4. Roles Policy

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

4.1 Applicable Standards

4.1.1 Applicable Standards from the HITRUST Common Security Framework

- 02.f - Disciplinary Process
- 06.d - Data Protection and Privacy of Covered Information
- 06.f - Prevention of Misuse of Information Assets
- 06.g - Compliance with Security Policies and Standards

4.1.2 Applicable Standards from the HIPAA Security Rule

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

4.2 Privacy Officer

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

1. Provides annual training to all employees 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 Security Officer as needed.

The current Ceresti Privacy Officer is Kevin Liang (kevin.liang@ceresti.com).

4.2.1 Workforce Training Responsibilities

1. The Privacy Officer facilitates the training of all employees as follows:
    1. New employees within their first month of employment;

    2. Existing employees annually;
    3. Existing employees whose functions are affected by a material change in the policies and procedures, within a month after the material change becomes effective;
    4. Existing employees as needed due to changes in security and risk posture of Ceresti.
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 Ceresti'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. Ceresti 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 Ceresti'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 Ceresti'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 Ceresti Customer;
    13. Users are required to understand their role in Ceresti'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 15 minutes of inactivity;
    17. Supervisors are required to report terminations of employees 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;

4.3 Security Officer

The Security Officer is responsible for facilitating the training and supervision of all employees [164.308(a)(3)(ii)(A) and 164.308(a)(5)(ii)(A)], investigation and sanctioning of any employee that is in violation of Ceresti 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 Ceresti Security Officer is Mark Wrenn (mark.wrenn@ceresti.com).

4.3.1 Organizational Responsibilities

The Security Officer, in collaboration with the Privacy Officer, is responsible for facilitating the development, testing, implementation, training, and oversight of all activities pertaining to Ceresti'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. The Security Officer is appointed by and reports to the Board of Directors and the CEO.

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 establish 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. Reviews and 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 employees 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 Ceresti infrastructure.
8. Develops and provides periodic security updates and reminder communications for all employees.
9. Implements procedures for the authorization and/or supervision of employees who work with ePHI or in locations where it may be accessed.
10. Maintains a program promoting employees to report non-compliance with policies and procedures.
    - Promptly, properly, and consistently investigates and addresses reported violations and takes steps to prevent recurrence.
    - Applies consistent and appropriate sanctions against employees who fail to comply with the security policies and procedures of Ceresti.
    - Mitigates, to the extent practicable, any harmful effect known to Ceresti of a use or disclosure of ePHI in violation of Ceresti's policies and procedures, even if effect is the result of actions of Ceresti 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 Ceresti Breach Policy.
12. The Security Officer facilitates the communication of security updates and reminders to all employees to which it pertains. Examples of security updates and reminders include, but are not limited to:
    - Latest malicious software or virus alerts;
    - Ceresti's requirement to report unauthorized attempts to access ePHI;
    - Changes in creating or changing passwords;
    - Additional security-focused training is provided to all employees by the Security Officer. This training includes, but is not limited to:
    - Data backup plans;
    - System auditing procedures;
    - Redundancy procedures;
    - Contingency plans;
    - Virus protection;
    - Patch management;
    - Media Disposal and/or Re-use;
    - Documentation requirements.
13. The Security Officer works with the COO to ensure that any security objectives have appropriate consideration during the budgeting process.
    - In general, security and compliance are core to Ceresti's technology and

service offerings; in most cases this means security-related objectives cannot be split out to separate budget line items.
    - For cases that *can* be split out into discrete items, such as licenses for commercial tooling, the Security Officer follows Ceresti's standard corporate budgeting process.
        - At the beginning of every fiscal year, the COO contacts the Security Officer to plan for the upcoming year's expenses.
        - The Security Officer works with the COO to forecast spending needs based on the previous year's level, along with changes for the upcoming year such as additional staff hires.
        - During the year, if an unforeseen security-related expense arises that was not in the budget forecast, the Security Officer works with the COO to reallocate any resources as necessary to cover this expense.

4.3.2 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 employees (i.e. team leaders, supervisors, managers, directors, co-workers, etc.) to supervise all employees and any other user of Ceresti'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 employees and provide access to users who comply with the Security regulation and Ceresti's security policies and procedures.

4.3.3 Sanctions of Workforce Responsibilities

All employees report non-compliance of Ceresti'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 Ceresti's security policies and procedures. The Security Officer may request the assistance from others.
    - Complete an audit trail/log to identify and verify the violation and sequence of

events.
    - Interview any individual that may be aware of or involved in the incident.
    - All individuals are required to cooperate with the investigation process and provide factual information to those conducting the investigation.
    - Provide individuals suspected of non-compliance of the Security rule and/or Ceresti's policies and procedures the opportunity to explain their actions.
    - The investigator thoroughly documents the investigation as the investigation occurs. This documentation must include a list of all employees involved in the violation.
2. Violation of any security policy or procedure by employees 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.
    - 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 employee from Ceresti.
3. The Security Officer facilitates taking appropriate steps to prevent recurrence of the violation (when possible and feasible).
4. In the case of an insider threat, the Security Officer and Privacy Officer are to set up a team to investigate and mitigate the risk of insider malicious activity. Ceresti employees are encouraged to come forward with information about insider threats, and can do so anonymously.
5. 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.