JDL HealthTech
HIPAA-Compliant IT Services

Is Your Wireless Network Leaking Data?

Sharing ePHI on Wireless Networks

More and more healthcare providers are embracing the convenience, speed and cost-effectiveness of wireless networking in their offices. Some utilize commercial-grade wireless security; others have installed products intended for home use. The level of security is not the same.

When you are routinely sharing ePHI and other sensitive information with staff and patients in your office, you must make sure that your networks—both wired and wireless—are totally secure.

Despite evolving standards for wireless (e.g., IEEE 802.11ac), wireless networks are vulnerable, especially when (1) part of an overall network infrastructure, (2) protected by residential-grade security, or (3) supporting unsecure wireless user devices such as smartphones.

Schedule Your Wireless Diagnosis Today

The #1 provider of HIPAA-compliant IT services in Florida, JDL HealthTech provides IT solutions that are HIPAA-compliant, including our Wireless Security Assessment—because all good decisions begin with good diagnostics. We will sign your Business Associate Agreement prior to conducting the assessment, or provide you with ours.

Don't delay your wireless diagnosis.

www.JDLHealthTech.com | 888.493.7833

Best Practices for Wi-Fi Include Periodic Wireless Security Assessments

Even the smallest wireless network, using one controller and a few access points, is vulnerable to compromise if adequate security is not maintained.

The following activities are central to the JDL **Wireless Security Assessment** and will identify opportunities to improve your wireless security:

- Review wireless security policy and wireless use policy for weaknesses
- Conduct internal wireless network security analysis and document internal security
- Review external boundary and document physical access to existing wireless areas within the building
- Review wireless footprint and identify nearby access points for future reference
- Inventory all wireless access points detected within assessment area, type of encryption used, and whether legitimate or rogue
- Validate and review SSIDs
- Suggest times for wireless devices to be off during after-hours and weekends
- Suggest strengthened security configurations for known wireless routers, as applicable
- Review and recommend encryption key sizes, and attempt to crack wireless keys and document weak keys
- Conduct external non-intrusive security assessment of wireless networks (intrusive security assessment on request)

Upon completion, we'll present a thorough report detailing current vulnerabilities in priority order and the actions required to resolve them. (We can also help with remediation.)