1. Introduction

Ceresti Health, Inc ("Ceresti") 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 a tech-enabled service, Ceresti 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 Ceresti to maintain compliance and assure the proper protections are used to store, process, and transmit ePHI for Ceresti customers.

Ceresti has two different kinds of customers. The first are **Payers and Providers** which contract with Ceresti to provide a tech-enabled service for their members.

Ceresti signs business associate agreements (BAAs) with these customers. These BAAs outline Ceresti obligations and customer obligations, as well as liability in the case of a breach.

The second type of customer are **Families**, which include the caregiver, the patient and authorized family members. These customers are users of the Ceresti software and hardware and coaching.

1.1 Scope

Ceresti has three different environments that are governed by these policies:

- Production - the environment used to deliver the Ceresti tech-enabled service. This environment is used by Ceresti coaches, and **Families** including family caregivers and their associated family members while on a Ceresti program.
- Office - the environment at the Ceresti office where Ceresti employees and contractor perform their daily work
- Development - the environment used by Ceresti software developers and QA to develop, build and test the Ceresti software suite.

1.1.1 Production Environment

Ceresti partners with Aptible (https://www.aptible.com) to host all data and server-side software in the secure HIPAA-compliant Amazon Web Services data center. All data stored in the Amazon cloud on behalf of our customers is encrypted at rest and in transit and is stored on a secondary internal network not accessible from the Internet. Security patches to the base Linux operating system are applied regularly and are actively monitored. Application vulnerabilities are tested on a regular monthly basis. Aptible maintains Docker containers and virtual private clouds (VPCs) and does active monitoring of the container environment. Details on the Aptible division of responsibilities can be found here.

Details on the Aptible reference architecture can be found here.

The Ceresti Health Station, typically a Samsung tablet, is deployed into the homes of our caregiver / patient dyads. It is locked down in 'kiosk-mode' such that the family caregiver can only interact with the Ceresti software program. The assessment data, messaging and all interactions with the Ceresti Health Station are all encrypted during transit to the secure Amazon Web Services data center. No ePHI is stored on the tablet.

1.1.2 Office Environment

Ceresti has a minimal office infrastructure. The office environment is used to run Ceresti operations and supports local Apple Mac computers, a few Windows computers and printers. A NAS device is on the network and is used for video and graphic production work and computer encrypted backups.

The Office Environment is connected to the Internet through a standard ISP and is protected by two levels of firewall.

1.1.3 Development Environment

The Ceresti software team uses Digital Ocean as a cloud hosting provider to implement and use development and test systems. These systems are Linux based and contain no ePHI. Their sole purpose is to enable the software development process.

1.2 Requesting Audit and Compliance Reports

Ceresti, at its sole discretion, shares audit reports, including its HITRUST reports and Corrective Action Plans (CAPs), with **Payers and Providers** on a case by case basis. All audit reports are shared under explicit NDA between Ceresti and the party to receive the materials.

The following process is used to request audit reports:

1. Email is sent to compliance-reports@ceresti.com. In the email, please specify the type of report being requested and any required timelines for the report.
2. Ceresti staff will log an issue with the details of the request into the Ceresti Quality Management System. The Ceresti Quality Management System is used to track

requests' status and outcomes.

3. Ceresti will confirm if a current NDA is in place with the party requesting the audit report. If there is no NDA in place, Ceresti will send one for execution.
4. Once it has been confirmed that an NDA is executed, Ceresti staff will move the issue to "Under Review".
5. The Ceresti Security Officer or Privacy Officer must Approve or Reject the Issue. If the Issue is rejected, Ceresti will notify the requesting party that we cannot share the requested report.
6. If the issue has been Approved, Ceresti will send the customer the requested audit report and complete the Quality Management System issue for the request.

1.3 Version Control

Refer to the GitHub repository at https://github.com/ceresti/policies-deployable/ for the full version history of these policies.