7. Auditing Policy

Ceresti 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. Ceresti 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 Ceresti to safeguard the confidentiality, integrity, and availability of applications, systems, and networks. To ensure that appropriate safeguards are in place and effective, Ceresti 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- Out of date software and/or software known to have vulnerabilities.

7.1 Applicable Standards

7.1.1 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

7.1.2 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

7.2 Auditing Policies

1. Responsibility for auditing information system access and activity is assigned to Ceresti's Security Officer. The Security Officer shall:
    - Assign the task of generating reports for audit activities to the employee responsible for the application, system, or network;
    - Assign the task of reviewing the audit reports to the employee responsible for the application, system, or network, the Privacy Officer, or any other individual determined to be appropriate for the task;
    - As needed, 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. Ceresti's auditing processes shall address access and activity at the following levels listed below.
    - Application: Application level audit trails generally monitor and log all user activities, including data accessed and modified and specific actions.
    - System: System level audit trails generally monitor and log user activities, applications accessed, and other system defined specific actions.
    - Network: Network level audit trails generally monitor information on what is operating, penetrations, and vulnerabilities.
3. Ceresti shall log 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 Ceresti.
4. Ceresti utilizes Aptible's services to scan all systems for malicious and unauthorized software.
5. Ceresti leverages Aptible's process monitoring tools throughout its Production environment.
6. Ceresti uses Aptible's HIDS and Incident Response system to manage Intrusion Detection. Aptible's HIDS system is based on the open source OSSEC software. See Aptible HIDS for more details or go to the Aptible web site (https://www.aptible.com).
7. Logs are reviewed weekly by the Security Officer.
8. The process for review of audit logs, trails, and reports shall include:
    - Description of the activity as well as rationale for performing the audit.
    - Identification of which Ceresti employees will be responsible for review

(employees shall not review audit logs that pertain to their own system activity).
    - Frequency of the auditing process.
    - Determination of significant events requiring further review and follow-up.
    - Identification of appropriate reporting channels for audit results and required follow-up.
9. Vulnerability testing software is used on a monthly schedule to test the Production software.
10. Software patches and updates will be applied to all systems in a timely manner.

7.3 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, or Customer.
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 Ceresti's Privacy or Security Officer.
3. A request for an audit must be approved by Ceresti'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 employee has accessed ePHI inappropriately, the minimum necessary/least privileged information shall be shared with Ceresti's Security Officer to determine appropriate sanction/corrective disciplinary action.
    - Only de-identified information shall be shared with Customer regarding the results of the investigative audit process. This information will be communicated to the appropriate personnel by Ceresti's Privacy Officer or designee. Prior to communicating with customers and partners regarding an audit, it is recommended that Ceresti consider seeking risk management and/or legal counsel.

7.4 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 employee(s). On a quarterly basis, logs are reviewed to assure the proper data is being captured and retained. The following process details how log reviews are done at Ceresti:
    1. The Security Officer initiates the log review by creating an Issue in the Ceresti Quality Management System.
    2. The Security Officer, or a Ceresti Security Engineer assigned by the Security

Officer, is assigned to review the logs.
    3. Relevant audit log findings are added to the Issue; these findings are investigated in a later step. Once those steps are completed, the Issue is then reviewed again.
    4. Once the review is completed, the Security Officer approves or rejects the Issue. Relevant findings are reviewed at this stage. If the Issue is rejected, it goes back for further review and documentation. The communications protocol around specific findings are outlined below.
    5. If the Issue is approved, the Security Officer then marks the Issue as Done, adding any pertinent notes required.
2. The reporting process shall allow for meaningful communication of the audit findings to those employees or Customers requesting the audit.
    - Significant findings shall be reported immediately in a written format. Ceresti'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 Ceresti'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 employees or Customers.
6. Log review activity is monitored on a quarterly basis using the Quality Management System reporting to assess compliance with above policy.

7.5 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 protected in transit and encrypted at rest to control access to the content of the logs.

3. Audit logs shall be stored in a separate database that supports strict access controls.
    - A separate database is used to apply the security principle of "separation of duties" to protect audit trails from hackers.

7.6 Workforce Training, Education, Awareness and Responsibilities

1. Ceresti employees are provided training, education, and awareness on safeguarding the privacy and security of business and ePHI. Ceresti'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. Ceresti employees 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 employee's failure to comply with organizational policies.

7.7 External Audits of Information Access and Activity

1. Prior to contracting with an external audit firm, Ceresti 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.

7.8 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:
    - Organizational history and experience.
    - Available storage space.
2. Reports summarizing audit activities shall be retained for a period of six years.
3. Audit log data is retained locally in the audit log database for a six-month period.

7.9 Potential Trigger Events

- High risk or problem prone incidents or events.
- Business associate, or customer complaints.
- Known security vulnerabilities.

- Atypical patterns of activity.
- Failed authentication attempts.
- Remote access use and activity.
- Activity post termination.
- Random audits.