk Assessment**: The intent of completing a risk assessment is to determine potential threats and vulnerabilities and the likelihood and impact should they occur. The output of this process helps to identify appropriate controls for reducing or eliminating risk.

- **Step 1.** System Characterization
    - The first step in assessing risk is to define the scope of the effort. To do this, identify where ePHI is received, maintained, processed, or transmitted. Using information-gathering techniques, we identify our boundaries relative to our partners and subcontractors.
    - Output – Characterization of the Platform system assessed, a good picture of the Platform environment, and delineation of Platform boundaries.
- **Step 2.** Threat Identification

    - Identify and document potential threats to successfully exercise a particular vulnerability. All potential threat-sources through the review of historical incidents and data from intelligence agencies, the government, etc., to help generate a list of potential threats.
    - Output – A threat list containing a list of threat-sources that could exploit system vulnerabilities.
- **Step 3.** Vulnerability Identification
    - Develop a list of technical and non-technical vulnerabilities that could be exploited or triggered by potential threat-sources. Vulnerabilities can range from incomplete or conflicting policies that govern computer usage to insufficient safeguards to protect facilities that house computer equipment to any number of software, hardware, or other deficiencies that comprise an organization's computer network.
    - Output – A list of the system vulnerabilities (observations) that could be exercised by potential threat-sources.
- **Step 4.** Control Analysis
    - Document and assess the effectiveness of technical and non-technical controls that have been or will be implemented to minimize or eliminate the likelihood / probability of a threat-source exploiting a vulnerability.
    - Output – List of current or planned controls (policies, procedures, training, technical mechanisms, insurance, etc.) used to mitigate the likelihood of a vulnerability being exercised and reduce the impact of such an adverse event.
- **Step 5.** Likelihood Determination
    - Determine the overall likelihood rating that indicates the probability that a vulnerability could be exploited by a threat-source given the existing or planned security controls.
    - Output – Likelihood rating of low (.1), medium (.5), or high (1). Refer to the NIST SP 800-30 definitions of low, medium, and high.
- **Step 6.** Impact Analysis
    - Determine the level of adverse impact that would result from a threat successfully exploiting a vulnerability. Factors of the data and systems to consider should include the importance to our mission; sensitivity and criticality (value or importance); costs associated; loss of confidentiality, integrity, and availability of systems and data.
    - Output – Magnitude of impact rating of low (10), medium (50), or high (100). Refer to the NIST SP 800-30 definitions of low, medium, and high.
- **Step 7.** Risk Determination
    - Establish a risk level. By multiplying the ratings from the likelihood determination and impact analysis, a risk level is determined. This represents the degree or level of risk to which an IT system, facility, or procedure might be exposed if a given vulnerability were exercised. The risk rating also presents actions that Senior Management must take for each risk level.
    - Output – Risk level of low (1-10), medium (>10-50) or high (>50-100). Refer to the

NIST SP 800-30 definitions of low, medium, and high.

- **Step 8.** Control Recommendations
    - Identify controls that could reduce or eliminate the identified risks, as appropriate to the organization's operations to an acceptable level. Factors to consider when developing controls may include effectiveness of recommended options (i.e., system compatibility), legislation and regulation, organizational policy, operational impact, and safety and reliability. Control recommendations provide input to the risk mitigation process, during which the recommended procedural and technical security controls are evaluated, prioritized, and implemented.
    - Output – Recommendation of control(s) and alternative solutions to mitigate risk.
- **Step 9.** Results Documentation
    - Results of the risk assessment are documented in an official report, spreadsheet, or briefing and provided to Senior Management to make decisions on policy, procedure, budget, operational, and/or technical changes.
    - Output – A risk assessment report that describes the threats and vulnerabilities, measures the risk, and provides recommendations for control implementation.

**Risk Mitigation**: Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the Risk Assessment process to ensure the confidentiality, integrity, and availability of customer ePHI. Determination of appropriate controls to reduce risk is dependent upon the risk tolerance of the organization consistent with its goals and mission.

- **Step 1.** Prioritize Actions
    - Using results from *Step 7 of the Risk Assessment*, sort the threat and vulnerability pairs according to their risk-levels in descending order. This establishes a prioritized list of actions needing to be taken, with the pairs at the top of the list getting/requiring the most immediate attention and top priority in allocating resources.
    - Output – Actions ranked from high to low.
- **Step 2.** Evaluate Recommended Control Options
    - Although possible controls for each threat and vulnerability pair are arrived at in *Step 8 of the Risk Assessment*, review the recommended control(s) and alternative solutions for reasonableness and appropriateness. The feasibility (e.g., compatibility, user acceptance, etc.) and effectiveness (e.g., degree of protection and level of risk mitigation) of the recommended controls should be analyzed. In the end, select a "most appropriate" control option for each threat and vulnerability pair.
    - Output – List of feasible controls.
- **Step 3.** Conduct Cost-Benefit Analysis
    - Determine the extent to which a control is cost-effective. Compare the benefit (e.g., risk reduction) of applying a control with its subsequent cost of application.

Controls that are not cost-effective are also identified during this step. Analyzing each control or set of controls in this manner, and prioritizing across all controls being considered, can greatly aid in the decision-making process.
    - Output – Documented cost-benefit analysis of either implementing or not implementing each specific control.
- **Step 4.** Select Control(s)
    - Taking into account the information and results from previous steps, our mission, and other important criteria, the Risk Management Team determines the best control(s) for reducing risks to the information systems and to the confidentiality, integrity, and availability of ePHI. These controls may consist of a mix of administrative, physical, and/or technical safeguards.
    - Output – Selected control(s)
- **Step 5.** Assign Responsibility
    - Identify the workforce members with the skills necessary to implement each of the specific controls outlined in the previous step, and assign their responsibilities. Also identify the equipment, training, and other resources needed for the successful implementation of controls. Resources may include time, money, equipment, etc.
    - Output – List of resources, responsible persons, and their assignments.
- **Step 6.** Develop Safeguard Implementation Plan
    - Develop an overall Implementation Plan and individual project plans needed to implement the safeguards and controls identified. The Implementation Plan should contain the following information:
        - Each risk or vulnerability/threat pair and risk level;
        - Prioritized actions;
        - The recommended feasible control(s) for each identified risk;
        - Required resources for implementation of selected controls;
        - Team member responsible for implementation of each control;
        - Start date for implementation
        - Target date for completion of implementation;
        - Maintenance requirements.
    - The overall implementation plan provides a broad overview of the safeguard implementation, identifying important milestones and timeframes, resource requirements (staff and other individuals' time, budget, etc.), interrelationships between projects, and any other relevant information. Regular status reporting of the plan, along with key metrics and success indicators, should be reported to Senior Management.
    - Individual project plans for safeguard implementation may be developed and contain detailed steps that resources assigned carry out to meet implementation timeframes and expectations. Additionally, consider including items in individual project plans such as a project scope, a list deliverables, key assumptions, objectives, task completion dates, and project requirements.

    - Output – Safeguard Implementation Plan
- **Step 7.** Implement Selected Controls
    - As controls are implemented, monitor the affected system(s) to verify that the implemented controls continue to meet expectations. Elimination of all risk is not practical. Depending on individual situations, implemented controls may lower a risk level but not completely eliminate the risk.
    - Continually and consistently communicate expectations to all Risk Management Team members, as well as Senior Management and other key people throughout the risk mitigation process. Identify when new risks are identified and when controls lower or offset risk rather than eliminate it.
    - Additional monitoring is especially crucial during times of major environmental changes, organizational or process changes, or major facilities changes.
    - If risk reduction expectations are not met, then repeat all or a part of the risk management process so that additional controls needed to lower risk to an acceptable level can be identified.
    - Output – Residual Risk documentation

**Risk Management Schedule**: The two principal components of the risk management process -- risk assessment and risk mitigation -- will be carried out according to the following schedule to ensure the continued adequacy and continuous improvement of the information security program:

- Scheduled Basis – an overall risk assessment of the information system infrastructure will be conducted annually. The assessment process should be completed in a timely fashion so that risk mitigation strategies can be determined and included in the corporate budgeting process.
- Throughout a System's Development Life Cycle – from the time that a need for a new, untested information system configuration and/or application is identified through the time it is disposed of, ongoing assessments of the potential threats to a system and its vulnerabilities should be undertaken as a part of the maintenance of the system.
- As Needed – the Security Officer (or other designated employee) or Risk Management Team may call for a full or partial risk assessment in response to changes in business strategies, information technology, information sensitivity, threats, legal liabilities, or other significant factors that affect Catalyze's Platform.

# Process Documentation

Maintain documentation of all risk assessment, risk management, and risk mitigation efforts for a minimum of six years.