PowerCloud Systems HIPAA Compliance Overview

The Health Insurance Portability and Accounting Act was enacted by the US Congress in 1996. The 3 safeguards outlined in the Security Rule of Title II, Subtitle F (Administrative, Physical, and Technical Safeguards) define the policies required to protect the electronic protected health information. The codification of this policy occurs under the Code of Federal Regulations (CFR) Title 45, Part 164, Subpart C.

The following table describes how PowerCloud Systems products meet specific HIPAA requirements:

HIPAA Requirement		How PowerCloud Systems Meets the Requirement
Technical Safeguards		
Unique User Identification		Each wireless access point managed via Enable Network's cloud controller is capable of transmitting 4 SSIDs per radio. Each SSID is capable of providing security, network, and access control. PowerCloud Systems supports 802.1X authentication (WPA2-Enterprise) via a captive portal, requiring username and password. Additionally, the primary network can be secured with our patented Individual Device Authentication (IDA) to control access to the network. User credentials can be validated against a properly configured Authentication server (RADUIS, LDAP, AD, etc.). SSIDs can alternatively be secured via captive portal, VLAN and walled garden. The event log captures all device connections and disconnections to the WLAN and is designed to be exported into the networks compliance reporting schema.
Emergency Access		PowerCloud Systems WLANs come equipped with an automatic failover mechanism which allows continued access to the local LAN under the configured security blanket even when internet availability is disrupted.
Automatic Logoff		PowerCloud Systems products can allow for automated user device logoff when configured using UAM (Universal Authentication Mechanism) and coupled with the appropriate business rules in the Authentication server. The guest/hotspot SSID can be configured for individual time limits as well. Additionally, all SSIDs can be scheduled individually.
Authentication, Integrity, and Encryption		PowerCloud Systems products utilize WPA2-PSK and WPA2-Enterprise (IEEE 802.1x) with AES encryption. All wireless security settings are enabled for strong encryption. All management control is secured with

		SSL utilizing X509 security certificates. . Further, access to individual access points is password protected.
Audit Controls		PowerCloud Systems' event logs are automatically stored securely in the cloud. Event logs may be reviewed, filtered, and exported to any appropriate media.
Administrative Safeguards		
Login Monitoring		PowerCloud Systems' provides a complete log of all administrative activity, including configuration changes and AP connectivity. Event logs are automatically stored securely in the cloud. Event logs may be reviewed, filtered, and exported to any appropriate media.
Password Management		An administrator can create, modify, and delete operator and administrator accounts within the system.
Response and Reporting		Security and administrative alerts can be configured to be sent to Administrators and operators via SMS message, email, or both. In addition, the dashboard provides a hot link to the alerts page when an alert is present. The dashboard also identifies which specific networks have alerts pending.
Data Backup and Recovery		The PowerCloud Systems cloud controller is hosted in multiple, geographically distributed Amazon EC2 data centers designed for high reliability and availability.
Emergency Mode Operation		The Enable network controller is cloud based, meaning there is no onsite hardware based LAN controller to fail. Moreover, each AP is designed to continue to operate and provide local LAN access (assuming they are configured for this function) should the connection to the internet be disrupted. All APs will continue to function with their designed security overlays.
Physical Safeguards		
Media Reuse		No user traffic is ever stored on a PowerCloud Systems AP. Further, no user traffic flows through the connection to the cloud controller. All control traffic is encrypted and secured with X509 certificates.