## Introduction

Catalyze, Inc (“Catalyze”) is committed to ensuring the confidentiality, privacy, integrity, and availability of all electronic protected health information (ePHI) it receives, maintains, processes and/or transmits on behalf of its Customers. As providers of compliant, hosted infrastructure used by health technology vendors, developers, designers, agencies, custom development shops, and enterprises, Catalyze strives to maintain compliance, proactively address information security, mitigate risk for its Customers, and assure known breaches are completely and effectively communicated in a timely manner. The following documents address core policies used by Catalyze to maintain compliance and assure the proper protections of infrastructure used to store, process, and trasmit ePHI for Catalyze Customers.

Catalyze provides secure and compliant cloud-based software. This hosted software falls into two broad categoring: 1) **Platform as a Service (Paas)** and 2) **Platform Add-ons**. These Categories are cited throughout polices as Customers in each category inherit different policices, procedures, and obligations from Catalyze.

### Platform as a Service (PaaS)

PaaS Customers utilized hosted software and infrastructure from Catalyze to deploy, host, and scale custom developed applications and configured databases. These customers are deployed into compliant containers run on systems secured and managed by Catalyze. Catalyze does not have insight or access into application level data of PaaS Customers and, as such, does not have the ability to secure or manage risk associated with application level vulnerabilities and security weaknesses. Catalyze makes every effort to reduce the risk of unauthorized disclosure, access, and/or breach of PaaS Customer data through network (firewalls, dedicated IP spaces, etc) and server settings (encryption at rest and in transit, OSSEC throughout the Platform, etc).

PaaS Customers can opt for a list of Services from Catalyze, which include Backup Service, Logging Service, IDS Service, and Disaster Recovery Service. These services are not standard and PaaS Customers must sign up for them in order for Catalyze to manage these areas of security and compliance.

### Platform Add-ons (or “Add-ons”)

Add-ons are API-driven services that are offered as part of the Catalyze Platform. These services currently include our Backend as a Service and secure Messaging Service. With Add-ons, Catalyze has access to data models and manages all application level configurations and security.

In the future there may be 3rd party Add-on services available as part of the Catalyze Platform. These 3rd party, or Partner, Services will be fully reviewed by Catalyze to assure they do not have a negative impact on Catalyze’s information security and compliance posture.

## Compliace Inheritance

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, both PaaS Customers and Add-on Customers.

## Catalyze Organizational Concepts

The physical infrastructure environment is hosted at 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. Catalyze does not have physical access into the network components. The Catalyze 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.

Within the Catalyze 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 containes, databases, APIs, log servers, etc. Catalyze assumes all data *may* contain ePHI, even though our Risk Assessment does not indicate this is the case, and provides appropriate protections based on that assumption.

In the case of PaaS Customers, it is the responsilibity of the Customer to restrict, secure, and assure the privacy of all ePHI data at the Application Level, as this is not under the control or perview of Catalyze.

There is data and network segmentation in place but differently implemented on Rackspace and AWS versions of the Catalyze Platform.

- With Rackspace, hosted load balancers segment data and traffic while Cisco firewalls route traffic to private subnets for each PaaS Customer and for Platform Add-ons.
- With AWS, hosted load balancers segment data across dedicated Virtual Privare Clouds for each PaaS Customer and for Platform Add-ons.

The result of segmentation strategies employed by Catalyze effectively create RFC 1918, or dedicated, private segmented and separated networks and IP spaces, for each PaaS Customer and for Platform Add-ons.

Additionally, IPtables is used on each each server for logical segmentation. The IPtables are configured to restrict access to only justified ports and protocols. Catalyze 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.

In the case of Platform Add-ons, 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 ePHI resides. The ePHI is separated into Riak and Percona databases through programming logic built, so that access to one database server will not present you with the full ePHI spectrum.

The bastion host, Apache web server, Dropwizard application servers are externally facing and accessible via the Internet. The database servers, where the ePHI resides, are located on the internal Catalyze 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 Platform Add-ons and operating systems are tested end-to-endfor usability, security and impact prior to deployment to production.

### Version Control

Policies were last updated April 4th, 2014.

## HIPAA Inheritance for PaaS 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 (optional) |
| Contingency Plan - 164.308(a)(7)(i) | Disaster Recovery Policy | Yes (optional) |
| 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 (optional) |
| Integrity - 164.312(‘c’)(1) | System Access, Auditing, and IDS Policies | Yes (optional) |
| 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 | Partially |
| Timelines of Notification - 13402(d)(1) | Breach Policy | Partially |
| Content of Notification - 13402(f)(1) | Breach Policy | Partially |

## HIPAA Inheritance for Platform Add-on 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<br>Policy | Partially |

| HITECH Act - Security Provisions | | |
|---|---|---|
| **HIPAA Rule** | **Catalyze Control** | **Inherited** |
| Notification in the Case of Breach - 13402(a) and (b) | Breach Policy | Partially |
| Timelines of Notification - 13402(d)(1) | Breach Policy | Partially |
| Content of Notification - 13402(f)(1) | Breach Policy | Partially |

## Policy Management Policy

Catalyze implements policies and procedures to maintain compliance and integrity of data. The Security Officer and Privacy Officer are responsible for maintaining policies and procedures and assuring all Catalyze workforce members, business associates, customers, and partners are adherent to all applicable policies. Previous versions of polices are retained to assure ease of finding policies at specific historic dates in time.

### Applicable Standards from the HITRUST Common Security Framework

- 12.c - Developing and Implementing Continuity Plans Including Information Security

### Applicable Standards from the HIPAA Security Rule

- 164.316(a) - Policies and Procedures
- 164.316(b)(1)(i) - Documentation

### Maintenance of Policies

1. All policies are stored and up to date to maintain Catalyze compliance with HIPAA, HITRUST, NIST, and other relevant standards. Updates and version control is done similar to source code control.

2. Policy update requests can be made by any workforce member at any time. Furthermore, all policies are reviewed annually by both the Security and Privacy Officer to assure accurate and up-to-date.

3. Edits and updates made by appropriate and authorized workforce members are done on their own versions, or branches. These changes are only merged back into final, or master, versions by the Privacy or Security Officer, similarly to a pull request. All changes are linked to workforce personnel who made them and the Officer who accepted them.

4. All policies are made accessible to all Catalyze workforce members.

5. All policies, and associated documentation, is retaiend for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

Additional documentation related to maintenance of policies is outlined in the Security officers responsibilities.

## Risk Management Policy

This policy establishes the scope, objectives, and procedures of Catalyze's information security risk management process. The risk management process is intended to support and protect the organization and its ability to fulfill its mission.

### Applicable Standards from the HITRUST Common Security Framework

- 03.a - Risk Management Program Development
- 03.b - Performing Risk Assessments
- 03.c - Risk Mitigation

### Applicable Standards from the HIPAA Security Rule

- 164.308(a)(1)(ii)(A) – HIPAA Security Rule Risk Analysis
- 164.308(a)(1)(ii)(B) – HIPAA Security Rule Risk Management
- 164.308(a)(8) – HIPAA Security Rule Evaluation

### Risk Management Policies

1. It is the policy of Catalyze to conduct thorough and timely risk assessments of the potential threats and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI) (and other confidential and proprietary electronic information) it stores, transmits, and/or processes for its Customers and to develop strategies to efficiently and effectively mitigate the risks identified in the assessment process as an integral part of the Catalyze's information security program.

2. Risk analysis and risk management are recognized as important components of Catalyze's corporate compliance program and information security program in accordance with the Risk Analysis and Risk Management implementation specifications within the Security Management standard and the evaluation standards set forth in the HIPAA Security Rule, 45 CFR 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(1)(i), and 164.308(a)(8).
    1. Risk assessments are done throughout product life cycles:
        1. Before the integration of new system technologies and before changes are made to Catalyze physical safeguards; and
            - These changes do not include routine updates to existing systems, deployments of new systems created based on previously configured systems, deployments of new Customers, or new code developed for operations and managment of the

Catalyze Platform.

2. While making changes to Catalyze physical equipment and facilities that introduce new, untested configurations.

2. Catalyze performs periodic technical and non-technical assessments of the security rule requirements as well as in response to environmental or operational changes affecting the security of ePHI.

3. Catalyze implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to:
   1. Ensure the confidentiality, integrity, and availability of all ePHI Catalyze receives, maintains, processes, and/or transmits for its Customers;
   2. Protect against any reasonably anticipated threats or hazards to the security or integrity of Customer ePHI;
   3. Protect against any reasonably anticipated uses or disclosures of Customer ePHI that are not permitted or required; and
   4. Ensure compliance by all workforce members.
4. Any risk remaining (residual) after other risk controls have been applied, requires sign off by the senior management and Catalyze's Security Officer.
5. All Catalyze workforce members are expected to fully cooperate with all persons charged with doing risk management work, including contractors and audit personnel. Any workforce member that violates this policy will be subject to disciplinary action based on the severity of the violation according to Catalyze's policies, which is outlined in the Catalyze Policy Management Policy.
6. The implementation, execution, and maintenance of the information security risk analysis and risk management process is the responsibility of Catalyze's Security Officer (or other designated employee), and the identified Risk Management Team.
7. All risk management efforts, including decisions made on what controls to put in place as well as those to not put into place, are documented and the documentation is maintained for six years.

### Risk Management Procedures

**Risk Assessment**: The intent of completing a risk assessment is to determine potential threats and vulnerabilities and the likelihood and impact should they occur. The output of this process helps to identify appropriate controls for reducing or eliminating risk.

- Step 1. System Characterization
  - The first step in assessing risk is to define the scope of the effort. To do this, identify where ePHI is received, maintained, processed, or transmitted. Using information-gathering

  techniques, the Catalyze Platform boundaries are identified.
  - Output – Characterization of the Catalyze Platform system assessed, a good picture of the Platform environment, and delineation of Platform boundaries.
- Step 2. Threat Identification
  - Potential threats (the potential for threat-sources to successfully exercise a particular vulnerability) are identified and documented. All potential threat-sources through the review of historical incidents and data from intelligence agencies, the government, etc., to help generate a list of potential threats.
  - Output – A threat list containing a list of threat-sources that could exploit Platform vulnerabilities.
- Step 3. Vulnerability Identification
  - Develop a list of technical and non-technical Platform vulnerabilities that could be exploited or triggered by potential threat-sources. Vulnerabilities can range from incomplete or conflicting policies that govern an organization's computer usage to insufficient safeguards to protect facilities that house computer equipment to any number of software, hardware, or other deficiencies that comprise an organization's computer network.
  - Output – A list of the Platform vulnerabilities (observations) that could be exercised by potential threat-sources.
- Step 4. Control Analysis
  - Document and assess the effectiveness of technical and non-technical controls that have been or will be implemented by Catalyze to minimize or eliminate the likelihood / probability of a threat-source exploiting a Platform vulnerability.
  - Output – List of current or planned controls (policies, procedures, training, technical mechanisms, insurance, etc.) used for the Platform to mitigate the likelihood of a vulnerability being exercised and reduce the impact of such an adverse event.
- Step 5. Likelihood Determination
  - Determine the overall likelihood rating that indicates the probability that a vulnerability could be exploited by a threat-source given the existing or planned security controls.
  - Output – Likelihood rating of low (.1), medium (.5), or high (1). Refer to the NIST SP 800–30 definitions of low, medium, and high.
- Step 6. Impact Analysis
  - Determine the level of adverse impact that would result from a threat successfully exploiting a vulnerability. Factors of the data and systems to consider should include the importance to Catalyze's mission; sensitivity and criticality (value or importance); costs associated; loss of confidentiality, integrity, and availability of systems and data.
  - Output – Magnitude of impact rating of low (10), medium (50), or high (100). Refer to the NIST SP 800–30 definitions of low, medium, and high.

- Step 7. Risk Determination
    - Establish a risk level. By multiplying the ratings from the likelihood determination and impact analysis, a risk level is determined. This represents the degree or level of risk to which an IT system, facility, or procedure might be exposed if a given vulnerability were exercised. The risk rating also presents actions that senior management must take for each risk level.
    - Output – Risk level of low (1–10), medium (>10–50) or high (>50–100). Refer to the NIST SP 800–30 definitions of low, medium, and high.
- Step 8. Control Recommendations
    - Identify controls that could reduce or eliminate the identified risks, as appropriate to the organization's operations to an acceptable level. Factors to consider when developing controls may include effectiveness of recommended options (i.e., system compatibility), legislation and regulation, organizational policy, operational impact, and safety and reliability. Control recommendations provide input to the risk mitigation process, during which the recommended procedural and technical security controls are evaluated, prioritized, and implemented.
    - Output – Recommendation of control(s) and alternative solutions to mitigate risk.
- Step 9. Results Documentation
    - Results of the risk assessment are documented in an official report, spreadsheet, or briefing and provided to senior management to make decisions on policy, procedure, budget, and Platform operational and management changes.
    - Output – A risk assessment report that describes the threats and vulnerabilities, measures the risk, and provides recommendations for control implementation.

**Risk Mitigation**: Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the Risk Assessment process to ensure the confidentiality, integrity and availability of Catalyze Platform ePHI. Determination of appropriate controls to reduce risk is dependent upon the risk tolerance of the organization consistent with its goals and mission.

- Step 1. Prioritize Actions
    - Using results from Step 7 of the Risk Assessment, sort the threat and vulnerability pairs according to their risk-levels in descending order. This establishes a prioritized list of actions needing to be taken, with the pairs at the top of the list getting/requiring the most immediate attention and top priority in allocating resources
    - Output – Actions ranked from high to low
- Step 2. Evaluate Recommended Control Options
    - Although possible controls for each threat and vulnerability pair are arrived at in Step 8 of the Risk Assessment, review the recommended control(s) and alternative solutions for reasonableness and appropriateness. The feasibility (e.g., compatibility, user acceptance, etc.) and effectiveness (e.g., degree of protection and level of risk mitigation) of the

recommended controls should be analyzed. In the end, select a “most appropriate” control option for each threat and vulnerability pair.

  - Output – list of feasible controls

- Step 3. Conduct Cost-Benefit Analysis
  - Determine the extent to which a control is cost-effective. Compare the benefit (e.g., risk reduction) of applying a control with its subsequent cost of application. Controls that are not cost-effective are also identified during this step. Analyzing each control or set of controls in this manner, and prioritizing across all controls being considered, can greatly aid in the decision-making process.
  - Output – Documented cost-benefit analysis of either implementing or not implementing each specific control

- Step 4. Select Control(s)
  - Taking into account the information and results from previous steps, Catalyze’s mission, and other important criteria, the Risk Management Team determines the best control(s) for reducing risks to the information systems and to the confidentiality, integrity, and availability of ePHI. These controls may consist of a mix of administrative, physical, and/or technical safeguards.
  - Output – Selected control(s)

- Step 5. Assign Responsibility
  - Identify the workforce members with the skills necessary to implement each of the specific controls outlined in the previous step, and assign their responsibilities. Also identify the equipment, training and other resources needed for the successful implementation of controls. Resources may include time, money, equipment, etc.
  - Output – List of resources, responsible persons and their assignments

- Step 6. Develop Safeguard Implementation Plan
  - Develop an overall implementation or action plan and individual project plans needed to implement the safeguards and controls identified. The Implementation Plan should contain the following information:
    - Each risk or vulnerability/threat pair and risk level;
    - Prioritized actions;
    - The recommended feasible control(s) for each identified risk;
    - Required resources for implementation of selected controls;
    - Team member responsible for implementation of each control;
    - Start date for implementationl
    - Target date for completion of implementation;
    - Maintenance requirements.
  - The overall implementation plan provides a broad overview of the safeguard

implementation, identifying important milestones and timeframes, resource requirements (staff and other individuals' time, budget, etc.), interrelationships between projects, and any other relevant information. Regular status reporting of the plan, along with key metrics and success indicators should be reported to Catalyze Senior Management.
    - Individual project plans for safeguard implementation may be developed and contain detailed steps that resources assigned carry out to meet implementation timeframes and expectations. Additionally, consider including items in individual project plans such as a project scope, a list deliverables, key assumptions, objectives, task completion dates and project requirements.
    - Output – Safeguard Implementation Plan

- Step 7. Implement Selected Controls As controls are implemented, monitor the affected system(s) to verify that the implemented controls continue to meet expectations. Elimination of all risk is not practical. Depending on individual situations, implemented controls may lower a risk level but not completely eliminate the risk.
    - Continually and consistently communicate expectations to all Risk Management Team members, as well as senior management and other key people throughout the risk mitigation process. Identify when new risks are identified and when controls lower or offset risk rather than eliminate it.
    - Additional monitoring is especially crucial during times of major environmental changes, organizational or process changes, or major facilities changes.
    - If risk reduction expectations are not met, then repeat all or a part of the risk management process so that additional controls needed to lower risk to an acceptable level can be identified.
    - Output – Residual Risk documentation

**Risk Management Schedule**: The two principle components of the risk management process - risk assessment and risk mitigation - will be carried out according to the following schedule to ensure the continued adequacy and continuous improvement of Catalyze's information security program:

- Scheduled Basis – an overall risk assessment of Catalyze's information system infrastructure will be conducted annually. The assessment process should be completed in a timely fashion so that risk mitigation strategies can be determined and included in the corporate budgeting process.
- Throughout a System's Development Life Cycle – from the time that a need for a new, untested information system configuration and/or application is identified through the time it is disposed of, ongoing assessments of the potential threats to a system and its vulnerabilities should be undertaken as a part of the maintenance of the system.
- As Needed – the Security Officer (or other designated employee) or Risk Management Team may call for a full or partial risk assessment in response to changes in business strategies, information technology, information sensitivity, threats, legal liabilities, or other significant factors that affect Catalyze's Platform.

### Process Documentation

Maintain documentation of all risk assessment, risk management, and risk mitigation efforts for a minimum of six years.

## Roles Policy

Catalyze has a Security Officer [164.308(a)(2)] and Privacy Officer [164.308(a)(2)] appointed to assist in maintaining and enforcing safegaurds towards compliance. The responsiblities associated with these roles are outlined below.

### Applicable Standards from the HITRUST Common Security Framework

- 06.d - Data Protection and Privacy of Covered Information
- 06.g - Compliance with Security Policies and Standards

### Applicable Standards from the HIPAA Security Rule

- 164.308(a)(2) - Assigned Security Responsibility
- 164.308(a)(5)(i) - Security Awareness and Training

### Privacy Officer

The Privacy Officer is responsible for assisting with compliance and security training for workforce members, assuring organization remains in compliance with evolving compliance rules, and helping the Security Officer in his responsibilities.

1. Provides annual training to all workforce members of established policies and procedures as necessary and appropriate to carry out their job functions, and documents the training provided.
2. Assists in the administration and oversight of business associate agreements.
3. Manage relationships with customers and partners as those relationships affect security and compliance of ePHI.
4. Assist Secruity Officer as needed.

The current Catalyze Privacy Officer is Travis Good (travis@catalyze.io).

### Workforce Training Responsibilities

1. The Privacy Officer facilitates the training of all workforce members as follows:
    1. New workforce members within their first month of employment;
    2. Existing workforce members annually;
    3. Existing workforce members whose functions are affected by a material change in the policies and procedures, within a month after the material change becomes effective;

    4. Existing workforce members as needed due to changes in security and risk posture of Catalyze.

2. The Security Officer or designee maintains documentation of the training session materials and attendees for a minimum of six years.

3. The training session focuses on, but is not limited to, the following subjects defined in Catalyze ‘s security policies and procedures:

    1. HIPAA Privacy, Security, and Breach notification rules;
    2. HITRUST Common Security Framework;
    3. NIST Security Rules;
    4. Risk Management procedures and documentation;
    5. Auditing. Catalyze may monitor access and activities of all users;
    6. Workstations may only be used to perform assigned job responsibilities;
    7. Users may not download software onto Catalyze’s workstations and/or systems without prior approval from the Security Officer;
    8. Users are required to report malicious software to the Security Officer immediately;
    9. Users are required to report unauthorized attempts, uses of, and theft of Catalyze’s systems and/or workstations;
    10. Users are required to report unauthorized access to facilities
    11. Users are required to report noted log-in discrepancies (i.e. application states users last log-in was on a date user was on vacation;
    12. Users may not alter ePHI maintained in a database, unless authorized to do so by a Catalyze Customer;
    13. Users are required to understand their role in Catalyze’s contingency plan;
    14. Users may not share their user names nor passwords with anyone;
    15. Requirements for users to create and change passwords;
    16. Users must set all applications that contain or transmit ePHI to automatically log off after “X” minutes of inactivity;
    17. Supervisors are required to report terminations of workforce members and other outside users;
    18. Supervisors are required to report a change in a users title, role, department, and/or location;
    19. Procedures to backup ePHI;
    20. Procedures to move and record movement of hardware and electronic media containing ePHI;
    21. Procedures to dispose of discs, cds, hard drives, and other media containing ePHI;
    22. Procedures to re-use electronic media containing ePHI;

23. SSH key and sensitive document encryption procedures.

## Security Officer

The Security Officer is responsible for facilitating the training and supervision of all workforce members [164.308(a)(3)(ii)(A) and 164.308(a)(5)(ii)(A)], investigation and sanctioning of any workforce member that is in violation of Catalyze security policies and non-compliance with the security regulations [164.308(a)(1)(ii)(c)], and writing, implementing, and maintaining all polices, procedures, and documentation related to efforts toward security and compliance [164.316(a-b)].

The current Catalyze Security Officer is Benjamin Uphoff (ben@catalyze.io).

## Organizational Responsibilities

The Security Officer, in collaboration with the Privacy Officer, is responsible for facilitating the development, implementation, and oversight of all activities pertaining to Catalyze's efforts to be compliant with the HIPAA Security Regulations, HITRUST CSF, and any other security and compliance frameworks. The intent of the Security Officer Responsibilities is to maintain the confidentiality, integrity, and availability of ePHI. These organizational responsibilities include, but are not limited to the following:

1. Oversees and enforces all activities necessary to maintain compliance and verifies the activities are in alignment with the requirements.

2. Helps to establishe and maintain written policies and procedures to comply with the Security rule and maintains them for six years from the date of creation or date it was last in effect, whichever is later.

3. Updates policies and procedures as necessary and appropriate to maintain compliance and maintains changes made for six years from the date of creation or date it was last in effect, whichever is later.

4. Facilitates audits to validate compliance efforts throughout the organization.

5. Documents all activities and assessments completed to maintain compliance and maintains documentation for six years from the date of creation or date it was last in effect, whichever is later.

6. Provides copies of the policies and procedures to management, customers, and partners, and has them available to review by all other workforce members to which they apply.

7. Annually, and as necessary, reviews and updates documentation to respond to environmental or operational changes affecting the security and risk posture of ePHI stored, transmitted, or processed within Catalyze infrastructure.

8. Develops and provides periodic security updates and reminder communications for all workforce members.

9. Implements procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it may be accessed.

10. Maintains a program promoting workforce members to report non-compliance with policies and procedures.
    1. Promptly, properly, and consistently investigates and addresses reported violations and takes steps to prevent recurrence.
    2. Applies consistent and appropriate sanctions against workforce members who fail to comply with the security policies and procedures of Catalyze.
    3. Mitigates, to the extent practicable, any harmful effect known to Catalyze of a use or disclosure of ePHI in violation of Catalyze's policies and procedures, even if effect is the result of actions of Catalyze business associates, customers, and/or partners.

11. Reports security efforts and incidents to administration immediately upon discovery. Responsibilities in the case of a known ePHI breach are documented in the Catalyze Breach Policy .

12. The Security Officer facilitates the communication of security updates and reminders to all workforce members to which it pertains. Examples of security updates and reminders include, but are not limited to:
    1. Latest malicious software or virus alerts;
    2. Catalyze's requirement to report unauthorized attempts to access ePHI;
    3. Changes in creating or changing passwords;
    4. Additional security-focused training is provided to all workforce members by the Security Officer. This training includes, but is not limited to:
        1. Data backup plans;
        2. System auditing procedures;
        3. Redundancy procedures;
        4. Contingency plans;
        5. Virus protection;
        6. Patch management;
        7. Media Disposal and/or Re-use;
        8. Documentation requirements.

### Supervision of Workforce Responsibilities

Although the Security Officer is responsible for implementing and overseeing all activities related to maintaining compliance, it is the responsibility of all workforce members (i.e. team leaders, supervisors, managers, directors, co-workers, etc.) to supervise all workforce members and any other user of Catalyze's systems, applications, servers, workstations, etc. that contain ePHI.

1. Monitor workstations and applications for unauthorized use, tampering, and theft and report non-compliance according to the Security Incident Response policy.

2. Assist the Security and Privacy Officers to ensure appropriate role-based access is provided to all users.

3. Take all reasonable steps to hire, retain, and promote workforce members and provide access to users who comply with the Security regulation and Catalyze's security policies and procedures.

### Sanctions of Workforce Responsibilities

All workforce members report non-compliance of Catalyze's policies and procedures to the Security Officer or other individual as assigned by the Security Officer. Individuals that report violations in good faith may not be subjected to intimidation, threats, coercion, discrimination against, or any other retaliatory action as a consequence.

1. The Security Officer promptly facilitates a thorough investigation of all reported violations of Catalyze's security policies and procedures. The Security Officer may request the assistance from others.
    1. Complete an audit trail/log to identify and verify the violation and sequence of events.
    2. Interview any individual that may be aware of or involved in the incident.
        1. All individuals are required to cooperate with the investigation process and provide factual information to those conducting the investigation.
        2. Provide individuals suspected of non-compliance of the Security rule and/or Catalyze's policies and procedures the opportunity to explain their actions.
    3. The investigators thoroughly documents the investigation as the investigation occurs.

2. Violation of any security policy or procedure by workforce members may result in corrective disciplinary action, up to and including termination of employment. Violation of this policy and procedures by others, including business associates, customers, and partners may result in termination of the relationship and/or associated privileges. Violation may also result in civil and criminal penalties as determined by federal and state laws and regulations.
    1. A violation resulting in a breach of confidentiality (i.e. release of PHI to an unauthorized individual), change of the integrity of any ePHI, or inability to access any ePHI by other users, requires immediate termination of the workforce member from Catalyze.

3. The Security Officer facilitates taking appropriate steps to prevent recurrence of the violation (when possible and feasible).

4. The Security Officer maintains all documentation of the investigation, sanctions provided, and actions taken to prevent reoccurrence for a minimum of six years after the conclusion of the investigation.

## Data Management Policy

Catalyze has procedures to create and maintain retrievable exact copies of electronic protected health information (ePHI) stored in conjuction with Catalyze Add-ons and for PaaS Customers using our Backup Service. This policy, and associated procedures, do not apply to PaaS Customers that do not choose Catalyze Backup Service. The policy and procedures will assure that complete, accurate, retrievable, and tested back-ups are available for all information systems used by Catalyze, Inc.

Data backup is an important part of the day-to-day operations of Catalyze. To protect the confidentiality, integrity, and availability of ePHI, both for Catalyze and Catalyze Customers, completes backups to assure that data remains available when it needed. Established guidelines and defined standards for accountability of hardware and electronic media containing ePHI further provide the confidentiality, integrity, availability, and security of ePHI.

Failure to backup a system in the absence of a system failure is a violation of this policy and may result in corrective disciplinary action, up to and including termination of employment. Violation of this policy and its procedures by workforce members may result in corrective disciplinary action, up to and including termination of employment. Violation of this policy and procedures by others, including providers, providers' offices, developers, customers, business associates and partners may result in termination of the relationship and/or associated privileges. Violation may also result in civil and criminal penalties as determined by federal and state laws and regulations.

### Applicable Standards from the HITRUST Common Security Framework

- 01.v - Information Access Restriction

### Applicable Standards from the HIPAA Security Rule

- 164.308(a)(7)(ii)(A) - Data Backup Plan
- 164.310(d)(2)(iii) - Accountability
- 164.310(d)(2)(iv) - Data Backup and Storage

### Backup Policy and Procedures

1. Data Backup:
    1. Perform daily snapshot backups of all systems that process, store, or transmit ePHI for Catalyze Customers.
        1. Catalyze Ops Team, lead by VP of Engineering, is designated to be in charge of backups.
        2. Train individual(s) assigned to complete backups and manage the backup media.
    2. Document backups completed.
        1. Site/location name

    2. Name of the system
    3. Type of data
    4. Date & time of backup
    5. Where backup stored (or to whom it was provided)

3. Store backups in a manner that protects them from loss or environmental damage.
4. Periodically store backups off-site (as deemed appropriate).
5. Test backups and document that files have been completely and accurately restored from the backup media.

## System Access Policy

Access to Catalyze systems and application is limited for all users, including but not limited to workforce members, volunteers, business associates, contracted providers, consultants, and any other entity, is allowable only on a minimum necessary basis. All users are responsible for reporting an incident of unauthorized user or access of the organization's information systems. These safeguards have been established to address the HIPAA Security regulations including the following:

### Applicable Standards from the HITRUST Common Security Framework

- 01.d - User Password Management
- 01.f - Password Use
- 01.r - Password Management System
- 01.a - Access Control Policy
- 01.b - User Registration
- 01.h - Clear Desk and Clear Screen Policy
- 01.j - User Authentication for External Connections
- 01.q - User Identification and Authentication
- 01.v - Information Access Restriction
- 02.i - Removal of Access Rights
- 06.e - Prevention of Misuse of Information Assets

### Applicable Standards from the HIPAA Security Rule

- 164.308a4iiC Access Establishment and Modification
- 164.308a3iiB Workforce Clearance Procedures
- 164.308a4iiB Access Authorization
- 164.312d Person or Entity Authentication
- 164.312a2i Unique User Identification
- 164.308a5iiD Password Management

- 164.312a2iii Automatic Logoff
- 164.310b Workstation Use
- 164.310c Workstation Security
- 164.308a3iiC Termination Procedures

### Access Establishment and Modification

- Requests for access to Catalyze Platform systems and applications is made formally to the VP of Engineering, Privacy Officer, or Security Officer.
  - Access is not granted until receipt, review, and approval by one of the workforce roles listed above;
  - The request for access is retained for future reference.

### Workforce Clearance Procedures

- The level of security assigned to a user to the organization’s information systems is based on the minimum necessary amount of data access required to carry out legitimate job responsibilities assigned to a user’s job classification and/or to a user needing access to carry out treatment, payment, or healthcare operations.
- All access requests are treated on a ‘least-access principle”.
- Catalyze maintains a minimum necessary approach to access to Customer data. As such, Catalyze, including all workforce members, does not readily have access to any ePHI.

### Access Authorization

- Role based access categories for each Catalyze system and application are pre-approved by the Security Officer or VP of Engineering.

### Person or Entity Authentication

- Each workforce member has and uses a unique user ID and password that identifies him/her as the user of the information system.
- Each Customer and Partner has and uses a unique user ID and password that identifies him/her as the user of the information system.

### Unique User Identification

- Access to the Catalyze Platform systems and applications is controlled by requiring unique User Login ID’s and passwords for each individual user and developer.
- Passwords requirements mandate strong password controls (see below).
- Passwords are not displayed at any time and are not transmitted or stored in plain text.

### Automatic Logoff

- Users are required to make information systems inaccessible by any other individual when unattended by the users (ex. by using a password protected screen saver or logging off the system).
- Information systems automatically log users off the systems after 10 minutes of inactivity.
- The Security Officer pre-approves exceptions to automatic log off requirements.

### Workstation Use

All workstations at Catalyze are company owned, and all are laptop Apple products running Mac operating system.

- Workstations may not be used to engage in any activity that is illegal or is in violation of organization's policies.
    - Access may not be used for transmitting, retrieving, or storage of any communications of a discriminatory or harassing nature or materials that are obscene or "X-rated". Harassment of any kind is prohibited. No messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes, sexual preference, or health condition shall be transmitted or maintained. No abusive, hostile, profane, or offensive language is to be transmitted through organization's system.
    - Information systems/applications also may not be used for any other purpose that is illegal, unethical, or against company policies or contrary to organization's best interests. Messages containing information related to a lawsuit or investigation may not be sent without prior approval.
    - Solicitation of non-company business, or any use of organization's information systems/applications for personal gain is prohibited.
    - Transmitted messages may not contain material that criticizes organization, its providers, its employees, or others.
    - Users may not misrepresent, obscure, suppress, or replace another user's identity in transmitted or stored messages.
    - Workstation hard drives will be encrypted using FileVault 2.0.
    - All workstations have firewalls enabled to prevent unauthorized access unless explicitly granted.

### Termination Procedures

- The Human Resources Department (or other designated department), users, and their supervisors are required to notify the Security Officer upon completion and/or termination of access needs and facilitating completion of the "Termination Checklist".
- The Human Resources Department, users, and supervisors are required to notify the IS Help Desk to terminate a user's access rights if there is evidence or reason to believe the following (these incidents are also reported on an incident report and is filed with the Privacy Officer):
    - The user has been using their access rights inappropriately;

    - A user's password has been compromised (a new password may be provided to the user if the user is not identified as the individual compromising the original password);
    - An unauthorized individual is utilizing a user's User Login ID and password (a new password may be provided to the user if the user is not identified as providing the unauthorized individual with the User Login ID and password).
- The Security Officer will terminate users' access rights immediately upon notification.
- The Security Officer audits and may terminate access of users that have not logged into organization's information systems/applications for an extended period of time.

### Paper Records

Catalyze does not use paper records for any sensitive information. Use of paper for recording and storing sensitive data is against Catalyze policies.

### Password Management

- User IDs and passwords are used to control access to Catalyze systems and may not be disclosed to anyone for any reason.
- Users may not allow anyone, for any reason, to have access to any information system using another user's unique user ID and password.
- On all production systems and application in the Catalyze environment, password configurations are set to require that passwords are a minimum of 7 character length, 90 day password expiration, account lockout after 5 invalid attempts, password history of last 4 passwords remembered, and account lockout after 15 minutes of inactivity.
- All system and application passwords are hashed by concatenating the user's password and a random 256-bit salt value, generated on a per-user basis, and then applying SHA–256 to the value to create a password hash. The password hash and the salt are then stored in the backend database and are used for password validation on future user authentication attempts.* Each information system automatically requires users to change passwords at a pre-determined interval as determined by the organization, based on the criticality and sensitivity of the ePHI contained within the network, system, application, and/or database.
- Passwords are inactivated immediately upon an employee's termination (refer to the termination procedures in this policy).
- All default system, application, and Partner passwords are changed before deployment to production.
- All passwords used in configuration scripts are secured and encrypted.
- If a user believes their user ID has been compromised, they are required to immediately report the incident to the Security Office.

## Auditing Policy

Catalyze shall 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. Catalyze 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.

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

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

This policy applies to all Catalyze Add-on systems, including BaaS, that store, transmit, or process ePHI. This policy, and associated procedures, do not apply to PaaS Customers that do not choose Catalyze Logging Service.

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

### Auditing Policies

1. Responsibility for auditing information system access and activity is assigned to Catalyze's Security Officer. The Security Officer shall:
    1. Assign the task of generating reports for audit activities to the workforce member responsible for the application, system, or network;
    2. 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;
    3. 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. Catalyze's auditing processes shall address access and activity at the following levels listed below. In the case of PaaS Custoners, Application and User level auditing is the responsibility of the Customer; Catalyze provides software to aggregate and view User and Application logs, but the log data collected is the responsibility of the PaaS Customer. 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.
    1. 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.
    2. Application: Application level audit trails generally monitor and log all user activities, including data accessed and modified and specific actions.
    3. System: System level audit trails generally monitor and log user activities, applications accessed, and other system defined specific actions. Catalyze utilizes file system monitoring from OSSEC to assure the integrity of file system data.
    4. Network: Network level audit trails generally monitor information on what is operating, penetrations, and vulnerabilities.

3. Catalyze shall log all incoming and outgoing traffic to into and out of its 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 to Catalyze.

4. Catalyze treats its Developer Portal as a Platform Add-on and, as such, it logs all activity associated with Developer Portal Access.

5. Catalyze uses OSSEC to monitor the integrity of log files by utilizing OSSEC System Integrity Checking capabilities.

6. Catalyze shall identify "trigger events" or criteria that raise awareness of questionable conditions of viewing of confidential information. The "events" may be applied to the entire Catalyze Plaform or may be specific to a Customer, partner, business associate, Platform Add-on or application (See Listing of Potential Trigger Events below).

7. In addition to trigger events, Catalyze utilizes OSSEC log correlation functionality to proactively identify and enable alerts based on log data.

8. Catalyze's Security Officer and Privacy Officer are authorized to select and use auditing tools that are designed to detect network vulnerabilities and intrusions. Such tools are explicitly prohibited by others, including Customers and Partners, without the explicit authorization of the Security Officer. These tools may include, but are not limited to:
    - Scanning tools and devices;
    - Password cracking utilities;
    - Network "sniffers."
    - Passive and active intrusion detection systems.

9. The process for review of audit logs, trails, and reports shall include:
    1. Description of the activity as well as rationale for performing the audit.
    2. Identification of which Catalyze workforce members will be responsible for review (workforce members shall not review audit logs that pertain to their own system activity).
    3. Frequency of the auditing process.
    4. Determination of significant events requiring further review and follow-up.
    5. Identification of appropriate reporting channels for audit results and required follow-up.

10. Vulnerability testing software may be used to probe the network to identify what is running (e.g., operating system or product versions in place), whether publicly-known vulnerabilities have been corrected, and evaluate whether the system can withstand attacks aimed at circumventing security controls.
    - Testing may be carried out internally or provided through an external third-party vendor. Whenever possible, a third party auditing vendor should not be providing the organization IT oversight services (e.g., vendors providing IT services should not be auditing their own services – separation of duties).
    - Testing shall be done on a routine basis, currently monthly.

11. Software patches and updates will be applied to all systems in a timely manner. In the case of routine updates, they will be applied after thorough testing. In the case of updates to correct known vulnerabilities, priority will be given to testing to speed the time to production.
    - In the case of PaaS Customers, updates to Application and Database versions are the responsibilty of Customers, though Catalyze will, at it's own discretion, notify and recommend updates to customer systems.

### 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 application 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 Catalyze's Privacy or Security Officer.

3. A request for an audit must be approved by Catalyze's Privacy Officer and/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.
   - Should the audit disclose that a workforce member has accessed ePHI inappropriately, the minimum necessary/least privileged information shall be shared with Catalyze's Security Officer to determine appropriate sanction/ corrective disciplinary action.
   - 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 Catalyze's Privacy Officer or designee. Prior to communicating with customers and partners regarding an audit, it is recommended that Catalyze consider seeking risk management and/or legal counsel.

### 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. Catalyze's 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/or legal counsel approval.

4. Security audits constitute an internal, confidential monitoring practice that may be included in Catalyze's 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 e PHI 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.

### Auditing Customer and Partner Activity

1. Periodic monitoring of Customer and Partner activity shall be carried out to ensure that access

and activity is appropriate for privileges granted and necessary to the arrangement between Catalyze and the 3rd party. Catalyze will make every effort to assure Customers and Partners do not gain access to data outside of their own Environments.

2. If it is determined that the Customer or Partner has exceeded the scope of access privileges, Catalyze's leadership must remedy the problem immediately.

3. If it is determined that a Customer or Partner has violated the terms of the HIPAA business associate agreement or any terms within the HIPAA regulations, Catalyze must take immediate action to remediate the situation. Continued violations may result in discontinuation of the business relationship.

### 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. For PaaS Customers, it is the responsibility of the Customer to encrypt log data before it is sent to Catalyze Logging Service.

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.

4. For PaaS Customers choosing to use Catalyze logging services, log data will be separated from the log data of other Catalyze Customers.

### Workforce Training, Education, Awareness and Responsibilities

1. Catalyze workforce members are provided training, education, and awareness on safeguarding the privacy and security of business and ePHI. Catalyze's 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. Catalyze workforce members are made aware of responsibilities with regard to privacy and security of information as well as applicable sanctions/corrective disciplinary actions should the auditing process detect a workforce member's failure to comply with organizational policies.
2. Catalyze Customers are provided with necessary information to understand Catalyze auditing capabilities, and PaaS Customers can choose the level of logging and auditing that Catalyze will implement on their behalf.

### External Audits of Information Access and Activity

1. Prior to contracting with an external audit firm, Catalyze 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: A. Organizational history and experience. B. Available storage space.

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

3. Log data is currently retained and readily accessible for a 1 month period. Beyond that, log data is available via cold backup.

4. For Paas Customers, they choose the length of backup retention and availability that Catalyze will implement and enforce.

### 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.

## Facility Access Policy

Catalyze works with Subcontractors to assure restriction of physical access to systems used as part of the Catalyze Platform. Catalyze and its Subcontractors control access to the physical buildings/facilities that house these systems/applications, or in which Catalyze workforce members operate, in accordance to the HIPAA Security Rule 164.310 and its implementation specifications. Physical Access to all of Catalyze facilities is limited to only those authorized in this policy. In an effort to safeguard ePHi from unauthorized access, tampering, and theft, access is allowed to areas only to those persons authorized to be in them and with escorts for unauthorized persons. All workforce members are responsible for reporting an incident of unauthorized visitor and/or unauthorized access to Catalyze's facility.

Of note, Catalyze does not have ready access to ePHI, it provides cloud-based, compliant infrastructure to covered entities and business associates. Catalyze does not house any systems used by its Platform in Catalyze facilities.

### Applicable Standards from the HITRUST Common Security Framework

- 08.b - Physical Entry Controls
- 08.d - Protecting Against External and Environmental Threats
- 08.j - Equipment Maintenance
- 08.l - Secure Disposal or Re-Use of Equipment
- 09.p - Disposal of Media

### Applicable Standards from the HIPAA Security Rule

- 164.310(a)(2)(ii) Facility Security Plan
- 164.310(a)(2)(iii) Access Control & Validation Procedures
- 164.310(b-c) Workstation Use & Security

### Catalyze-controlled Facility Access Policies

1. Visitor and third party support access is recorded and supervised. All visitors are escorted.

2. Repairs are documented and the documentation is retained.

3. Fire extinguishers and detectors are installed according to applicable laws and regulations.

4. Maintenance is controlled and conducted by authorized personnel in accordance with supplier-recommended intervals, insurance policies and the organizations maintenance program.

5. Electronic and physical media containing covered information is securely destroyed (or the information securely removed) prior to disposal.

6. The organization securely disposes media with sensitive information.

7. Physical access is restricted using smartlocks that track all access.

    - Restricted areas and facilities are locked and when unattended (where feasible).
    - Only authorized workforce members receive access to restricted areas (as determined by the Security Officer).
    - Access and keys are revoked upon termination of workforce members.
    - Workforce members must report a lost and/or stolen key(s) to the Security Officer.

    - The Security Officer facilitates the changing of the lock(s) within 7 days of a key being reported lost/stolen

8. Enforcement of Facility Access Policies
    - Report violations of this policy to the restricted area's department team leader, supervisor, manager, or director, or the Privacy Officer.
    - Workforce members in violation of this policy are subject to disciplinary action, up to and including termination.
    - Visitors in violation of this policy are subject to loss of vendor privileges and/or termination of services from Catalyze.
9. Workstation Security
    - Workstations may only be accessed and utilized by authorized workforce members to complete assigned job/contract responsibilities.
    - All workforce members are required to monitor workstations and report unauthorized users and/or unauthorized attempts to access systems/applications as per the System Access Policy.
    - All workstations purchased by Catalyze are the property of Catalyze and are distributed to users by the company.

## Incident Response Policy

Catalyze implements an information security incident response process to consistently detect, respond, and report incidents, minimize loss and destruction, mitigate the weaknesses that were exploited, and restore information system functionality and business continuity as soon as possible.

The incident response process addresses:

- Continuous monitoring of threats through intrusion detection systems (IDS) and other monitoring applications;
- Establishment of an information security incident response team;
- Establishment of procedures to respond to media inquiries;
- Establishment of clear procedures for identifying, responding, assessing, analyzing, and follow-up of information security incidents;
- Workforce training, education, and awareness on information security incidents and required responses; and
- Facilitation of clear communication of information security incidents with internal, as well as external, stakeholders

### Applicable Standards from the HITRUST Common Security Framework

- 02.f - Disciplinary Process
- 06.f - Prevention of Misuse of Information Assets

- 11.a - Reporting Information Security Events
- 11.c - Responsibilities and Procedures
- 11.a - Reporting Information Security Events

### Applicable Standards from the HIPAA Security Rule

- 164.308(a)(5)(i) – Security Awareness and Training
- 164.308(a)(6) – Security Incident Procedures

### Incident Management Policies

The Catalyze incident response process follows the process recommended by SANS, an industry leader in security (www.sans.org). Process flows are a direct representation of the SANS process. Review Appendix 1 for a flowchart identifying each phase.

**Identification Phase**:

1. Immediately upon observation Catalyze members report suspected and known Precursors, Events, Indications, and Incidents in one of the following ways: 4. Direct report to management, the Security Officer, Privacy Officer, or other; 5. Email; 6. Phone call; 7. Secure Chat. 8. Anonymously through workforce members desired channels.
    1. The individual receiving the report facilitates completion of an Incident Identification form and notifies the Security Officer (if not already done).
    2. The Security Officer determines if the issue is a Precursor, Incident, Event, or Incident.
        1. If the issue is an event, indication, or precursor the Security Officer forwards it to the appropriate resource for resolution.
            1. Non-Technical Event (minor infringement): the Security Officer completes a SIR Form (see Appendix 2) and investigates the incident.
            2. Technical Event: Assign the issue to an IT resource for resolution. This resource may also be a contractor or outsourced technical resource, in the event of a small office or lack of expertise in the area.
        2. If the issue is a security incident the Security Officer activates the Security Incident Response Team (SIRT) and notifies senior management.
            1. If a non-technical security incident is discovered the SIRT completes the investigation, implements preventative measures, and resolves the security incident.
                1. Once the investigation is completed, progress to Phase V, Follow-up.
            2. If the issue is a technical security incident, commence to Phase II: Containment.
                1. The Containment, Eradication, and Recovery Phases are highly technical. It is important to have them completed by a highly qualified technical security resource with oversight by the SIRT team.
                2. Each individual on the SIRT and the technical security resource document all

measures taken during each phase, including the start and end times of all efforts.

3. The lead member of the SIRT team facilitates initiation of a Security Incident Report (SIR) Form (See Appendix 2 for sample format) or an Incident Survey Form (See Appendix 4). The intent of the SIR form is to provide a summary of all events, efforts, and conclusions of each Phase of this policy and procedures.

3. The Security Officer, Privacy Officer, or Catalyze representative appointed notifies any affected Customers and Partners. If no Customers and Partners are affectted, notification is at the discretion of the Security and Privacy Officer.

**Containment Phase (Technical)**

In this Phase, Catalyze’s IT department attempts to contain the security incident. It is extremely important to take detailed notes during the security incident response process. This provides that the evidence gathered during the security incident can be used successfully during prosecution, if appropriate.

1. The SIRT reviews any information that has been collected by the Security Officer or any other individual investigating the security incident.
2. The SIRT secures the network perimeter.
3. The IT department performs the following:
    1. Securely connect to the affected system over a trusted connection.
    2. Retrieve any volatile data from the affected system.
    3. Determine the relative integrity and the appropriateness of backing the system up.
    4. If appropriate, back up the system.
    5. Change the password(s) to the affected system(s).
    6. Determine whether it is safe to continue operations with the affect system(s).
        1. If it is safe, allow the system to continue to function;
            1. Complete any documentation relative to the security incident on the SIR Form.
            2. Move to Phase V, Follow-up.
        2. If it is NOT safe to allow the system to continue operations, discontinue the system(s) operation and move to Phase III, Eradication.
    7. The individual completing this phase provides written communication to the SIRT.
4. Continuously apprise Senior Management of progress.
5. Continue to notify affected Customers and Partners with relevant updates as needed

**Eradication Phase (Technical)**

The Eradication Phase represents the SIRT’s effort to remove the cause, and the resulting security exposures, that are now on the affected system(s).

1. Determine symptoms and cause related to the affected system(s).
2. Strengthen the defenses surrounding the affected system(s), where possible (a risk assessment may be needed and can be determined by the Security Officer). This may include the following:
    1. An increase in network perimeter defenses.
    2. An increase in system monitoring defenses.
    3. Remediation (“fixing”) any security issues within the affected system, such as removing unused services/general host hardening techniques.
3. Conduct a detailed vulnerability assessment to verify all the holes/gaps that can be exploited have been addressed.
    1. If additional issues or symptoms are identified, take appropriate preventative measures to eliminate or minimize potential future compromises.
4. Complete the Eradication Form (see Appendix 4).
5. Update the documentation with the information learned from the vulnerability assessment, including the cause, symptoms, and the method used to fix the problem with the affected system(s).
6. Apprise Senior Management of the progress.
7. Continue to notify affected Customers and Partners with relevant updates as needed.
8. Move to Phase IV, Recovery.

**Recovery Phase (Technical)**

The Recovery Phase represents the SIRT’s effort to restore the affected system(s) back to operation after the resulting security exposures, if any, have been corrected.

1. The technical team determines if the affected system(s) have been changed in any way.
    1. If they have, the technical team restores the system to its proper, intended functioning (“last known good”).
        1. Once restored, the team validates that the system functions the way it was intended/had functioned in the past. This may require the involvement of the business unit that owns the affected system(s).
        2. If operation of the system(s) had been interrupted (i.e., the system(s) had been taken offline or dropped from the network while triaged), restart the restored and validated system(s) and monitor for behavior.
        3. If the system had not been changed in any way, but was taken offline (i.e., operations had been interrupted), restart the system and monitor for proper behavior.
    2. Update the documentation with the detail that was determined during this phase.
    3. Apprise Senior Management of progress.
    4. Continue to notify affected Customers and Partners with relevant updates as needed.

5. Move to Phase V, Follow-up.

**Follow-up Phase (Technical and Non-Technical)**

The Follow-up Phase represents the review of the security incident to look for “lessons learned” and to determine whether the process that was taken could have been improved in any way. It is recommended all security incidents be reviewed shortly after resolution to determine where response could be improved. Timeframes may extend to one to two weeks post-incident.

1. Responders to the security incident (SIRT Team and technical security resource) meet to review the documentation collected during the security incident.
2. Create a “lessons learned” document and attach it to the completed SIR Form.
    1. Evaluate the cost and impact of the security incident to Catalyze using the documents provided by the SIRT and the technical security resource.
    2. Determine what could be improved.
    3. Communicate these findings to Senior Management for approval and for implementation of any recommendations made post-review of the security incident.
    4. Carry out recommendations approved by Senior Management; sufficient budget, time and resources should be committed to this activity.
    5. Close the security incident.

**Periodic Evaluation**

It is important to note that the processes surrounding security incident response should be periodically reviewed and evaluated for effectiveness. This also involves appropriate training of resources expected to respond to security incidents, as well as the training of the general population regarding the Catalyze’s expectation for them, relative to security responsibilities. The incident response plan is tested annually.

### Security Incident Response Team (SIRT)

Individuals needed and responsible to respond to a security incident make up a Security Incident Response Team (SIRT). Members may include the following:

- Security Officer
- Privacy Officer
- Senior Management
- VP of Engineering

## Breach Policy

To provide guidance for breach notification when impermissive or unauthorized access, acquisition, use and/or disclosure of the ePHI occurs. Breach notification will be carried out in compliance with the American Recovery and Reinvestment Act (ARRA)/Health Information Technology for Economic and Clinical Health Act (HITECH) as well as any other federal or state notification law.

The Federal Trade Commission (FTC) has published breach notification rules for vendors of personal health records as required by ARRA/HITECH. The FTC rule applies to entities not covered by HIPAA, primarily vendors of personal health records. The rule is effective September 24, 2009 with full compliance required by February 22, 2010.

The American Recovery and Reinvestment Act of 2009 (ARRA) was signed into law on February 17, 2009. Title XIII of ARRA is the Health Information Technology for Economic and Clinical Health Act (HITECH). HITECH significantly impacts the Health Insurance Portability and Accountability (HIPAA) Privacy and Security Rules. While HIPAA did not require notification when patient protected health information (PHI) was inappropriately disclosed, covered entities and business associates may have chosen to include notification as part of the mitigation process. HITECH does require notification of certain breaches of unsecured PHI to the following: individuals, Department of Health and Human Services (HHS), and the media. The effective implementation for this provision is September 23, 2009 (pending publication HHS regulations).

In the case of a breach, Catalyze shall notify all affected Customers. It is the responsibility of the Customers to notify affected individuals.

### Applicable Standards from the HITRUST Common Security Framework

- 11.a Reporting Information Security Events
- 11.c Responsibilities and Procedures

### Applicable Standards from the HIPAA Security Rule

- Security Incident Procedures - 164.308(a)(6)(i)
- HITECH Notification in the Case of Breach - 13402(a) and 13402(b)
- HITECH Timeliness of Notification - 13402(d)(1)
- HITECH Content of Notification - 13402(f)(1)

### Catalyze Breach Policy

1. Discovery of Breach: A breach of ePHI shall be treated as “discovered” as of the first day on which such breach is known to the organization, or, by exercising reasonable diligence would have been known to Catalyze (includes breaches by the organization’s Customers, Partners, or subcontractors). Catalyze shall be deemed to have knowledge of a breach if such breach is known or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or Partner of the organization. Following the discovery of a potential breach, the organization shall begin an investigation (see organizational policies for security incident response and/or risk management incident response) immediately, conduct a risk assessment, and based on the results of the risk assessment, begin the process to notify each Customer affected by the breach. Catalyze shall

also begin the process of determining what external notifications are required or should be made (e.g., Secretary of Department of Health & Human Services (HHS), media outlets, law enforcement officials, etc.)

2. Breach Investigation: The Catalyze Security Officer shall name an individual to act as the investigator of the breach (e.g., privacy officer, security officer, risk manager, etc.). The investigator shall be responsible for the management of the breach investigation, completion of a risk assessment, and coordinating with others in the organization as appropriate (e.g., administration, security incident response team, human resources, risk management, public relations, legal counsel, etc.) The investigator shall be the key facilitator for all breach notification processes to the appropriate entities (e.g., HHS, media, law enforcement officials, etc.). All documentation related to the breach investigation, including the risk assessment, shall be retained for a minimum of six years. A template breach log is located here.

3. Risk Assessment: For an acquisition, access, use or disclosure of ePHI to constitute a breach, it must constitute a violation of the HIPAA Privacy Rule. A use or disclosure of ePHI that is incident to an otherwise permissible use or disclosure and occurs despite reasonable safeguards and proper minimum necessary procedures would not be a violation of the Privacy Rule and would not qualify as a potential breach. To determine if an impermissible use or disclosure of ePHI constitutes a breach and requires further notification, the organization will need to perform a risk assessment to determine if there is significant risk of harm to the individual as a result of the impermissible use or disclosure. The organization shall document the risk assessment as part of the investigation in the incident report form noting the outcome of the risk assessment process. The organization has the burden of proof for demonstrating that all notifications to appropriate Customers or that the use or disclosure did not constitute a breach. Based on the outcome of the risk assessment, the organization will determine the need to move forward with breach notification. The risk assessment and the supporting documentation shall be fact specific and address:
    - Consideration of who impermissibly used or to whom the information was impermissibly disclosed;
    - The type and amount of ePHI involved;
    - The cause of the breach, and the entity responsible for the breach, either Customer, Catalyze, or Partner.
    - The potential for significant risk of financial, reputational, or other harm.

4. Timeliness of Notification: Upon discovery of a breach, notice shall be made to the affected Catalyze Customers no later than 4 hours after the discovery of the breach. It is the responsibility of the organization to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of delay.

5. Delay of Notification Authorized for Law Enforcement Purposes: If a law enforcement official states to the organization that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, the organization shall:
    - If the statement is in writing and specifies the time for which a delay is required, delay such

    notification, notice, or posting of the timer period specified by the official; or
    - If the statement is made orally, document the statement, including the identify of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described above is submitted during that time.

6. Content of the Notice: The notice shall be written in plain language and must contain the following information:
    - A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
    - A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved), if known;
    - Any steps the Customer should take to protect Customer data from potential harm resulting from the breach.
    - A brief description of what Catalyze is doing to investigate the breach, to mitigate harm to individuals and Customers, and to protect against further breaches.
    - Contact procedures for individuals to ask questions or learn additional information, which may include a toll-free telephone number, an e-mail address, a web site, or postal address.

7. Methods of Notification: Catalyze Customers will be notified via email and phone within the timeframe for reporting breaches, as outlined above.

8. Maintenance of Breach Information/Log: As described above and in addition to the reports created for each incident, Catalyze shall maintain a process to record or log all breaches of unsecurede ePHI regardless of the number of records and Customers affected. The following information should be collected/logged for each breach (see sample Breach Notification Log):
    - A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of records and Customers affected, if known.
    - A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, etc.), if known.
    - A description of the action taken with regard to notification of patients regarding the breach.
    - Resolution steps taken to mitigate the breach and prevent future occurrences.

9. Workforce Training: Catalyze shall train all members of its workforce on the policies and procedures with respect to ePHI as necessary and appropriate for the members to carry out their job responsibilities. Workforce members shall also be trained as to how to identify and report breaches within the organization.

10. Complaints: Catalyze must provide a process for individuals to make complaints concerning the

organization’s patient privacy policies and procedures or its compliance with such policies and procedures.

11. Sanctions: The organization shall have in place and apply appropriate sanctions against members of its workforcem, Customers, and Partners who fail to comply with privacy policies and procedures.

12. Retaliation/Waiver: Catalyze may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any privacy right. The organization may not require individuals to waive their privacy rights under as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

### Catalyze PaaS Customer Responsibilities

1. The Catalyze Customer that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured ePHI shall, without unreasonable delay and in no case later than 60 calendar days after discovery of a breach, notify Catalyze of such breach. The Customer shall provide Catalyze with the following information:
    - A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of records and Customers affected, if known.
    - A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, etc.), if known.
    - A description of the action taken with regard to notification of patients regarding the breach.
    - Resolution steps taken to mitigate the breach and prevent future occurrences.

2. Notice to Media: Catalyze Customers are responsible for providing notice to prominent media outlets at the Customer’s discretion.

3. Notice to Secretary of HHS: Catalyze Customers are responsible for providing notice to the Secretary of HHS at the Customer’s discretion.

### Sample Letter to Customers in Case of Breach

[Date]

[Name here][Address 1 Here] [Address 2 Here][City, State Zip Code]

Dear [Name of Customer]:

I am writing to you from Catalyze, Inc. with important information about a recent breach that affects your account with us. We became aware of this breach on [Insert Date] which occurred on or about [Insert Date]. The breach occurred as follows:

Describe event and include the following information: A. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known. B. A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved), if known. C. Any steps the Customer should take to protect themselves from potential harm resulting from the breach. D. A brief description of what Catalyze is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches. E. Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, web site, or postal address.

Other Optional Considerations:

- Recommendations to assist customer in remedying the breach.

We will assist you in remedying the situation.

Sincerely,

Travis Good Co-founder, Catalyze, Inc travis@catalyze.io 303–351–2640

## Disaster Recover Policy

The Catalyze Contingency Plan establishes procedures to recover Catalyze following a disruption resulting from a disaster. This policy, and associated procedures, do not apply to PaaS Customers that do not choose Catalyze Disaster Recovery Service.

The following objectives have been established for this plan:

1. Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
    1. *Notification/Activation phase* to detect and assess damage and to activate the plan;
    2. *Recovery phase* to restore temporary IT operations and recover damage done to the original system;
    3. *Reconstitution phase* to restore IT system processing capabilities to normal operations.
2. Identify the activities, resources, and procedures needed to carry out Catalyze processing requirements during prolonged interruptions to normal operations.
3. Assign responsibilities to designated OPDIV personnel and provide guidance for recovering Catalyze during prolonged periods of interruption to normal operations.
4. Ensure coordination with other Catalyze staff who will participate in the contingency planning strategies.
5. Ensure coordination with external points of contact and vendors who will participate in the contingency planning strategies.

This Catalyze Contingency Plan has been developed as required under the Office of Management and Budget (OMB) Circular A–130, Management of Federal Information Resources, Appendix III, November 2000, and the Health Insurance Portability and Accountability Act (HIPAA) Final Security Rule, Section §164.308(a) (7), which requires the establishment and implementation of procedures for responding to events that damage systems containing electronic protected health information.

This Catalyze Contingency Plan is promulgated under the legislative requirements set forth in the Federal Information Security Management Act (FISMA) of 2002 and the guidelines established by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800–34, titled “Contingency Planning Guide for Information Technology Systems” dated June 2002.

This Catalyze Contingency Plan complies with the OPDIV IT Contingency Planning Policy as follows:

> The organization shall develop a contingency planning capability to meet the needs of critical supporting operations in the event of a disruption extending beyond 48 hours. The procedures for execution of such a capability shall be documented in a formal contingency plan and shall be reviewed at least annually and updated as necessary. Personnel responsible for target systems shall be trained to execute contingency procedures. The plan, recovery capabilities, and personnel shall be tested to identify weaknesses of the capability at least annually.

The Catalyze Contingency Plan also complies with the following federal and departmental policies:

- The Computer Security Act of 1987;
- OMB Circular A–130, Management of Federal Information Resources, Appendix III, November 2000;
- Federal Preparedness Circular (FPC) 65, Federal Executive Branch Continuity of Operations, July 1999;
- Presidential Decision Directive (PDD) 67, Enduring Constitutional Government and Continuity of Government Operations, October 1998;
- PDD 63, Critical Infrastructure Protection, May 1998;
- Federal Emergency Management Agency (FEMA), The Federal Response Plan (FRP), April 1999;
- Defense Authorization Act (Public Law 106–398), Title X, Subtitle G, “Government Information Security Reform,” October 30, 2000

Example of the types of disasters that would initiate this plan are natural disaster, political disturbances, man made disaster, external human threats, internal malicious activties.

### Applicable Standards from the HITRUST Common Security Framework

- 12.c - Developing and Implementing Continuity Plans Including Information Security

### Applicable Standards from the HIPAA Security Rule

- 164.308(a)(7)(i) - Contingency Plan

### Line of Succession

OPDIV sets forth an order of succession to ensure that decision-making authority for the Catalyze Contingency Plan is uninterrupted. The Chief Technology Officer (CTO) and Security Officer, Ben Uphoff, and VP of Engineering, Brian Lewis, are responsible for ensuring the safety of personnel and the execution of procedures documented within this Catalyze Contingency Plan. If the CTO and VP of Engineering are unable to function as the overall authority or chooses to delegate this responsibility to a successor, the CEO or CPO shall function as that authority. To provide contact initiation should the contingency plan need to be initiated, please use the contact list below.

- Ben Uphoff, CTO: 414–335–0253, ben@catalyze.io
- Brian Lewis, VP of Engineering: 210–589–0014, b@catalyze.io
- Travis Good, CEO: 303–351–2640, travis@catalyze.io
- Mohan Balachandran, CPO: 214–215–7998, mohan@catalyze.io

### Responsibilities

The following teams have been developed and trained to respond to a contingency event affecting the IT system.

1. The **Ops Team** is responsible for recovery of the Catalyze hosted environment, network devices, and all servers. Members of the team include personnel who are also responsible for the daily operations and maintenance of Catalyze. The team leader is the VP of Engineering and directs the Dev Ops Team.
2. The **Web Services Team** is responsible for assuring all application servers, web services, and platform add-ons are working. It is also responsible for testing redeployments and assessing damage to the environment. The team leader is the CTO and directs the Web Services Team.

### Testing and Maintenance

The CTO and VP of Engineering shall establish criteria for validation/testing of a Contingency Plan, an annual test schedule, and ensure implementation of the test. This process will also serve as training for personnel involved in the plan’s execution. At a minimum the Contingency Plan shall be tested annually (within 365 days). The types of validation/testing exercises include tabletop and technical testing. Contingency Plans for all application systems must be tested at a minimum using the tabletop testing process. However, if the application system Contingency Plan is included in the technical testing of their respective support systems that technical test will satisfy the annual requirement.

*Tabletop Testing*

Tabletop Testing is conducted in accordance with the CMS Contingency Planning Tabletop Test

Procedures. The primary objective of the tabletop test is to ensure designated personnel are knowledgeable and capable of performing the notification/activation requirements and procedures as outlined in the CP, in a timely manner. The exercises include, but are not limited to:

- Testing to validate the ability to respond to a crisis in a coordinated, timely, and effective manner, by simulating the occurrence of a specific crisis; and
- Crisis communications and call tree verification.

*Technical Testing*

The primary objective of the technical test is to ensure the communication processes and data storage and recovery processes can function at an alternate site to perform the functions and capabilities of the system within the designated requirements. Technical testing shall include, but is not limited to:

- Process from backup system at the alternate site;
- Restore system using backups; and
- Switch voice and data telecommunications to alternate processing site.

### 1. Notification and Activation Phase

This phase addresses the initial actions taken to detect and assess damage inflicted by a disruption to Catalyze. Based on the assessment of the Event, sometimes according to the Catalyze Incident Response Policy, the Contingecy Plan may be activated by either the CTO or VP of Engineering.

Contact information for key personnel is located in Appendix A. The notification sequence is listed below:

- The first responder is to notify the CTO. All known information must be relayed to the CTO.

- The VP of Engineering is to contact the Web Services Team and inform them of the event. The CTO is to instruct all Team Leaders to begin assessment procedures.

- The CTO is to notify team members and direct them to complete the assessment procedures outlined below to determine the extent of damage and estimated recovery time. If damage assessment cannot be performed locally because of unsafe conditions, the CTO is to following the steps below.
    - Damage Assessment Procedures:
        - The CTO and VP of Engineering are to logically assess damage, gain insight into whether the infrastructure is salvageable, and begin to formulate a plan for recovery.

    - Alternate Assessment Procedures:
        - Upon notification from the CTO, the VP of Engineering is to follow the procedures for damage assessment with combined Dev Ops and Web Services Teams.

- The Catalyze Contingency Plan is to be activated if one or more of the following criteria are met:

  - Catalyze will be unavailable for more than 48 hours.
  - Hosting facility is damaged and will be unavailable for more than 24 hours.
  - Other criteria, as appropriate and as defined by Catalyze.
  - If the plan is to be activated, the CTO is to notify all Team Leaders and inform them of the details of the event and if relocation is required.
  - Upon notification from the CTO, Team Leaders are to notify their respective teams. Team members are to be informed of all applicable information and prepared to respond and relocate if necessary.
  - The CTO is to notify the hosting facility partners that a contingency event has been declared and to ship the necessary materials (as determined by damage assessment) to the alternate site.
  - The CTO is to notify remaining personnel and executive leadership on the general status of the incident.
    - Notification can be message, email, or phone.

### 2. Recovery Phase

This section provides procedures for recovering the application at an alternate site, whereas other efforts are directed to repair damage to the original system and capabilities.

The following procedures are for recovering the Catalyze infrastructure at the alternate site. Procedures are outlined per team required. Each procedure should be executed in the sequence it is presented to maintain efficient operations.

Recovery Goal: The goal is to rebuild Catalyze infrastructure to a production state.

The tasks outlines below are not sequential and some can be run in parallel.

1. Contact Partners and Customers affected - Web Services
2. Assess damage to the environment - Web Services
3. Begin replication of new environment. A this point it is determined whether to recover in AWS or in Rackspace. - Dev Ops
4. Test new environment using pre-written tests - Web Services
5. Test logging, security, and alerting functionality - Dev Ops
6. Deploy environment to production - Web Services
7. Update DNS to new environment. - Dev Ops

### 3. Reconstitution Phase

This section discusses activities necessary for restoring Catalyze operations at the original or new site. When the hosted data center at the original or new site has been restored, Catalyze operations at the alternate site may be transitioned back. The goal is to provide a seamless transition of operations from the alternate site to the computer center.

1. Original or New Site Restoration
    - Begin replication of new environment. - Dev Ops
    - Test new environment using pre-written tests. - Web Services
    - Test logging, security, and alerting functionality. - Dev Ops
    - Deploy environment to production - Web Services
    - Update DNS to new environment. - Dev Ops
2. Plan Deactivation

If the Catalyze environment is moved back to the original site from the alternative site, all hardware used at the alternate site should be handled and disposed of according to the Catalyze Media Disposal Policy.

## Disposable Media Policy

Catalyze recognizes that media containing ePHI may be reused when appropriate steps are taken to ensure that all stored ePHI has been effectively rendered inaccessible. Destruction/disposal of ePHI shall be carried out in accordance with federal and state law. The schedule for destruction/disposal shall be suspended for ePHI involved in any open investigation, audit, or litigation.

Catalyze utilizes dedicated hardware from Subcontractors. ePHI is only stored on SD volumes in our hosted environment. All SD volumes utilized by Catalyze and Catalyze Customers are encrypted. Catalyze does not use, own, or manage any mobile devices, SSD cards, or tapes that have access to ePHI.

### Applicable Standards from the HITRUST Common Security Framework

- 0.9o - Management of Removable Media

### Applicable Standards from the HIPAA Security Rule

- 164.310(d)(1) - Device and Media Controls

### Disposable Media Policy

1. All removable media is restricted, audited, and is encrypted.

2. Catalyze assumes all disposable media in its Platform may contain ePHI, so it treats all disposable media with the same protections and disposal policies.

3. All destruction/disposal of ePHI media will be done in accordance with federal and state laws and regulations and pursuant to the Catalyze's written retention policy/schedule. Records that have satisfied the period of retention will be destroyed/disposed of in an appropriate manner.

4. Records involved in any open investigation, audit or litigation should not be destroyed/disposed of. If notification is received that any of the above situations have occurred or there is the potential for such, the record retention schedule shall be suspended for these records until such time as the situation has been resolved. If the records have been requested in the course of a judicial or administrative hearing, a qualified protective order will be obtained to ensure that the records are returned to the organization or properly destroyed/disposed of by the requesting party.
5. Before reuse of any media, for example all ePHI is rendered inaccessible, cleaned, or scrubbed. All media is formatted to restrict future access.
6. All Catalyze Subcontractors provide that, upon termination of the contract, they will return or destroy/dispose of all patient health information. In cases where the return or destruction/disposal is not feasible, the contract limits the use and disclosure of the information to the purposes that prevent its return or destruction/disposal.
7. A record of all ePHI media sanitization is retained by the organization.
8. Any media containing ePHI is disposed using a method that ensures the ePHI could not be recovered or reconstructed.
9. The methods of destruction, disposal, and reuse are reassessed periodically, based on current technology, accepted practices, and availability of timely and cost-effective destruction, disposal, and reuse technologies and services.

## IDS Policy

In order to preserve the integrity of data that Catalyze stores, processes, or transmits for Customers, Catalyze implements strong intrusion detection tools and policies to proactively track and retroactively investigate unauthorized access. Catalyze currently utilizes OSSEC to track file system integrity, monitor log data, and detect rootkit access.

### Applicable Standards from the HITRUST Common Security Framework

- 09.ab - Monitoring System Use
- 06.e - Prevention of Misuse of Information
- 10.h - Control of Operational Software

### Applicable Standards from the HIPAA Security Rule

- 164.312(b) - Audit Controls

### Intrusion Detection Policy

- OSSEC is used to monitor and correlate log data from different systems on an ongoing basis.

Reports generated by OSSEC are reviewed by the Security Officer on a monthly basis.

- OSSEC generates alerts to analyze and investigate suspicious activity or suspected violations.
- OSSEC monitors file system integrity and sends real time alerts when suspicious changes are made to the file system.
- Automatic monitoring is done to identify patterns that might signify the lack of availability of certain services and systems (DOS attacks).

## Employees Policy

Catalyze is committed to ensuring all workforce members actively address security and compliance in their roles at Catalyze. As such, training is imperative to assuring an understanding of current best practices, the different types and sensitivities of data, and the sanctions associated with non-compliance.

### Applicable Standards from the HITRUST Common Security Framework

- 02.e - Information Security Awareness, Education, and Training
- 06.e - Prevention of Misuse of Information Assets
- 07.c - Acceptable Use of Assets
- 08.j - Controls Against Malicious Code
- 01.y - Teleworking

### Applicable Standards from the HIPAA Security Rule

- 164.308(a)(5)(i) - Security Awareness and Training

### Employment Policies

1. All new workforce members, including contractors, are given training on security policies and procedures, including operations security, within 30 days of employment.
   - Records of training are kept for all workforce members.
   - Ongoing security training is conducted monthly.

2. All workforce members are granted access to formal organizational policies, which include the sanction sanction policy for security violations.

3. The Catalyze Employee Handbook clearly states the responsibilities and acceptable behavior regarding information system usage, including rules for email, Internet, mobile devices and social media usage.

4. All workforce members are educated about the approved set of tools to be installed on workstations.

5. All new workforce members are given HIPAA training within 60 days of beginning employment.

Training includes HIPAA reporting requirements, including the ability to anonomously report security incidents, and the levels of compliance and obligations for Catalyze and its Customers and Partners.

6. All remote (teleworking) workforce members are trained on the risks, the controls implemented, their responsibilities, and sanctions associated with violation of policies. Additionally, remote security is maintained through the use of VPN tunnels for all access to production systems with access to ePHI data.

## Approved Tools Policy

Catalyze utilizes a suite of approved software tools for internal use by workforce members. These software tools are either self hosted, with security managed by Catalyze, or they are hosted by a Subcontractor with appropriate business associate agreements in place to preserve data integrity. Use of other tools require approval from Catalyze leadership.

### List of Approved Tools

- **Gitlab**. Gitlab is an open source tool built on top of Git, the version control platform. Gitlab is hosted and secured by Catalyze. It is utilized for storage of configuration scripts and other infrastructure automation tools, as well as for source and version control of application code used by Catalyze.
- **Box**. Box is used for storage of files and sharing of files with Partners and Customers.
- **Google Apps**. Google Apps is used for email and document collaboration.

## 3rd Party Policy

Catalyze makes every effort to assure all 3rd party organizations are compliant and do not compromise the integrity, security, and privacy of Catalyze or Catalyze Customer data. 3rd Parties include Customers, Partners, Subcontractors, and Contracted Developers.

### Applicable Standards from the HITRUST Common Security Framework

- 05.i - Identification of Risks Related to External Parties
- 05.k - Addressing Security in Third Party Agreements
- 09.e - Service Delivery
- 09.f - Monitoring and Review of Third Party Services
- 09.g - Managing Changes to Third Party Services
- 10.1 - Outsourced Software Development

### Applicable Standards from the HIPAA Security Rule

- 164.314(a)(1)(i) - Business Associate Contracts or Other Arrangements

### Policies to Assure 3rd Parties Support Catalyze Compliance

1. The following steps are required before 3rd parties are granted access to any Catalyze systems:
   - Due diligence with the 3rd party;
   - Controls implemented to maintain compliance;
   - Written agreements, with appropriate security requirements, is executed.
2. All connections and data in transit between Catalyze Platform and 3rd parties are encrypted.
3. Access granted to external parties is limited to the minimum necessary and granted only for the duration required.
4. A standard business assocaite agreement with Customers and Partners is defined and includes the required security controls in accordance with the organizations security policies. Additionally, responsibility is assigned in these agreements.
5. Catalyze has Service Level Agreements (SLAs) with Subcontractors with an agreed service arrangement address liability, service definitions, security controls, and aspects of services management.
   - Catalyze utilizes monitoring tools to regularly evaluate Subcontractors against relevant SLAs.
6. Third parties are unable to make changes to any Catalyze infrastructure without explicit permission from Catalyze. Additionally, no Catalyze Customers or Partners have access outside of their own environment, meaning they cannot access, modify, or delete anything related to other 3rd parties.
7. Whenever outsourced development is utilized by Catalyze, all changes to production systems will be approved and implemented by Catalyze workforce members only. All outsourced development requires a formal contract with Catalyze.
8. Catalyze maintains and annually reviews a list all current Partners and Subcontractors.
9. Catalyze assesses security requirements and compliance considerations with all Partners and Subcontracts.
10. Regular review is conducted as required by SLAs to assure security and compliance. These reviews include reports, audit trails, security events, operational issues, failures and disruptions, and identified issues are investigated and resolved in a reasonable and timely manner.
11. Any changes to Partner and Subcontractor services and systems are reviewed before implementation.

## Key Definitions

- *Application*: An application hosted by Catalyze, either maintained and created by Catalyze, or maintaiend and created by a Customer or Partner.

- *Application Level*: Controls and security associated with an Application. In the case of PaaS Customers, Catalzye does not have access to and cannot assure compliance with security standards and policies at the Application Level.
- *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. Offered with all Catalyze Add-ons and as an option for PaaS Customers.
- *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*: 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.

- *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. Offered with all Catalyze Add-ons and as an option for PaaS Customers.

- *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 Catalyze 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 Catalyze, 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 providering IDS notification to customers in the case of suspicious activity. Offered with all Catalyze Add-ons and as an option for PaaS Customers.

- *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. Offered with all Catalyze Add-ons and as an option for PaaS Customers.

- *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 Catalyze.

- *Partner*: Contractual bound 3rd party vendor with integration with the Catalyze Platform. May offer Add-on services.

- *Platform*: The overall technical environment of Catalyze.

- *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 (See Appendix).

- *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.

- *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 Catalyze'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.
      - 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.
      - 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.

  2. The media on which the PHI is stored or recorded has been destroyed in the following ways:
      - 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.
      - 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 Catalyze.

- *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.

## Catalyze HIPAA Business Associate Agreement (“BAA”)

This HIPAA Business Associate Agreement (this “BAA”) defines the rights and responsibilities of Provider and Customer with respect to Protected Health Information (“PHI”) as defined in the Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated thereunder, including the HITECH Act and Omnibus Rule, as each may be amended from time to time (collectively, “HIPAA”). This BAA shall be applicable only in the event and to the extent Provider meets, with respect to Customer, the definition of a Business Associate set forth at 45 C.F.R. §160.103, or applicable successor provisions. This BAA shall only be applicable to Customer’s Hosting Services or Services to the extent that Customer uses the Hosting Services for Customer’s Applications and as specified in the Platform as a Service Agreement of which this Exhibit C is attached and fully referenced and incorporated herein (the “PaaS Agreement”). This BAA is intended to ensure that Business Associate and Customer will establish and implement appropriate safeguards where Business Associate may receive, create, maintain, use or disclose in connection with the functions, activities and services that Business Associate performs on behalf of Customer solely to perform its duties and responsibilities under the PaaS Agreement.

1. Applicability and Definitions. This BAA applies only where:
    1. Customer uses the Hosting Services to store or transmit any PHI as defined in 45 C.F.R. §160.103
    2. Customer has applied the required security configurations, as specified in Section 5.2 of this BAA to Customer’s Applications. Customer acknowledges that this BAA does not apply to any other accounts it may have now or in the future. Unless otherwise expressly defined in this BAA, all capitalized terms in this BAA will have the meanings set forth in the PaaS Agreement or in HIPAA.

2. Additional Meanings.

    - “Business Associate” shall mean Provider, or Catalyze, Inc.
    - “HITECH ACT” shall mean the Health Information Technology for Economic and Clinical Health Act.
    - “Individual” shall have the same meaning as the term “individual” in 45 CFR § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).
    - “Privacy Rule” shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E.
    - “Protected Health Information” or “PHI” shall have the same meaning as the term “protected health information” in 45 CFR § 160.103, limited to the information received by Business Associate from or on behalf of Customer.
    - “Required By Law” shall have the same meaning as the term “required by law” in 45 CFR § 164.103.
    - “Security Rule” shall mean the Security Standards for the Protection of Electronic Protected Health Information, located at 45 CFR Part 160 and Subparts A and C of Part 164.

3. Permitted and Required Uses and Disclosures.

    1. Service Offerings. Business Associate may use or disclose PHI for or on behalf of Customer as defined in the PaaS Agreement.
    2. Administration and Management of Services. Business Associate may Use and Disclose PHI as necessary for the sole purpose of the proper management and administration of Hosting Services. Any disclosures under this section will be made only if Business Associate obtains reasonable assurances from the recipient of the PHI that (i) the recipient will hold the PHI confidentially and will use or disclose the PHI only as required by law or for the purpose for which it was disclosed to the recipient, and (ii) the recipient will notify Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

4. Obligations of Business Associate.

    1. Limit on Uses and Disclosures. Business Associate will use or disclose PHI only as permitted by this BAA or as required by law, provided that any such use or disclosure would not violate HIPAA if done by a Covered Entity, unless permitted for a Business Associate under HIPAA.
    2. Safeguards. Business Associate will use reasonable and appropriate safeguards to prevent Use or Disclosure of PHI other than as provided for by this BAA, consistent with the requirements of Subpart C of 45 C.F.R. Part 164 (with respect to Electronic PHI) as determined by Business Associate and as reflected in the PaaS Agreement, which includes Disk Encryption and Encryption In-Transit services.
    3. Reporting. For all reporting obligations under this BAA, the parties acknowledge that, because Business Associate does not know the details of PHI contained in any of Customer Applications, there will be no obligation on the Business Associate to provide information about the identities of the Individuals who may have been affected, or a description of the type of information that may have been subject to a Security Incident, Impermissible Use or Disclosure, or Breach. Business Associate will ensure Customer access to Audit Logging to help Customer in addressing Customer’s obligations for reporting under this BAA. Customer acknowledges Business Associate is under no obligation to provide additional support for Customer’s BAA reporting obligations but may choose to provide such additional services at its sole discretion or at Customer expense.
        1. Reporting of Impermissible Uses and Disclosures. Business Associate will report to Customer any Use or Disclosure of PHI not permitted or required by this BAA of which Business Associate becomes aware.
        2. Reporting of Security Incidents. Business Associate will report to Customer on no less than fourteen business (14) days from the date any Security Incidents involving PHI of which Business Associate becomes aware in which there is a successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an Information System in a manner that risks the confidentiality, integrity, or availability of such information. Notice is hereby deemed

provided, and no further notice will be provided, for unsuccessful attempts at such unauthorized access, use, disclosure, modification, or destruction, such as pings and other broadcast attacks on a firewall, denial of service attacks, port scans, unsuccessful login attempts, or interception of encrypted information where the key is not compromised, or any combination of the above.

        3. Reporting of Breaches. Business Associate will report to Customer any Breach of Customer's Unsecured PHI that Business Associate may discover to the extent required by 45 C.F.R. § 164.410. Business Associate will make such report without unreasonable delay, and in no case later than fourteen (14) business days after discovery of such Breach. Business Associate undertakes no obligation to report network security related incidents which occur on its managed network but does not directly involve Customer's use of Hosting Services.

    4. Subcontractors. Business Associate will ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of Business Associate agree to restrictions and conditions at least as stringent as those found in this BAA, and agree to implement reasonable and appropriate safeguards to protect PHI.
    5. Access to PHI. Customer acknowledges that Business Associate is not required by this BAA to make disclosures of PHI to Individuals or any person other than Customer, and that Business Associate does not, therefore, expect to maintain documentation of such disclosure as described in 45 CFR § 164.528. In the event that Business Associate does make such disclosure, it shall document the disclosure as would be required for Customer to respond to a request by an Individual for an accounting of disclosures in accordance with 45 CFR §164.504(e)(2)(ii)(G) and §164.528, and shall provide such documentation to Customer promptly on Customer's request. In the event that a request for an accounting is made directly to Business Associate shall, within 5 Business Days, forward such request to Customer.
    6. Accounting of Disclosures. Business Associate will make available to Customer the information required to provide an accounting of Disclosures in accordance with 45 C.F.R. § 164.528 of which Business Associate is aware, if requested by Customer. Because Business Associate cannot readily identify which Individuals are identified or what types of PHI are included in Customer Content, Customer will be solely responsible for identifying which Individuals, if any, may have been included in Customer Content that Provider has disclosed and for providing a brief description of the PHI disclosed.
    7. Internal Records. Provider will make its internal practices, books, and records relating to the Use and Disclosure of PHI available to the Secretary of the U.S. Department of Health and Human Services ("HHS") for purposes of determining Customer compliance with HIPAA. Nothing in this section will waive any applicable privilege or protection, including with respect to trade secrets and confidential commercial information.

5. Customer's Obligations:

    1. Appropriate Use of HIPAA Accounts. Customer is responsible for implementing appropriate

privacy and security safeguards in order to protect PHI in compliance with HIPAA and this BAA. Without limitation, Customer shall: (i) not include protected health information (as defined in 45 CFR 160.103) in any Services that are not or cannot be HIPAA compliant, (ii) utilize the highest level of audit logging in connection with its use of all Customer Applications, and (iii) maintain the maximum retention of logs in connection with its use of all Services.

2. HIPAA Account Appropriate Configurations: Customer is solely responsible for configuring, and will configure, all Customer Applications as follows:
    1. Encryption. Customer shall encrypt all PHI stored or transmitted outside the Services in accordance with the Secretary of HHS's Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals, available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html, as it may be updated from time to time, and as may be made available on any successor or related site designated by HHS.
    2. SSL Termination: All services must be served via SSL. Customer is responsible for providing, maintaining and updating a valid SSL certificate for use with the Service. SSL certificates must be a minimum of 4096 bit key size. Customer agrees to comply with Business Associate's requirements regarding SSL termination.
    3. Necessary Consents. Customer warrants that it has obtained any necessary authorizations, consents, and other permissions that may be required under applicable law prior to placing Customer Content, including without limitation PHI, on the Services.
    4. Restrictions on Disclosures. Customer shall not agree to any restriction requests or place any restrictions in any notice of privacy practices that would cause Business Associate to violate this BAA or any applicable law.
    5. Compliance with HIPAA. Customer shall not request or cause Business Associate to make a Use or Disclosure of PHI in a manner that does not comply with HIPAA or this BAA.

6. Term and Termination

    1. Term. The term of this BAA will commence on the PaaS Agreement Effective Date and will remain in effect until the earlier of the termination of the PaaS Agreement or notification by Customer that an account is no longer subject to this BAA.
    2. Effect of Termination. At termination of this BAA, Business Associate, if feasible, will return or destroy all PHI that Business Associate still maintains, if any. If return or destruction is not feasible, Business Associate will extend the protections of this Agreement to the PHI, limit further uses and disclosures to those purposes that make the return of the PHI infeasible, and make not further use or disclosure of PHI.
    3. If Customer requests contemporaneously with any termination event or notice, Business Associate will allow Customer to have access to Customer's account for a reasonable

period of time following termination as necessary for Customer to retrieve or delete any PHI at its then current monthly recurring rate; provided, however, that if the security of Customer's servers has been compromised, or the Agreement was terminated by Customer's failure to use reasonable security precautions, Business Associate may: (i) provide Customer with restricted access via a dedicated or private link or tunnel to Customer account or (ii) refuse to allow Customer to have access to Customer's account but will use reasonable efforts to copy Customer data on to media Customer provides to Business Associate, and will ship the media to Customer at Customer expense. Business Associate's efforts to copy Customer data onto Customer media shall be billable as an Additional Service at Business Associate's then current hourly rates.

7. No Agency Relationship. As set forth in the Agreement, nothing in this BAA is intended to make either party an agent of the other. Nothing in this BAA is intended to confer upon Customer the right or authority to control Business Associate's conduct in the course of Business Associate complying with the Agreement and BAA.

8. Nondisclosure. Customer agrees that the terms of this BAA are not publicly known and constitute Business Associate Confidential Information under the Agreement.

9. Entire Agreement; Conflict. Except as amended by this BAA, the Agreement will remain in full force and effect. This BAA, together with the Agreement as amended by this BAA: (a) is intended by the parties as a final, complete and exclusive expression of the terms of their agreement; and (b) supersedes all prior agreements and understandings (whether oral or written) between the parties with respect to the subject matter hereof. If there is a conflict between the Agreement, this BAA or any other amendment or BAA to the Agreement or this BAA, the document later in time will prevail.

10. Miscellaneous.

    1. Amendment. Customer and Business Associate agrees to take such action as is reasonably necessary to amend this HIPAA BAA from time to time as is necessary for either party to comply with the requirements of the Privacy Rule and related laws and regulations.
    2. Survival. Customer and Business Associate's respective rights and obligations under this HIPAA BAA shall survive the termination of the Agreement.
    3. Interpretation. Any ambiguity in the PaaS Agreement shall be resolved to permit Customer to comply with HIPAA and the Privacy Rule.

SIGNATURE FOLLOWS

## HIPAA Mappings to Catalyze Controls

Below is a list of HIPAA Safegaurds and Requirements and the Catalyze controls in place to meet those.

| **Administrative Controls** | |
|---|---|
| **HIPAA Rule** | **Catalyze Control** |
| Security Management Process - 164.308(a)(1)(i) | Risk Management Policy |
| Assigned Security Responsibility - 164.308(a)(2) | Roles Policy |
| Workforce Security - 164.308(a)(3)(i) | Employee Policies |
| Information Access Management - 164.308(a)(4)(i) | System Access Policy |
| Security Awareness and Training - 164.308(a)(5)(i) | Employee Policy |
| Security Incident Procedures - 164.308(a)(6)(i) | IDS Policy |
| Contingency Plan - 164.308(a)(7)(i) | Disaster Recovery Policy |
| Evaluation - 164.308(a)(8) | Auditing Policy |

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

| **Technical Safeguards** | |
|---|---|
| **HIPAA Rule** | **Catalyze Control** |
| Access Control - 164.312(a)(1) | System Access Policy |
| Audit Controls - 164.312(b) | Auditing Policy |
| Integrity - 164.312(‘c’)(1) | System Access, Auditing, and IDS Policies |
| Person or Entity Authentication - 164.312(d) | System Access Policy |
| Transmission Security - 164.312(e)(1) | System Access and Data Management Policy |

| **Organizational Requirements** | |
|---|---|

| HIPAA Rule | Catalyze Control |
|---|---|
| Business Associate Contracts or Other Arrangements - 164.314(a)(1)(i) | Business Associate Agreements and 3rd Parties Policies |

**Policies and Procedures and Documentation Requirements**

| HIPAA Rule | Catalyze Control |
|---|---|
| Policies and Procedures - 164.316(a) | Policy Management Policy |
| Documentation - 164.316(b)(1)(i) | Policy Management Policy |

**HITECH Act - Security Provisions**

| HIPAA Rule | Catalyze Control |
|---|---|
| Notification in the Case of Breach - 13402(a) and (b) | Breach Policy |
| Timelines of Notification - 13402(d)(1) | Breach Policy |
| Content of Notification - 13402(f)(1) | Breach Policy |