Introduction

MolecularMatch provides secure and compliant clinical trial and drug-based information resources deliveried through cloud-based software.

We are committed to ensuring the confidentiality, privacy, integrity, and availability of all electronic protected health information (ePHI) received, maintained, processed and/or transmitted on behalf of our Customers or individuals. We strive to maintain compliance, proactively address information security issues, and mitigate the risk of data loss. Known breaches are completely and effectively communicated in a timely manner. The following documents address core policies used to maintain compliance and assure the proper protections of web, infrastructure, and administrative components of the solution.

Compliance Inheritance

We provide a web application enabling patients, physicians, and principal investigators to search for and manage the enrollment process around clinical trials. Principal Investigators of these clinical trials might be allowed to have the ability to review de-identified information about patients and express an interest in evaluating them for a fit with their clinical trial. We have been through a HIPAA compliance audit by a 3rd party to validate and map organizational policies and technical settings to HIPAA rules (where applicable).

Sometimes business associate agreements (BAAs) with Covered Entities (CEs) are signed. These BAAs outline the obligations of both our company and the Covered Entity, as well as liability in the case of a breach as defined by the HIPAA standard. When providing a web application and other related services that are part of the technology requirements that exist in HIPAA and HITRUST, as well as future compliance frameworks, we manage those aspects of their responsibilities for compliance.

We do use third-party subcontractors to aid in managing some of the compliance and risk. Currently a secure, HIPAA compliant platform-as-a-service, cloud solution for hosting and managing web and data servers subcontractor (**"PaaS Subcontractor"**) is being used. As such, those aspects that the PaaS Subcontractor manages on our behalf are inherited by Customers, and the PaaS Subcontractor assumes the risk associated with those aspects of compliance. In doing so, the PaaS Subcontractor helps us achieve and maintain compliance, as well as mitigates our risk.

Below are mappings of HIPAA Rules to controls as well as a mapping of what Rules are managed by the PaaS Subcontractor.

The current PaaS Subcontractor is Catalyze.io.

Organizational Concepts

The physical infrastructure environment is hosted by the Paas Subcontractor via Rackspace and Amazon Web Services (AWS). The network components and supporting network infrastructure is contained within AWS and Rackspace infrastructure and managed by Rackspace and AWS. Neither ourselves nor the PaaS Subcontractor have physical access into the network components. The PaaS Subcontractor's environment consists of Cisco firewalls, Apache web servers, Dropwizard Java application servers, Percona and Riak database servers, Logstash logging servers, Linux Ubuntu monitoring servers, Puppet access control server, OSSEC IDS services, Docker containers, Linux CentOS bastion host, and developer tools servers running on Linux Ubuntu. In addition, we use a node.js web application framework and MongoDB for storage of all data. These are hosted within the infrastructure mentioned above.

Within our Platform, both on Rackspace and AWS, all data transmission is encrypted and all hard drives are encrypted so data at rest is also encrypted; this applies to all servers - those hosting Docker containers, databases, APIs, log servers, etc. We always assume all production data *may* contain ePHI, even though our Risk Assessment does not indicate this is the case, and thus provide proactive protections based on this assumption.

We restrict, secure, and assure the privacy of all ePHI data at the Application Level, as this is not under the control or purview of the PaaS Subcontractor. This is done using appropriate access controls, monitoring, and security frameworks. Specifically all data is encrypted in transit using SSL. Users are managed in the application server and no user regardless of role can see another user's ePHI.

There is data and network segmentation in place. This is currently managed by the PaaS Subcontractor. Load balancers segment data, while firewalls route traffic to private subnets, creating dedicated Virtual Private Clouds. As a result of segmentation strategies employed by the PaaS Subcontractor, they have effectively create RFC 1918, or dedicated, private segmented and separated networks and IP spaces, for our web application.

Additionally, the PaaS Subcontractor uses IPtables on each server for logical segmentation. The IPtables are configured to restrict access to only justified ports and protocols. The PaaS Subcontractor has implemented strict logical access controls so that only authorized personnel are given access to the internal management servers. The environment is configured so that data is transmitted from the load balancers to the application servers over an SSL encrypted session.

Once the data is received from the application server, a series of Application Programming Interface (API) calls is made to the database servers where the potential ePHI resides. The ePHI is separated through programming logic built, so that access to one database server will not allow access to the full ePHI spectrum.

Only the web application servers are public facing and accessible via the Internet. The database servers, where any potential ePHI would reside, are located on the private, internal network and can only be accessed directly over an SSH connection through the bastion host. The access to the internal database is restricted to a limited number of personnel and strictly controlled to only

those personnel with a business justified reason. Remote access to the internal servers is not accessible except through the load balancers and bastion host.

All updates to the web application and data servers are tested end-to-end for usability, security, and impact prior to deployment to production.

Version Control

Policies were last updated October 29th, 2014.

Policies are maintained in our GitHub repository. All workforce members have read-only access to the policies. They can suggest changes and make a request for those changes to be reviewed by making "Pull requests". Otherwise, the members of the compliance team resonsible for maintaining and reviewing the policies are the only ones with read-and-write access to the policy repository. PDF copies of the current polciies are also stored on Google Drive for convenience purposes.

Policies are stored for at least 6-years using the Git Hub repository as the main archiving mechanism.