Auditing Policy

MolecularMatch will audit access and activity of electronic protected health information (ePHI) applications and systems in order to ensure compliance. The Security Rule requires healthcare organizations to implement reasonable hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI. Audit activities may be limited by application, system, and/or network auditing capabilities and resources. We shall make reasonable and good-faith efforts to safeguard information privacy and security through a well-thought-out approach to auditing that is consistent with available resources.

This policy, and associated procedures for intrusion detection, has been subcontracted 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 monitoring and auditing systems are available on all systems hosted by our sub-contractor.

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

It is our policy to safeguard the confidentiality, integrity, and availability of applications, systems, and networks. To ensure that appropriate safeguards are in place and effective, we shall audit access and activity to detect, report, and guard against:

- Breaches in confidentiality and security of patient protected health information;
- Performance problems and flaws in applications;
- Improper alteration or destruction of ePHI;

The PaaS Subcontractor also supports this aim by detecting, reporting, and guarding against:

- Network vulnerabilities and intrusions;
- Out of date software and/or software known to have vulnerabilities.
- Breaches in confidentiality and security of patient protected health information;
- Performance problems and flaws in applications;
- Improper alteration or destruction of ePHI;

Applicable Standards from the HITRUST Common Security Framework

- 0.a Information Security Management Program
- 01.a Access Control Policy
- 01.b User Registration
- 01.c Privilege Management

- 09.aa Audit Logging
- 09.ac Protection of Log Information
- 09.ab - Monitoring System Use
- 06.e - Prevention of Misuse of Information

Applicable Standards from the HIPAA Security Rule

- 45 CFR ¬ß 164.308(a)(1)(ii)(D) - Information System Activity Review
- 45 CFR ¬ß 164.308(a)(5)(ii)(B) & (C) - Protection from Malicious Software & Log-in Monitoring
- 45 CFR ¬ß 164.308(a)(2) - HIPAA Security Rule Periodic Evaluation
- 45 CFR ¬ß 164.312(b) - Audit Controls
- 45 CFR ¬ß 164.312(c)(2) - Mechanism to Authenticate ePHI
- 45 CFR ¬ß 164.312(e)(2)(i) - Integrity Controls

Auditing Policies

We are responsible for:

1. Auditing information system access and activity. The Security Officer shall:
    - Coordinate auditing activities with the PaaS Subcontractor.
    - Assign the task of generating reports for audit activities to the workforce member responsible for the application, system, or network;
    - Assign the task of reviewing the audit reports to the workforce member responsible for the application, system, or network, the Privacy Officer, or any other individual determined to be appropriate for the task;
    - Organize and provide oversight to a team structure charged with audit compliance activities (e.g., parameters, frequency, sample sizes, report formats, evaluation, follow-up, etc.).
2. The auditing processes shall address access and activity at the following levels listed below. In the case of PaaS Subcontractor, System and Netowrk level auditing is the responsibility of the PaaS Subcontractor as per BAA and Service Agreement. PaaS Subcontractor provides software to aggregate and view User and Application logs, but the log data collected is our responsibility. Auditing processes may address date and time of each log-on attempt, date and time of each log-off attempt, devices used, functions performed, etc.
    - User: User level audit trails generally monitor and log all commands directly initiated by the user, all identification and authentication attempts, and data and services accessed.

    - Application: Application level audit trails generally monitor and log all user activities, including data accessed and modified and specific actions.
3. We shall log all incoming and outgoing traffic for the production system and its operating environment. This includes all successful and failed attempts at data access and editing. Data associated with this data will include origin, destination, time, and other relevant details that are available.

PaaS Vendor is responsible for:

1. Using the following tools or suitable alternatives:
    - Use OSSEC to scan all systems for malicious and unauthorized software every 2 hours and at reboot of systems. Alerts from OSSEC are sent to Kibana, the centralized logging service used.
    - Use Nagios to monitor systems in its environment.
    - Log all activity associated with relevant portals and dashboards (e.g. Developer Portal Access).
    - Use OSSEC to monitor the integrity of log files by utilizing OSSEC System Integrity Checking capabilities.
    - Identify “trigger events” or criteria that raise awareness of questionable conditions of viewing of confidential information. *(See Listing of Potential Trigger Events below)*
    - Utilize OSSEC log correlation functionality to proactively identify and enable alerts based on log data.
2. The auditing processes shall address access and activity at the following levels listed below.
    - System: System level audit trails generally monitor and log user activities, applications accessed, and other system defined specific actions.
    - Network: Network level audit trails generally monitor information on what is operating, penetrations, and vulnerabilities.
3. Reviewing at appropriate time intervals by Security Officer.

The process for review of audit logs, trails, and reports shall include:

- Description of the activity as well as rationale for performing the audit.
- Address date and time of each audited activity, devices used, functions performed, etc.
- Identification of which workforce members will be responsible for review. Workforce members shall not review audit logs that pertain to their own system activity.
- Determine the frequency of auditing, typically weekly or monthly depending on the system/area involved.
- Determine which significant events require further review and follow-up.
- Identify appropriate reporting channels for audit results and required follow-up.

See Vulnerability Scanning Policy

See Intrusion Detection Policy

Use the Audit Log Review Form

Audit Requests

1. A request may be made for an audit for a specific cause. The request may come from a variety of sources including, but not limited to, Privacy Officer, Security Officer, Customer, Partner, or an Application owner or user.
2. A request for an audit for specific cause must include time frame, frequency, and nature of the request. The request must be reviewed and approved by either the Privacy Officer.
3. A request for an audit must be approved by either the Privacy Officer or Security Officer before proceeding. Under no circumstances shall detailed audit information be shared with parties without proper permissions and access to see such data.
    - Only de-identified information shall be shared with Customer or Partner regarding the results of the investigative audit process. This information will be communicated to the appropriate personnel by the Privacy Officer or designee. Prior to communicating with Customer or Partner regarding an audit, it is recommended that risk management and/or legal counsel is sought.

Review and Reporting of Audit Findings

1. Audit information that is routinely gathered must be reviewed in a timely manner, currently monthly, by the responsible workforce member(s).
2. The reporting process shall allow for meaningful communication of the audit findings to those workforce members, Customers, or Partners requesting the audit.
    - Significant findings shall be reported immediately in a written format. Our security incident response form may be utilized to report a single event.
    - Routine findings shall be reported to the sponsoring leadership structure in a written report format.
3. Reports of audit results shall be limited to internal use on a minimum necessary/need-to-know basis. Audit results shall not be disclosed externally without administrative and legal counsel approval.
4. Security audits constitute an internal, confidential monitoring practice that may be included in performance improvement activities and reporting. Care shall be taken to ensure that the results of the audits are disclosed to administrative level oversight structures only and that information which may further expose organizational risk is shared with extreme caution. Generic security audit information may be included in organizational reports (individually-identifiable ePHI shall not be included in the reports).
5. Whenever indicated through evaluation and reporting, appropriate corrective actions must be undertaken. These actions shall be documented and shared with the responsible workforce members, Customers, and/or Partners.

Audit Log Security Controls and Backup

1. Audit logs shall be protected from unauthorized access or modification, so the information they contain will be made available only if needed to evaluate a security incident or for routine audit activities as outlined in this policy.
2. All audit logs are encrypted in transit and at rest to control access to the content of the logs.
3. Audit logs shall be stored on a separate system to minimize the impact auditing may have on the privacy system and to prevent access to audit trails by those with system administrator privileges. This is done to apply the security principle of “separation of duties” to protect audit trails from hackers.

Workforce Training, Education, Awareness, and Responsibilities

1. Workforce members are provided training, education, and awareness on safeguarding the privacy and security of business and ePHI. Our commitment to auditing access and activity of the information applications, systems, and networks is communicated through new employee orientation, ongoing training opportunities and events, and applicable policies. Workforce members are made aware of responsibilities with regard to privacy and security of information as well as applicable sanctions and/or corrective disciplinary actions should the auditing process detect a workforce member’s failure to comply with organizational policies.

External Audits of Information Access and Activity

1. Prior to contracting with an external audit firm, we shall:
    - Outline the audit responsibility, authority, and accountability;
    - Choose an audit firm that is independent of other organizational operations;
    - Ensure technical competence of the audit firm staff;
    - Require the audit firm’s adherence to applicable codes of professional ethics;
    - Obtain a signed HIPAA business associate agreement;
    - Assign organizational responsibility for supervision of the external audit firm.

Retention of Audit Data

1. Audit logs shall be maintained based on organizational needs. There is no standard or

law addressing the retention of audit log/trail information. Retention of this information shall be based on:

    - Organizational history and experience.
    - Available storage space.
    - Log data is currently retained and readily accessible for a 1-month period. Beyond that, log data is available via cold backup.

2. Reports summarizing audit activities shall be retained for a period of six years.

Potential Trigger Events

- High risk or problem prone incidents or events.
- Business associate, customer, or partner complaints.
- Known security vulnerabilities.
- Atypical patterns of activity.
- Failed authentication attempts.
- Remote access use and activity.
- Activity post termination.
- Random audits.