Key Definitions

All definitions are relative to MolecularеMatch ("the Company").

- *Application*: An application running on the Platform by or for the Company, either maintained and created by the Company, or maintained and created by a Subcontractor or Partner.
- *Application Level*: Controls and security associated with an Application.
- *Audit*: Internal process of reviewing information system access and activity (e.g., log-ins, file accesses, and security incidents). An audit may be done as a periodic event, as a result of a patient complaint, or suspicion of employee wrongdoing.
- *Audit Controls*: Technical mechanisms that track and record computer/system activities.
- *Audit Logs*: Encrypted records of activity maintained by the system which provide: 1) date and time of activity; 2) origin of activity (app); 3) identification of user doing activity; and 4) data accessed as part of activity.
- *Access*: Means the ability or the means necessary to read, write, modify, or communicate data/ information or otherwise use any system resource.
- *BaaS*: Backend-as-a-Service. A set of APIs, and associated SDKs, for rapid mobile and web application development. APIs offer the ability to create users, do authentication, store data, and store files.
- *Backup*: The process of making an electronic copy of data stored in a computer system. This can either be complete, meaning all data and programs, or incremental, including just the data that changed from the previous backup.
- *Backup Service*: A logging service for unifying system and application logs, encrypting them, and providing a dashboard for them. Usually managed by a PaaS Subcontractor although it might be also done by the Company directly.
- *Breach*: Means the acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI. For purpose of this definition, “compromises the security or privacy of the PHI” means poses a significant risk of financial, reputational, or other harm to the individual. A use or disclosure of PHI that does not include the identifiers listed at §164.514(e)(2), limited data set, date of birth, and zip code does not compromise the security or privacy of the PHI. Breach excludes:
    1. Any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of a Covered Entity (CE) or Business Associate (BA) if such acquisition, access, or use was made in good faith and within the

scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule.
    2. Any inadvertent disclosure by a person who is authorized to access PHI at a CE or BA to another person authorized to access PHI at the same CE or BA, or organized health care arrangement in which the CE participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule.
    3. A disclosure of PHI where a CE or BA has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.
- *Business Associate (BA)*: A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. Often abbreviated at "BA".
- *Covered Entity*: A health plan, health care clearinghouse, or a healthcare provider who transmits any health information in electronic form.
- *De-identification*: The process of removing identifiable information so that data is rendered to not be PHI.
- *Disaster Recovery*: The ability to recover a system and data after being made unavailable.
- *Disaster Recovery Service*: A disaster recovery service for disaster recovery in the case of system unavailability. This includes both the technical and the non-technical (process) required to effectively stand up an application after an outage. Often partially or wholly subcontracted to a PaaS Subcontractor or other Partner.
- *Disclosure*: Disclosure means the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.
- *Customers*: Contractually bound users of the Company's Platform.
- *Electronic Protected Health Information (ePHI)*: Any individually identifiable health information protected by HIPAA that is transmitted by, processed in some way, or stored in electronic media.
- *Environment*: The overall technical environment, including all servers, network devices, and applications.
- *Event*: An event is defined as an occurrence that does not constitute a serious adverse effect on the Company, its operations, or its Customers, though it may be less than optimal. Examples of events include, but are not limited to:
    - A hard drive malfunction that requires replacement;
    - Systems become unavailable due to power outage that is non-hostile in nature, with redundancy to assure ongoing availability of data;
    - Accidental lockout of an account due to incorrectly entering a password multiple

times.

- *Hardware (or hard drive)*: Any computing device able to create and store ePHI.
- *Health and Human Services (HHS)*: The government body that maintains HIPAA.
- *Individually Identifiable Health Information*: That information that is a subset of health information, including demographic information collected from an individual, and is created or received by a health care provider, health plan, employer, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.
- *Indication*: A sign that an Incident may have occurred or may be occurring at the present time. Examples of indications include:
    - The network intrusion detection sensor alerts when a known exploit occurs against an FTP server. Intrusion detection is generally reactive, looking only for footprints of known attacks. It is important to note that many IDS “hits” are also false positives and are neither an event nor an incident;
    - The antivirus software alerts when it detects that a host is infected with a worm;
    - Users complain of slow access to hosts on the Internet;
    - The system administrator sees a filename with unusual characteristics;
    - Automated alerts of activity from log monitors like OSSEC;
    - An alert from OSSEC about file system integrity issues.
- *Intrusion Detection System (IDS)*: A software tool use to automatically detect and notify in the event of possible unauthorized network and/or system access.
- *IDS Service*: An Intrusion Detection Service for providing IDS notification to customers in the case of suspicious activity. Often partially or wholly subcontracted to a PaaS Subcontractor or other Partner.
- *Law Enforcement Official*: Any officer or employee of an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to investigate or conduct an official inquiry into a potential violation of law; or prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.
- *Logging Service*: A logging service for unifying system and application logs, encrypting them, and providing a dashboard for them. Often partially or wholly subcontracted to a PaaS Subcontractor or other Partner.
- *Messaging*: API-based services to deliver and receive SMS messages.
- *Minimum Necessary Information*: Protected health information that is the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. The

"minimum necessary" standard applies to all protected health information in any form.

- *Off-Site*: For the purpose of storage of Backup media, off-site is defined as any location separate from the building in which the backup was created. It must be physically separate from the creating site.
- *Organization*: For the purposes of this policy, the term "organization" shall mean the Company as defined at the top of this document.
- *Partner*: Contractual bound 3rd party vendor with integration with the Company's Platform. May offer Add-on services.
- *Platform*: The overall technical environment of the Company.
- *Protected Health Information (PHI)*: Individually identifiable health information that is created by or received by the organization, including demographic information, that identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:
    - Past, present or future physical or mental health or condition of an individual.
    - The provision of health care to an individual.
    - The past, present, or future payment for the provision of health care to an individual.
- *Role*: The category or class of person or persons doing a type of job, defined by a set of similar or identical responsibilities.
- *Sanitization*: Removal or the act of overwriting data to a point of preventing the recovery of the data on the device or media that is being sanitized. Sanitization is typically done before re-issuing a device or media, donating equipment that contained sensitive information or returning leased equipment to the lending company.
- *Trigger Event*: Activities that may be indicative of a security breach that require further investigation.
- *Restricted Area*: Those areas of the building(s) where protected health information and/or sensitive organizational information is stored, utilized, or accessible at any time.
- *Role*: The category or class of person or persons doing a type of job, defined by a set of similar or identical responsibilities.
- *PaaS Subcontractor*: A contractually bound, third-party, Platform as a Service, HIPAA compliant vendor (PaaS Subcontractor). May be considered a *Partner* as well.
- *Precursor*: A sign that an Incident may occur in the future. Examples of precursors include:
    - Suspicious network and host-based IDS events/attacks;
    - Alerts as a result of detecting malicious code at the network and host levels;
    - Alerts from file integrity checking software;

    - Audit log alerts.
- *Risk*: The likelihood that a threat will exploit a vulnerability, and the impact of that event on the confidentiality, availability, and integrity of ePHI, other confidential or proprietary electronic information, and other system assets.
- *Risk Management Team*: Individuals who are knowledgeable about the Organization's HIPAA Privacy, Security and HITECH policies, procedures, training program, computer system set up, and technical security controls, and who are responsible for the risk management process and procedures outlined below.
- *Risk Assessment*: (Referred to as Risk Analysis in the HIPAA Security Rule); the process:
    - Identifies the risks to information system security and determines the probability of occurrence and the resulting impact for each threat/vulnerability pair identified given the security controls in place;
    - Prioritizes risks; and
    - Results in recommended possible actions/controls that could reduce or offset the determined risk.
- *Risk Management*: Within this policy, it refers to two major process components: risk assessment and risk mitigation. This differs from the HIPAA Security Rule, which defines it as a risk mitigation process only. The definition used in this policy is consistent with the one used in documents published by the National Institute of Standards and Technology (NIST).
- *Risk Mitigation*: Referred to as Risk Management in the HIPAA Security Rule, and is a process that prioritizes, evaluates, and implements security controls that will reduce or offset the risks determined in the risk assessment process to satisfactory levels within an organization given its mission and available resources.
- *Security Incident* (or just Incident): A security incident is an occurrence that exercises a significant adverse effect on people, process, technology, or data. Security incidents include, but are not limited to:
    - A system or network breach accomplished by an internal or external entity; this breach can be inadvertent or malicious;
    - Unauthorized disclosure;
    - Unauthorized change or destruction of ePHI (i.e. delete dictation, data alterations not following the Company's procedures);
    - Denial of service not attributable to identifiable physical, environmental, human or technology causes;
    - Disaster or enacted threat to business continuity;
    - Information Security Incident: A violation or imminent threat of violation of information security policies, acceptable use policies, or standard security practices. Examples of information security incidents may include, but are not limited to, the following:

    - Denial of Service: An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources;
    - Malicious Code: A virus, worm, Trojan horse, or other code-based malicious entity that infects a host;
    - Unauthorized Access/System Hijacking: A person gains logical or physical access without permission to a network, system, application, data, or other resource. Hijacking occurs when an attacker takes control of network devices or workstations;
    - Inappropriate Usage: A person violates acceptable computing use policies;
    - Other examples of observable information security incidents may include, but are not limited to:
        - Use of another person's individual password and/or account to login to a system;
        - Failure to protect passwords and/or access codes (e.g., posting passwords on equipment);
        - Installation of unauthorized software;
        - Terminated workforce member accessing applications, systems, or network.
- *Threat*: The potential for a particular threat-source to successfully exercise a particular vulnerability. Threats are commonly categorized as:
    - Environmental – external fires, HVAC failure/temperature inadequacy, water pipe burst, power failure/fluctuation, etc.
    - Human – hackers, data entry, workforce/ex-workforce members, impersonation, insertion of malicious code, theft, viruses, SPAM, vandalism, etc.
    - Natural – fires, floods, electrical storms, tornados, etc.
    - Technological – server failure, software failure, ancillary equipment failure, etc. and environmental threats, such as power outages, hazardous material spills.
    - Other – explosions, medical emergencies, misuse or resources, etc.
- *Threat Source*: Any circumstance or event with the potential to cause harm (intentional or unintentional) to an IT system. Common threat sources can be natural, human or environmental which can impact the organization's ability to protect ePHI.
- *Threat Action*: The method by which an attack might be carried out (e.g., hacking, system intrusion, etc.).
- *Unrestricted Area*: Those areas of the building(s) where protected health information and/or sensitive organizational information is not stored or is not utilized or is not accessible there on a regular basis.
- *Unsecured Protected Health Information*: Protected health information (PHI) that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Pub. L.111-5 on the HHS website.

1. Electronic PHI has been encrypted as specified in the HIPAA Security rule by the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key and such confidential process or key that might enable decryption has not been breached. To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt. The following encryption processes meet this standard.
2. Valid encryption processes for data at rest (i.e. data that resides in databases, file systems and other structured storage systems) are consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.
3. Valid encryption processes for data in motion (i.e. data that is moving through a network, including wireless transmission) are those that comply, as appropriate, with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPSec VPNs; or 800-113, Guide to SSL VPNs, and may include others which are Federal Information Processing Standards FIPS 140-2 validated.
4. The media on which the PHI is stored or recorded has been destroyed in the following ways:
5. Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.
6. Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publications 800-88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved.

- *Vendors*: Persons from other organizations marketing or selling products or services, or providing services to the Company.
- *Vulnerability*: A weakness or flaw in an information system that can be accidentally triggered or intentionally exploited by a threat and lead to a compromise in the integrity of that system, i.e., resulting in a security breach or violation of policy.
- *Workstation*: An electronic computing device, such as a laptop or desktop computer, or any other device that performs similar functions, used to create, receive, maintain, or transmit ePHI. Workstation devices may include, but are not limited to: laptop or desktop computers, personal digital assistants (PDAs), tablet PCs, and other handheld devices. For the purposes of this policy, “workstation” also includes the combination of hardware, operating system, application software, and network connection.
- *Workforce*: Means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.