# HIPAA Compliance for LAN and WLAN

This document describes the implications of HIPAA (the Health Insurance Portability and Accountability Act of 1996) on Nile's LAN/WLAN solution

2022

# Table of Contents

# Introduction

This document describes the implications of HIPAA (the Health Insurance Portability and Accountability Act of 1996) on a LAN/WLAN solution and highlights how Nile products can help customers maintain a HIPAA-compliant network. The target audience of this document is healthcare IT administrators who are responsible for the design and implementation of a wireless network.

## Overview

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that requires the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. HIPAA applies to any healthcare facility that exchanges patient health information. HIPAA's objective is to ensure that health information remains private and secure.

## The Privacy and the Security Rules

The HIPAA Privacy Rule establishes standards for protecting patients' medical records and other PHI. It specifies what rights patients have over their information and requires covered entities to protect that information. As a subset of the Privacy Rule, the Security Rule applies specifically to electronic PHI, or ePHI. The Security Rule mandates the following safeguards:

- Administrative safeguards define personnel and management processes to train employees who work with private health information, as well as procedures for detecting and handling privacy violations. These include Security Awareness training, Security Incident procedures, Contingency plans and periodic evaluation of the implemented security plans and procedures to ensure continued compliance with HIPAA Security Rule.
- Physical safeguards are policies and procedures that govern the addition and removal of hardware, access to equipment, etc. These include policies and procedures for facility access control, workstation security and device & media controls.
- Technical safeguards are guidelines for data encryption, data corroboration, and audit logging. These include Access Control, Audit Control, Integrity Control & Transmission Control.

## How does Nile support your HIPAA requirements?

The requirements described earlier are explored below to show how Nile's services support the HIPAA requirements and can be used in your network.

### Administrative Safeguards

| Requirement | How does Nile fit in? |
|---|---|
| Log-in Monitoring | Nile provides detailed logging and audit functionality of all the activities done in the Nile Portal. Nile also provides customers with the ability to integrate with their SIEMs product (like Splunk). |
| Password Management | It is mandatory for all Root admins to enable MFA to access the Nile portal. Nile also fully supports SAML based Idp federation and Role provisioning for seamless Single Sign On access. |
| Response and Reporting | Nile Wireless IDS/IPS service scans wireless spectrum and detects for presence of unauthorized, rogue access points, security attack tools, and interferers which can impact Nile service, and send alerts to customers. |
| Data Backup and Recovery | The Nile Cloud is hosted in multiple geographically distributed data centers for high availability and reliability. |
| Emergency Mode Operation | The Nile Service Block will continue to operate even if it loses connectivity to the cloud. In case of internet outage, the NSB will continue to pass traffic locally to the LAN. |

### Physical Safeguards

| Requirement | How does Nile fit in? |
|---|---|
| Facility Security Plan | Nile recommends keeping the NSB equipment in a safe area, protected by cameras and locks. |
| Media Re-use | Nile NSB does not store any customer health information in their equipment / media. |

## Technical Safeguards

| Requirement | How does Nile fit in? |
|---|---|
| Unique User Identification | Nile APs can support multiple SSIDs simultaneously, each with its own segments. Niles supports SAML based authentication. |
| Emergency Access | The Nile wireless LAN stays up, even if connectivity to the Nile Cloud becomes unavailable. Users can continue accessing LAN resources without interruption. |
| Authentication, Integrity, and Encryption | Nile supports<br>• WPA2 Personal<br>• WPA2 Enterprise<br>• WPA3 Personal (strict)<br>• WPA3 Personal (Transition)<br>• WPA3 Enterprise 192-bit (strict)<br>• WPA3 Enterprise (strict)<br>• WPA3 Enterprise (Transition)<br>• Captive Portal (With SSO Federation support)<br><br>Communication between the APs and the Nile Cloud is conducted over a secure SSL connection. |
| Audit Controls | Nile Portal has all the device information, including wireless association/dis-association, login / logout time, RADIUS authentication and DHCP related events are available. |