



BridgeWave

HIPAA

HIPAA COMPLIANCE

(Health Insurance Portability & Accountability Act)

BRIDGEWAVE PRODUCTS MEET HIPAA COMPLIANCE REQUIREMENTS

BridgeWave Communications products are wireless Ethernet point-to-point links, compliant with Ethernet networking standards and FCC Parts 15 and 101 regulations. These products provide Gigabit and Fast Ethernet wireless performance with security superior to a fiber-optic cable connection. Health Insurance Portability and Accountability Act (HIPAA) compliant networks must include security mechanisms to guard against unauthorized access to data that is transmitted over a communications network. Similar to fiber-optic cable connections, BridgeWave wireless link security is based on securing the physical access to the end points of the link, where the wireless signal is converted between wireless and fiber optic or copper media.

While these products transmit data wirelessly over the air, the millimeter-wave energy is focused in tightly formed beams between the end-points and is virtually un-interceptable. The products' millimeter-wave beamwidths range between just 0.5 and 1.4 degrees and provide over-the-air physical security that is typically superior even to fiber-optic cable, due to the extreme difficulty involved in intercepting the signals. BridgeWave wireless links are not subject to signal interception risks that are present using products operating in the lower operating frequencies, which typically require additional security measures (such as encryption) to prevent over-the-air interception.

Despite the extreme difficulty involved in intercepting a BridgeWave radio transmission, attempts to do so will result in link outages, in the same manner as if a fiber optic cable was cut. In this case, network equipment (switches or routers) connected to the radio end-points can detect the link outage and can report alarms and maintain event logs that comply with HIPAA requirements.

The BridgeWave products only provide direct access to the transmitted data through the products' physical Ethernet network ports – fiber and/or copper. The network management interfaces on BridgeWave's product do not provide access to the transmitted data streams and are furthermore protected by user password access controls.

While BridgeWave links are inherently secure at a physical level, BridgeWave also offers the option to add an additional layer of security for application and network management traffic using 256-bit AES encryption. This provides the highest level of commercially-available data security, while maintaining full line-rate network performance. This option should be selected when site security policies require that data leaving the site must be encrypted or that all wireless transmissions must be encrypted.

If you have questions about the use of BridgeWave products in HIPAA-compliant networks, please contact your BridgeWave sales representative.

DIRECT, POINT-TO-POINT SECURE WIRELESS

BridgeWave Wireless: Direct Point-to-Point Connection

Fiber Path: Connected Through Central Office

Central Office

- Narrow wireless beams provide physical data security -- superior to inter-building fiber cabling
- Ability to isolate management traffic flows prevents access to application data through management interfaces
- Role-based password protection secures management interfaces
- SNMP link outage traps enable alarm functions and event logs through network management station
- 256-bit AES encryption option



BridgeWave

BridgeWave Communications, Inc.
3350 Thomas Road, Santa Clara, CA 95054
Ph: 866-577-6908 | Fax: 408 567-0775

www.bridgewave.com

HIPAA COMPLIANCE