

HIPAA Compliance

Trango Products Meet or Exceed HIPAA Requirements

This HIPAA Compliance statement applies to the following Trango Systems products:

TrangoLINK Sparta Elite™



The *Health Insurance Portability and Accountability Act* (HIPAA) require standards of security for the electronic exchange of health care data. Trango Systems' Elite Series microwave communication systems meet or exceed HIPAA compliancy regulations for data security and protecting Electronic Protected Health Information (EPHI).

Trango point-to-point high-speed wireless communication systems operate under common Ethernet networking standards and are compliant with all FCC *Part 15* and *Part 101* regulations. Trango products feature highly secure mechanisms that offer significant levels of over-the-air security to prevent unauthorized access of wirelessly transmitted data. All the Elite series products offer both Layer 2 and Layer 3 IPsec based encryption tunnels with extremely low latency. These features provide data security that is superior to fiber, copper and other types of traditional data communication. Trango Systems wireless equipment utilizes the following security features to ensure HIPAA compliance.

- » Integrated standards based NSA SuiteB* compatible security (up to TOP SECRET level protection) to provide data
 - Confidentiality using FIPS-197 certified AES-GCM 128/256bit real time encryption
 - Integrity using FIPS 180-3 certified Secure Hash Algorithm SHA-256/SHA-384
 - Secure Key Exchange using Elliptic Curve Diffie Hellman (ECDH)
- » Sensitive data can be encrypted over an IPsec tunnel between two points in the network. Encryption of non-IP EtherTypes (MPLS, VPLS, PBB, etc.) and Layer 2 header protection is supported using special IPsec encapsulation.
- » FIPS140-2 compliant with tamper detection and response mechanism for immediate zeroization of critical security parameters
- » Automated key management using Internet Key Exchange (IKE v2) with
 - Seamless key change periodically after configured lifetime expiry
 - Perfect forward secrecy support
- » Secure management with SSH, HTTPS using three-level password protection for radio management interfaces and radio authentication using pre-shared key
- » Auditing support with syslog, trap/alarm generation on configuration changes and system monitoring.
- » Traffic replay protection using nonces, sequence numbers and padding
- » Data compression to increase throughput and disguise the true length and content of the data to prevent against traffic analysis attacks
- » True HW based random number generator to aid in creation of security keys, nonces and cookies
- » High-availability with monitored hot standby, space and frequency diversity support
- » Licensed microwave frequency antennas send highly focused narrow beams of millimeter-wave energy (<2° beamwidth) making the traffic "path" nearly impossible to intercept to even attempt to compromise a link. This provides exceptional over-the-air physical security
- » Segregated and independent data ports can physically isolate data streams and different traffic types at the path endpoints

If you have further questions about the HIPAA-compliant security features of Trango products, please contact your Trango sales representative.

* NSA SuiteB: http://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml