Northland Communications

Overview of Company and Product Security Capabilities

Revision 05.04.22

Summary

Complying with regulations, including HIPAA, CPNI, and PCI, often requires a combination of technology, company policy and company process. Northland can make statements related to technology it provides, but customers are responsible for aligning technology with policy and process in order to remain compliant.

This document provides:

1. A summary of the policies and standards that Northland complies with
2. Details of product capabilities that can assist a customer when determining if a Northland product complies with certification standards such as HIPAA, PCI or others

Northland Policies and Standards

1. Northland maintains PCI compliance through its financial partners regarding its own business operations when handling credit card information
2. Northland is an FCC regulated company and is required to adhere to CPNI (Customer Proprietary Network Information) standards. Northland provides training to employees on CPNI and has controls to limit access to customer information
3. Northland publishes a customer privacy policy, which strictly governs access by employees and others to customer communications and information
4. Northland publishes a security and reliability statement that outlines security controls in place which includes access control and security systems
5. Northland will comply with requests by customers for third party audits in situations where the customer needs to ensure compliance with any standard
6. Strict confirmation of authorized contacts. Northland takes measures to ensure that only authorized contacts can make changes to services
7. Northland employees also sign and comply with the Confidentiality Policy in Employee Handbook that highlights importance of protecting confidential information

Limitation of Liability

1. With exception to the specific claims made in this document, Northland assumes no responsibility for ensuring that a customer complies with any certification standard
2. Northland will have no liability of any nature in the absence of gross negligence or willful misconduct, and that, in any event, regardless of the form of the action, the Customer's exclusive remedy, and the total liability of Northland, arising out of, or in any way connected directly or indirectly with service provided by Northland, for any cause whatsoever, shall be limited to payment by carrier in any amount equivalent to the proportionate charge to the customer for the period of service for which the issue occurs. In no event shall Northland be liable to customer for any special, consequential or incidental damages.
3. Northland describes some products as being HIPAA compliant based upon the security features of the products that are inclusive of HIPAA guidelines. It remains the responsibility of the customer to ensure that the features are implemented properly by the customer and are adequate based on HIPAA guidelines or any specific security requirements a customer may have.

Northland Communications

Overview of Company and Product Security Capabilities

Revision 05.04.22

Product Specific Capabilities and Limitations

1. Cloud Fax

    a. Product Description – Provides a hosted faxing service where customers can send and receive faxes via email

    b. HIPAA compliant status – Cloud Fax meets HIPAA guidelines for compliance provided that the customer follows the guidelines along with utilizing the following security features

    c. Security Features
        i. Can be configured for zero retention as required by HIPAA
        ii. Faxes are isolated between customers
        iii. The Email interface between Cloud Fax and the customer supports TLS 1.2 encryption
        iv. Access to system management is limited to core staff of authorized Northland network engineers and only through encrypted connections.
        v. Northland utilizes complex passwords for access that are rotated regularly and maintained in a secure location

2. Business Unlimited

    a. Product Description – A virtual PBX that is hosted within the Northland Communications' cloud utilizing customer's internet connection to provide both voice connectivity via VoIP and unified communication features to their business.

    b. HIPAA compliance – Business Unlimited meets HIPAA guidelines for compliance, provided that the customer follows the guidelines along with utilizing the following security features.

    Includes the following components:

        i. **CommPortal** – Customer web interface for managing voice and unified communications features.
            1. Secured with SSL and strict password requirements
            2. Customer can choose which accounts have administrative access

ii. MaX UC - A desktop and mobile softphone application that can send and receive phone calls and provide additional unified communications features such as SMS texting, internal chat, peer to peer video and more.
    1. TLS/SRTP Voice Encryption_– Enabled by default
    2. SMS – not encrypted, which is currently not required for HIPAA compliance

iii. MaX Meeting - A virtual web conferencing and collaboration tool that can be integrated into Northland's Business Unlimited solution or provided as a standalone service.
    1. Video and Audio Encryption enabled by default
    2. Ability to optionally protect conference rooms with passwords on any or all meetings.
    3. When using a personal meeting room ID and allowing participants to join before host, password entrance is required.

iv. Desktop Phone Options

    1. Mitel 6867i and Mitel 6864i do not support encryption, which is currently not required for HIPAA compliance.
    2. YealinkW60 and 56H cordless bundle does not support encryption, which is currently not required for HIPAA compliance.
    3. Yealink CP930W, CP920 and CP960 Conference phones do no support encryption, which is currently not required for HIPAA compliance.
    4. Yealink T33G, T54W and T58A support TLS and SRTP Voice Encryption, and both are enabled by default.

v. Advanced Technology Attachments (ATA)

    1. Patton 4112 ATA does not support encryption, which is currently no required for HIPAA compliance.

3. Private MPLS Data

    a. Product Description – Securely extends a customer wide area network from multiple locations through Northland's network. Able to be combined with internet and voice services.

    b. HIPAA compliant status – Private MPLS meets HIPAA guidelines for compliance based on features below.

    c. Security Features
        i. All data is contained within Northland's secured network or through third party connections that are not on the internet
        ii. Customer data is isolated in a private VLAN using MPLS VRF standards
        iii. Network connections are continuously monitored

4. Internet Bandwidth

    a. Product Description - Internet access over a variety of connection options to a customer location from Northland.

    b. HIPAA compliant status – Internet bandwidth is not compliant itself and requires the customer to follow HIPAA guidelines to secure internal resources from the internet (such as having a firewall between the internet and the private network)

    c. Security Features
        i. Northland can optionally provide a NAT firewall that protects a customer's network from the internet
        ii. Internet access is fully open with no firewall limitations. The customer is responsible to ensure that they have a firewall at their location.

5. Physical Colocation

    a. Product Description – Datacenter space provided to customers to place network and computing equipment
    b. HIPAA compliant status – Colocation meets HIPAA guidelines based on the security features below.

    c. Security Features
        i. Escorted Access only
        ii. Third Party monitored security system
        iii. Video Camera recording systems
        iv. FOB access control and logging

6. Virtual Servers

    a. Product Description – Virtual server space provided to customers to run Windows and Linux based operating systems for applications and backup purposes.

    b. HIPAA compliant status – Colocation meets HIPAA guidelines based on the security features below.

    c. Security Features
        i. Physical Security as described in datacenter sections
        ii. Strict network and computing isolation based on VMWare ESXi standards
        iii. Limited access to network engineering staff only

7. Domain Name Service (DNS)

   a. Product Description – A complimentary service that resolves hostnames into IP address for customers with registered domain names

   b. HIPAA compliant status – DNS is an external service for domain name resolution and there are no specific HIPAA guidelines for DNS. Northland provides the following security features for DNS

   c. Security Features
      i. DNS servers running latest version of standard BIND
      ii. DNSSEC
      iii. Strict access control to DNS records by authorized staff only
      iv. No external access to customers to permit management of DNS