HIPAA Inheritance for Catalyze Customers

Catalyze provides compliant hosted software infrastructure for its Customers. Catalyze has been through a HIPAA compliance audit by a national, 3rd party compliance firm, to validate and map organizational policies and technical settings to HIPAA rules. Catalyze is currently undergoing a HITRUST audit to achieve HITRUST Certification.

Catalyze signs business associate agreements (BAAs) with its Customers. These BAAs outline Catalyze obligations and Customer 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, Catalyze manages various aspects of compliance for Customers. The aspects of compliance that Catalyze manages for Customers are inherited by Customers, and Catalyze assumes the risk associated with those aspects of compliance. In doing so, Catalyze helps Customers achieve and maintain compliance, as well as mitigates Customers risk.

Certain aspects of compliance cannot be inherited. Because of this, Catalyze Customers, in order to achieve full compliance or HITRUST Certification, must implement certain organizational policies. These policies and aspects of compliance fall outside of the services and obligations of Catalyze.

Below are mappings of HIPAA Rules to Catalyze controls and a mapping of what Rules are inherited by Customers.

Administrative Controls		
HIPAA Rule	**Catalyze Control**	**Inherited**
Security Management Process - 164.308(a)(1)(i)	Risk Management Policy	Yes
Assigned Security Responsibility - 164.308(a)(2)	Roles Policy	Partially

Workforce Security - 164.308(a)(3)(i)	Employee Policies	Partially
Information Access Management - 164.308(a)(4)(i)	System Access Policy	Yes
Security Awareness and Training - 164.308(a)(5)(i)	Employee Policy	No
Security Incident Procedures - 164.308(a)(6)(i)	IDS Policy	Yes
Contingency Plan - 164.308(a)(7)(i)	Disaster Recovery Policy	Yes
Evaluation - 164.308(a)(8)	Auditing Policy	Yes

Physical Safeguards		
HIPAA Rule	**Catalyze Control**	**Inherited**
Facility Access Controls - 164.310(a)(1)	Facility and Disaster Recovery Policies	Yes
Workstation Use - 164.310(b)	System Access, Approved Tools, and Employee Policies	Partially
Workstation Security - 164.310(‘c’)	System Access, Approved Tools, and Employee Policies	Partially
Device and Media Controls - 164.310(d)(1)	Disposable Media and Data Management Policies	Yes

Technical Safeguards		
HIPAA Rule	**Catalyze Control**	**Inherited**
Access Control - 164.312(a)(1)	System Access Policy	Partially
Audit Controls - 164.312(b)	Auditing Policy	Yes

Integrity - 164.312(‘c’)(1)	System Access, Auditing, and IDS Policies	Yes
Person or Entity Authentication - 164.312(d)	System Access Policy	Yes
Transmission Security - 164.312(e)(1)	System Access and Data Management Policy	Yes

Organizational Requirements		
HIPAA Rule	**Catalyze Control**	**Inherited**
Business Associate Contracts or Other Arrangements - 164.314(a)(1)(i)	Business Associate Agreements and 3rd Parties Policies	Partially

Policies and Procedures and Documentation Requirements		
HIPAA Rule	**Catalyze Control**	**Inherited**
Policies and Procedures - 164.316(a)	Policy Management Policy	Partially
Documentation - 164.316(b)(1)(i)	Policy Management Policy	Partially

HITECH Act - Security Provisions		
HIPAA Rule	**Catalyze Control**	**Inherited**
Notification in the Case of Breach - 13402(a) and (b)	Breach Policy	Yes

Timelines of Notification - 13402(d)(1)	Breach Policy	Yes
Content of Notification - 13402(f)(1)	Breach Policy	Yes