9. Facility Access Policy

All production data is housed in the AWS HIPAA Data Center and is operationally managed by Aptible. Any electronic PHI (ePHI) is stored in a separate network segment inaccessible from the internet and is encrypted in transit and at rest.

Ceresti inherits all the physical and logical controls from AWS and Aptible operations.

Ceresti's office used on a daily basis by it's employees is secured by a card key entrance and by a second office door lock. Any PHI that resides on paper is locked in a secure cabinet and only accessed by authorized users.

All Ceresti computers used for ePHI have fully encrypted hard drives.

All employees are responsible for reporting an incident of unauthorized visitor and/or unauthorized access to Ceresti's facility.

9.1 Applicable Standards

9.1.1 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

9.1.2 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

9.2 Workstation Security

- Workstations may only be accessed and utilized by authorized employees to complete assigned job/contract responsibilities.
- All employees 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 Ceresti are the property of Ceresti and are distributed to users by the company.