6. System Access Policy

Access to Ceresti systems and applications is controlled for all users. This includes customers, employees, consultants, business associates, and volunteers. Access by any other entity is allowable only on a minimum necessary basis. All employees, consultants, business associates, and volunteers 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:

6.1 Applicable Standards

6.1.1 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

6.1.2 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

6.2 Access Establishment and Modification

1. Requests for access to Ceresti systems and applications is made formally using the following process:
    1. A Ceresti employee initiates the access request by creating an Issue in the Ceresti Quality Management System.
        - User identities must be verified prior to granting access to new accounts.
        - Identity verification must be done in person where possible; for remote employees, identities must be verified over the phone.
        - For new accounts, the method used to verify the user's identity must be recorded on the Issue.
    2. The Security Officer or Privacy Officer will grant access to systems as dictated by the employee's job title. If additional access is required outside of the minimum necessary to perform job functions, the requester must include a description of why the additional access is required as part of the access request.
    3. Once the review is completed, the Security Officer or Privacy Officer approves or rejects the Issue. If the Issue is rejected, it goes back for further review and documentation.
    4. If the review is approved, the Security Officer or Privacy Officer then marks the Issue as Done, adding any pertinent notes required. The Security Officer or Privacy Officer then grants requested access.
        - New accounts will be created with a temporary secure password that meets all requirements from §6.12, which must be changed on the initial login.
        - All password exchanges must occur over an authenticated channel.
        - Account management may be delegated to a Ceresti employee at the discretion of the Security Officer or Privacy Officer .
2. Access is not granted until receipt, review, and approval by the Ceresti Security Officer or Privacy Officer ;
3. The request for access is retained for future reference.
4. All access to Ceresti systems and services is reviewed and updated on a bi-annual basis to ensure proper authorizations are in place commensurate with job functions. The process for conducting reviews is outlined below:
    1. The Security Officer initiates the review of user access by creating an Issue in the Ceresti Quality Management System.
    2. The Security Officer is assigned to review levels of access for each Ceresti employee.
    3. If user access is found during review that is not in line with the least privilege

    principle, the process below is used to modify user access and notify the user of access changes. 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. If the Issue is rejected, it goes back for further review and documentation.
    5. If the review is approved, the Security Officer then marks the Issue as Done, adding any pertinent notes required.
    6. Review of user access is monitored on a quarterly basis using the Quality Management System reporting to assess compliance with above policy.
5. Any Ceresti employee can request change of access using the process outlined in §6.2 paragraph 1.
6. Access to Ceresti systems is controlled using the associated system user management and authentication.
7. Temporary accounts are not used unless absolutely necessary for business purposes.
    - Accounts are reviewed every 90 days to ensure temporary accounts are not left unnecessarily.
    - Accounts that are inactive for over 90 days are disabled.
8. Privileged users must first access systems using standard, unique user accounts before switching to privileged users and performing privileged tasks.
    - For production systems, this is enforced by creating non-privileged user accounts that must invoke `sudo` to perform privileged tasks.
    - Rights for privileged accounts are granted by the Security Officer or Privacy Officer using the process outlined in §6.2 paragraph 1.
9. All application to application communication using service accounts is restricted and not permitted unless absolutely needed. Automated tools are used to limit account access across applications and systems.
10. Generic accounts are not allowed on Ceresti systems.
11. Remote access to the Ceresti office IT systems is prohibited.
12. In cases of increased risk or known attempted unauthorized access, immediate steps are taken by the Security and Privacy Officer to limit access and reduce risk of unauthorized access.
13. Direct system to system, system to application, and application to application authentication and authorization are limited and controlled to restrict access.

6.3 Workforce Clearance

1. 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.
2. All access requests are treated on a "least-access principle."
3. Ceresti maintains a minimum necessary approach to access to ePHI data.

6.4 Access Authorization

1. Role based access categories for each Ceresti system and application are pre-approved by the Security Officer, or an authorized delegate of the Security Officer.
2. Ceresti utilizes hardware and software firewalls to segment data, prevent unauthorized access, and monitor traffic for denial of service attacks.
3. Ceresti leverages and benefits from access protection provided by both Aptible and AWS as part of their core services.

6.5 Person or Entity Authentication

1. Each employee has and uses a unique user ID and password that identifies him/her as the user of the information system.
2. All Customer support desk interactions must be verified before Ceresti support personnel will satisfy any request having information security implications.

6.6 Unique User Identification

1. Access to the Ceresti systems and applications is controlled by requiring unique User Login IDs and passwords for each individual user and developer.
2. Passwords requirements mandate strong password controls (see below).
3. Passwords are not displayed at any time and are not transmitted or stored in plain text.
4. Default accounts on all production systems, including root, are disabled.
5. Shared accounts are not allowed within Ceresti systems or networks.

6.7 Automatic Logoff

1. 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).
2. Information systems automatically log users off the systems after 15 minutes of inactivity.
3. The Security Officer pre-approves exceptions to automatic log off requirements.

6.8 Employee Workstation Use

All workstations at Ceresti are company owned, and all are Apple products running Mac OSX or Linux or are PCs running Microsoft Windows.

1. Workstations may not be used to engage in any activity that is illegal or is in violation of organization's policies.
2. 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.
3. 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.
4. Solicitation of non-company business, or any use of organization's information systems/applications for personal gain is prohibited.
5. Transmitted messages may not contain material that criticizes the organization, its providers, its employees, or others.
6. Users may not misrepresent, obscure, suppress, or replace another user's identity in transmitted or stored messages.
7. Workstations that are used to access ePHI will have their hard drives encrypted using FileVault 2.0 or equivalent.
8. All workstations have firewalls enabled to prevent unauthorized access unless explicitly granted.
9. All workstations are to have the following messages added to the lock screen and login screen: *This computer is owned by Ceresti Health, Inc. By logging in, unlocking, and/or using this computer you acknowledge you have seen, and follow, these policies (https://policy.ceresti.com) and have completed this training (https://training.ceresti.com/). Please contact us if you have problems with this - privacy@ceresti.com.*

6.9 Wireless Access Use

1. Wireless networks managed within Ceresti facilities (offices, etc.) are secured with the following configurations:
   - All data in transit over wireless is encrypted using WPA2 encryption;

    - Passwords are rotated on a regular basis, presently quarterly. This process is managed by the Ceresti Security Officer.
2. Ceresti production systems are not accessible directly over wireless channels.
3. When accessing production systems via remote wireless connections, the same system access policies and procedures apply to wireless as all other connections, including wired.

6.10 Employee Termination Procedures

1. Ceresti managers, supervisors and users are required to notify the Security Officer upon completion and/or termination of access needs and facilitating completion of the "Termination Checklist".
2. Ceresti managers, supervisors and users are required to notify the Security Officer 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).
3. The Security Officer will terminate users' access rights immediately upon notification, and will coordinate with the appropriate Ceresti managers, supervisors and users to terminate access to any non-production systems managed by those personnel.
4. 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.

6.11 Password Management

1. User IDs and passwords are used to control access to Ceresti systems and may not be disclosed to anyone for any reason.
2. Users may not allow anyone, for any reason, to have access to any information system using another user's unique user ID and password.
3. On all production systems and applications in the Ceresti environment, password configurations are set to require:
    - a minimum length of 8 characters;
    - a mix of upper case characters, lower case characters, and numbers or special characters;

    - a 90-day password expiration, or 60-day password expiration for administrative accounts;
    - prevention of password reuse using a history of the last 6 passwords;
    - where supported, modifying at least 4 characters when changing passwords;
    - account lockout after 5 invalid attempts.
4. All system and application passwords must be stored and transmitted securely.
    - Where possible, passwords should be stored in a hashed format using a salted cryptographic hash function (SHA-256 or equivalent).
    - Passwords that must be stored in non-hashed format must be encrypted at rest pursuant to the requirements in §16.8.
    - Transmitted passwords must be encrypted in flight pursuant to the requirements in §16.9.
5. 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.
6. Passwords are inactivated immediately upon an employee's termination (refer to the Employee Termination Procedures in §6.10).
7. All default system and application passwords are changed before deployment to production.
8. Upon initial login, users must change any passwords that were automatically generated for them.
9. Password change methods must use a confirmation method to correct for user input errors.
10. All passwords used in configuration scripts are secured and encrypted.
11. If a user believes their user ID has been compromised, they are required to immediately report the incident to the Security Office.
12. In cases where a user has forgotten their password, the following procedure is used to reset the password.
    - The user submits a password reset request to password-reset@ceresti.com. The request should include the system to which the user has lost access and needs the password reset.
    - An administrator with password reset privileges is notified and connects directly with the user requesting the password reset.
    - The administrator verifies the identity of the user either in-person or through a separate communication channel such as phone or Slack.
    - Once verified, the administrator resets the password.

The password-reset email inbox is used to track and store password reset requests. The

Security Officer is the owner of this group and modifies membership as needed.