HIPAA Inheritance for Catalyze Customers

MolecularMatch uses a compliant hosted software infrastructure by a Sucontractor. This Platform as a Service Subcontractor (PaaS Subcontractor) has been through a HIPAA compliance audit by a national, third-party compliance firm, to validate and map organizational policies and technical settings to HIPAA rules. The PaaS Subcontractor is currently undergoing a HITRUST audit to achieve HITRUST Certification.

The PaaS Subcontractor has signed a business associate agreements (BAAs) with our Company. This BAAs outlines t'she PaaS Subcontractor obligations and our own obligations, as well as liability in the case of a breach. In providing infrastructure and managing security configurations that are a part of the technology requirements that exist in HIPAA and HITRUST, as well as future compliance frameworks, the PaaS Subcontractor manages various aspects of compliance for our Company. The aspects of compliance that the PaaS Subcontractor manages for our Company are inherited by our Company, and the PaaS Subcontractor assumes the risk associated with those aspects of compliance. In doing so, the PaaS Subcontractor helps our Compay achieve and maintain compliance, as well as mitigates our Company's risk.

Certain aspects of compliance cannot be inherited. Because of this in order to achieve full compliance or HITRUST Certification, our Company has implemented certain organizational policies. These policies and aspects of compliance fall outside of the services and obligations of the PaaS Subcontractor.

Below are mappings of HIPAA Rules to the PaaS Subcontractor controls and a mapping of what Rules are inherited by our Company.

HIPAA ID	HIPAA Rule - Administrative Controls	Compay's Control	Inherited
164.308(a)(1)(i)	Security Management Process	Risk Management Policy	Yes
164.308(a)(2)	Assigned Security Responsibility	Roles Policy	Partially
164.308(a)(3)(i)	Workforce Security	Employee Policies	Partially
164.308(a)(4)(i)	Information Access Management	System Access Policy	Yes
164.308(a)(5)(i)	Security Awareness and Training	Employee Policy	No
164.308(a)(6)(i)	Security Incident Procedures	IDS Policy	Yes

164.308(a)(6)(i)	Security Incident Procedures	IDS Policy	Yes
164.308(a)(7)(i)	Contingency Plan	Disaster Recovery Policy	Yes
164.308(a)(8)	Evaluation	Auditing Policy	Yes
HIPAA ID	**HIPAA Rule - Physical Safeguards**	**Compay's Control**	**Inherited**
164.310(a)(1)	Facility Access Controls	Facility Access Policy and Disaster Recovery Policy	Yes
164.310(b)	Workstation Use	System Access Policy, Approved Tools Policy, and Employee Policy	Partially
164.310(c)	Workstation Security	System Access Policy, Approved Tools Policy, and Employee Policy	Partially
164.310(d)(1)	Device and Media Controls	Disposable Media Policy and Data Management Policy	Yes
HIPAA ID	**HIPAA Rule - Technical Safeguards**	**Compay's Control**	**Inherited**
164.312(a)(1)	Access Control	System Access Policy	Partially
164.312(b)	Audit Controls	Auditing Policy	Yes
164.312(c)(1)	Integrity	System Access Policy, Auditing Policy, and Intrusion Detection Policy	Yes
164.312(d)	Person or Entity Authentication	System Access Policy	Yes
164.312(e)(1)	Transmission Security	System Access Policy and Data Management Policy	Yes

HIPAA ID	**HIPAA Rule - Organizational Requirements**	**Compay's Control**	**Inherited**
164.314(a)(1)(i)	Business Associate Contracts or Other Arrangements	Business Associate Agreements 3rd Parties Policies	Partially
HIPAA ID	**HIPAA Rule - Policies and Procedures and Documentation Requirements**	**Compay's Control**	**Inherited**
164.316(a)	Policies and Procedures	Policy Management Policy	Partially
164.316(b)(1)(i)	Documentation	Policy Management Policy	Partially
HIPAA ID	**HITECH Act - Security Provisions HIPAA Rule**	**Compay's Control**	**Inherited**
13402(a) 13402(b)	Notification in the Case of Breach	Breach Policy	Yes
13402(d)(1)	Timelines of Notification	Breach Policy	Yes
13402(f)(1)	Content of Notification	Breach Policy	Yes