silex technology

WHITE PAPER

Ensuring Vital Signals: Reliable Connectivity for Hospitals with Wi-Fi Bridges

2025

silextechnology.com

Contents

Mission Critical Connections: Building Reliable Wireless Infrastructure

At 3:13 AM in Room 247, Mrs. Chen's heart monitor detects severe bradycardia—her heart rate has dropped dangerously low to 35 beats per minute, likely from her recently adjusted cardiac medication. The monitor's algorithm recognizes the life-threatening rhythm and attempts to transmit an urgent alert to the nurses' station. But the device's connection has dropped. The critical alarm can't reach the monitoring station's central display. No notification appears on her care teams' mobile devices.

For three crucial minutes, Mrs. Chen's dangerously slow heart rhythm goes undetected. The severe bradycardia rapidly reduces blood flow to her brain. She becomes confused, then dizzy, and finally loses consciousness as her blood pressure plummets. Connection is restored at 3:16 AM. Immediately, urgent alerts flood the wing—three minutes of queued alarms all arriving at once. Nurse Rodriguez rushes to Room 247, but Mrs. Chen is already unresponsive. What should have been an immediate response to adjust her medication and prevent cardiovascular collapse has become an emergency resuscitation effort.

In those three minutes of broken connectivity, a network interruption transformed a preventable medication-related emergency into a life-threatening crisis. The monitoring technology worked perfectly—detecting the severe bradycardia within seconds—but without reliable connectivity to transmit the alert, the most sophisticated medical devices were dangerously silent.

Network interruptions, however brief, create cascading risks that put patient safety at stake. But scenarios like these are preventable when healthcare facilities have the right wireless infrastructure in place.

THE CONNECTIVITY CHALLENGE WE'RE SOLVING TOGETHER

As healthcare technology specialists, you're navigating an increasingly complex landscape. Legacy medical equipment needs to connect to modern networks. Cybersecurity threats are evolving faster than ever. Regulatory compliance requirements continue to tighten. And through it all, patient care can never be compromised.

Whether you're managing enterprise wireless infrastructure across multiple hospital wings or ensuring that a single critical device maintains its connection during patient transport, you understand that today's healthcare environment demands solutions that are both immediately effective and built for long-term reliability.

WHY WE CREATED THIS WHITE PAPER

At Silex Technology, we've spent more than 20 years working alongside hospital IT teams and biomedical engineers, learning about the unique connectivity challenges you face. In this white paper we'll share our understanding of how the right connectivity solutions can transform your approach to medical device networking.

For IT professionals: We know you're balancing network security, managing countless potential vulnerabilities, and ensuring compliance with evolving cybersecurity mandates. You need solutions that consolidate rather than complicate your security management while providing the centralized control your infrastructure demands.

For biomedical engineers: We understand you need solutions that work right out of the box, enhance patient care immediately, and integrate seamlessly with existing medical equipment. You can't afford lengthy implementation cycles or solutions that create new problems while solving old ones.
Throughout this white paper, we'll explore practical solutions to the connectivity challenges that keep you up at night. You'll learn how Wi-Fi bridges can address everything from legacy equipment integration to cybersecurity threat management, backed by real-world examples and technical insights developed through years of healthcare partnerships.

Most importantly, you'll discover how the right connectivity approach can simplify rather than complicate your technology environment—because the future of healthcare connectivity isn't about managing more complexity; it's about creating reliable, secure solutions that let you focus on what matters most: exceptional patient care.

Let's explore how we can work together to build the connected healthcare infrastructure your patients deserve.

Critical Connectivity Challenges in Hospital Environments

Working in hospital technology means understanding that every connectivity decision you make has the potential to impact patient outcomes. Whether you're an IT professional managing enterprise wireless infrastructure or a biomedical engineer ensuring critical devices stay connected, you face challenges that simply don't exist in other industries. These are more than technical hurdles—they're critical to patient safety and require specialized solutions built specifically for healthcare environments.

WHY CONNECTIVITY IS MISSION CRITICAL

The foundation of modern patient care depends on reliable wireless connectivity. Today's hospitals rely on seamless Wi-Fi to enable:

- Continuous patient monitoring through connected devices that provide real-time health data and instant alerts for clinical intervention
- Mobile medical equipment that can move freely throughout the facility while maintaining secure network connections
- Rapid diagnostic imaging transmission that enables faster clinical decision-making and improved collaboration between specialists
- Integrated medical device ecosystems that reduce manual data entry errors and streamline clinical workflows
- Advanced healthcare technologies including AI-powered diagnostics and remote monitoring capabilities

Yet achieving this level of connectivity reliability isn't simply a matter of deploying standard Wi-Fi solutions–and even some enterprise-grade products fall short. Hospital environments present unique technical, regulatory, and operational challenges that require purpose-built wireless infrastructure. Let's examine the specific obstacles you face and why traditional networking approaches fall short in healthcare settings.

WHEN CONNECTIVITY FAILURES BECOME PATIENT SAFETY RISKS

In your daily work, you've likely experienced the direct connection between network reliability and patient care quality. When body area networks monitoring patient vitals lose connectivity, the sensors can't transmit critical data to controllers designed to detect life-threatening events like cardiac arrhythmias or respiratory distress. These cyber-physical sensor networks require more than basic connectivity—they need sophisticated transmission scheduling that prioritizes life-critical data over routine hospital traffic.

The challenge you face is that different medical data streams have vastly different criticality levels and latency requirements. Cardiac monitoring data demands immediate transmission, while administrative updates can tolerate delays. Yet many wireless infrastructures lack the intelligent queue management needed to consistently prioritize emergency data when network congestion occurs.

As a biomedical engineer, you see this impact firsthand when connectivity failures leave clinical staff without real-time patient monitoring capabilities. These aren't minor inconveniences—they represent gaps in patient care that could delay critical interventions.

NAVIGATING THE HEALTHCARE CYBERSECURITY LANDSCAPE

The cybersecurity challenge you're managing is unlike any other industry. Healthcare data breaches now cost an average of $9.77 million—making healthcare the most expensive sector for data breaches for 14 consecutive years[1] . What makes your environment particularly complex is the sheer number of connected devices you must secure, each representing a potential entry point for malicious actors.

You're also dealing with the growing problem of "shadow data"—unmanaged information sources that affect 35% of data breaches and increase breach costs by 16%[2] . In hospital settings, shadow data often emerges when medical devices connect to your wireless network without proper IT oversight, creating security blind spots that can persist undetected.

You're managing devices from dozens of manufacturers, each with different security standards, update cycles, and Wi-Fi capabilities. Some still operate on outdated wireless standards or lack WPA3 support, forcing you to maintain inconsistent security policies across your device ecosystem. This creates a monitoring and patching nightmare where you must track vulnerabilities across numerous device types, each with unique security requirements.

THE PRESSURE FOR IMMEDIATE SOLUTIONS

Unlike traditional enterprise IT environments that have the luxury of extended planning cycles, healthcare demands rapid responses to emerging challenges. When clinical staff can't access patient records at the bedside, when vital sign monitors disconnect during critical moments, or when mobile equipment loses connectivity during transport, you need solutions that work immediately—not after months of procurement and implementation.

This urgency is particularly challenging when dealing with legacy medical equipment that represents significant capital investments. These devices often lack built-in Wi-Fi capabilities or operate on outdated wireless standards, yet they must integrate seamlessly into modern secure networks to maintain operational efficiency and regulatory compliance.

MANAGING COMPLEXITY WHILE MAINTAINING SECURITY

The threat landscape you're defending against continues to evolve rapidly. Malicious attacks account for 55% of all data breaches, with insider attacks averaging $4.99 million in costs[3] . The challenge is compounded because many medical devices were designed when connectivity was secondary to core functionality, often lacking the robust security features needed for enterprise-grade threat protection.

Your regulatory compliance requirements add another layer of complexity. You must satisfy multiple regulatory bodies while maintaining operational efficiency, often working with wireless infrastructure that lacks modern compliance features. This forces you to implement complex workarounds that may introduce additional security risks or operational inefficiencies.

[1] "Cost of a Data Breach Report 2024," IBM Research

[2] "Cost of a Data Breach Report 2024," IBM Research

[3] "Cost of a Data Breach Report 2024," IBM Research

INTEGRATING DIVERSE MEDICAL DEVICES SEAMLESSLY

The medical devices you support—vital sign monitors, infusion pumps, imaging systems, mobile diagnostic equipment—must not only connect reliably but communicate effectively while maintaining the quality of service clinical operations demand. This requires sophisticated resource allocation where different devices compete for network resources based on data criticality and deadline requirements.

Many of the wireless networks you're managing were designed for basic connectivity rather than the high-density, mission-critical applications that define modern healthcare. You often need to perform upgrades while maintaining continuous operations, as healthcare environments cannot tolerate the extended downtime that major infrastructure overhauls typically require.

This constraint means you need solutions that integrate with existing infrastructure while providing immediate improvements in performance and capabilities—solutions that enhance rather than replace your current investments.

COST AND RESOURCE ALLOCATION CHALLENGES

The proliferation of different Wi-Fi interfaces across medical devices creates significant training burdens for your IT teams. When hospitals deploy equipment from multiple manufacturers—each with unique wireless configuration requirements, management interfaces, and troubleshooting procedures—your network administrators must become proficient in dozens of different systems.

This training requirement extends beyond initial deployment. Every firmware update, security patch, or configuration change requires device-specific knowledge that your team must maintain across the entire device ecosystem. The result is substantial ongoing education costs and increased response times when critical connectivity issues arise. The hidden cost isn't just in formal training programs—it's in the accumulated time your technical staff spends learning, documenting, and maintaining expertise across multiple wireless systems.

When your existing medical devices require Wi-Fi upgrades to meet current security standards, you face substantial recertification costs that often exceed the original equipment purchase price. For hospitals managing dozens or hundreds of connected medical devices, these individual recertification costs can quickly escalate into budget-threatening expenses. The extended approval processes required for embedded wireless modifications can leave equipment vulnerable to security threats or incompatible with modern network infrastructure during transition periods.

MOVING FORWARD WITH PURPOSE-BUILT SOLUTIONS

These challenges underscore why standard enterprise networking solutions often fall short in healthcare environments. The unique operational requirements, regulatory constraints, and patient safety imperatives you manage daily demand Wi-Fi solutions specifically engineered for healthcare settings.

Medical-grade Wi-Fi enhances patient safety with reliable, high-performance connectivity for critical devices and hospital operations. Unlike commercial solutions, these systems undergo rigorous testing, use premium components, and receive 100% verification during manufacturing. This ensures seamless communication, real-time data access, and unwavering support for patient monitoring, creating a safer, more efficient healthcare environment

In the following sections, we'll explore how purpose-built wireless infrastructure can address these specific challenges while providing the reliability, security, and ease of management that both IT teams and biomedical engineers require. Rather than adding complexity to your environment, the right solutions can actually simplify your connectivity management while enhancing patient care capabilities.

Silex Technology Ethernet to Wi-Fi Bridge - Purpose-Built for Healthcare Connectivity

When we designed our suite of Ethernet to Wi-Fi Bridge solutions, we started by listening to healthcare technology professionals like you. We heard about the urgent need to connect legacy medical equipment to modern wireless networks. We learned about the security challenges of managing hundreds of diverse connected devices. We understood the pressure to implement solutions quickly without disrupting patient care workflows. Our response is a comprehensive portfolio of Wi-Fi bridge solutions engineered specifically for the demanding requirements of healthcare environments. Each product in our lineup addresses specific challenges you face daily—from FIPS compliance requirements in government facilities to ultra-low power needs for mobile medical carts.

SILEX TECHNOLOGY WI-FI BRIDGE PRODUCT PORTFOLIO

- BR-500AC: Our flagship bridge features fast roaming with IEEE 802.11r/ai and Quality of Service (WME) prioritization to ensure critical medical data receives transmission priority—all backed by our industry-leading 5-year warranty. It's ideal for high-performance imaging systems, critical care monitoring equipment, surgical devices requiring uninterrupted connectivity, and mobile equipment that moves frequently between hospital units.
- SD-330AC-1402: Our FIPS 140-2 certified Wi-Fi bridge solution available, features dual functionality connecting both Ethernet and serial devices with the highest security standards. Features TAA compliance for government procurement and unique dual functionality as both serial device server and Wi-Fi bridge. Supports legacy RS-232C/RS-422 serial interfaces with end-to-end TLS encryption. Essential for facilities requiring the highest security standards, like government healthcare installations, and for connecting legacy serial medical devices to wireless networks.
- BR-330AC-LP: Engineered for ultra-low power consumption at just 2.75W—a 45% power reduction versus conventional bridges. Supports TLS 1.2 security while maximizing battery life for mobile applications. Perfect for mobile medical carts, portable diagnostic equipment, battery-powered patient monitors, crash carts, and any medical device where extended battery life is critical for continuous patient care.

AMC Manager® YOUR TRUSTED FOUNDATION FOR HEALTHCARE CONNECTIVITY

At Silex Technology, we don't just manufacture wireless bridges—we partner with healthcare technology professionals to solve real connectivity challenges. Our comprehensive approach combines uncompromising reliability, advanced security, streamlined management, and comprehensive compliance capabilities to provide the wireless bridge solution that healthcare organizations need to succeed in today's complex environment. In our next chapter, we'll uncover all the ways our Wi-Fi bridge solutions are purpose-built for the operational needs of your organization.

Designed for Critical Healthcare Capabilities

Choosing a wireless infrastructure partner for your healthcare environment is about finding a company that truly understands the unique challenges you face every day. Silex Technology has built its reputation by working closely with hospital IT teams and biomedical engineers who share our commitment to patient care excellence. We bring more than 20 years of healthcare connectivity expertise to deliver the reliable, secure wireless infrastructure our partners demand.

Our "Absolutely Must Connect" approach drives every design decision we make. While consumer-oriented connectivity technologies might be acceptable for occasional use, healthcare environments demand wireless infrastructure that operates continuously without failure. Medical devices simply cannot afford intermittent connectivity—patient monitors must maintain constant communication with nursing stations, infusion pumps must reliably transmit dosage data, and diagnostic equipment must seamlessly share critical imaging data with healthcare providers.

This philosophy isn't just marketing—it's reflected in our comprehensive manufacturing and testing processes. Each Wi-Fi bridge device undergoes individual testing and calibration using our proprietary ART (Atheros Radio Test) methodology before delivery. ensuring consistent performance specifications that you can depend on from installation through operational lifetime.

Our ISO-certified manufacturing facility in Japan ensures adherence to international quality management standards essential for healthcare environments. This manufacturing excellence is reflected in our products' robust design and reliable performance, helping ensure that each device performs consistently throughout its operational lifetime, even under the demanding conditions typical of hospital environments.Japanese manufacturing excellence

Japan's manufacturing sector has earned global recognition for its deep-rooted cultural traditions of meticulous hard work, studiousness, precision, innovation, and perseverance[4] —qualities that directly translate into superior product quality and manufacturing excellence. This Japanese commitment to quality and continuous improvement (kaizen philosophy) has resulted in a durable global competitive advantage, with Japanese companies consistently setting benchmarks for operational excellence and innovative products across industries.

Silex Technology embodies these Japanese manufacturing principles at our ISO-certified facility in Japan, where every Wi-Fi bridge is built to the exacting standards that have made Japanese manufacturing synonymous with reliability worldwide. Our manufacturing processes reflect the same attention to detail and commitment to quality that has established Japan as a global leader in precision manufacturing.

[4] Japan's Most Durable Competitive Advantage, Hennessy Funds

MEETING THE CRITICAL NEEDS OF CONNECTED HEALTHCARE

Our products are designed to deliver the three critical capabilities that hospital IT teams and biomedical engineers require: **uncompromising reliability, enterprise-grade security, and simplified management**—all purpose-built for the demanding healthcare environment. Let's examine how each capability addresses the real-world challenges you face daily.

UNCOMPROMISING RELIABILITY WHEN LIVES DEPEND ON CONNECTIVITY

In healthcare, network reliability isn't just about convenience—it's about patient safety. The BR-500AC is engineered to eliminate these risks through advanced reliability features designed specifically for medical environments.

ADVANCED ROAMING TECHNOLOGY FOR SEAMLESS MOBILITY

Healthcare happens on the move—medical carts transport between units, portable diagnostic equipment moves to patient bedsides, and critical care devices must maintain connectivity during emergency responses. The BR-500AC and BR-330AC-LP feature fast roaming capabilities that ensure your medical equipment stays connected even as it moves throughout your facility.

Supporting the cutting edge Wi-Fi standard IEEE 802.11r (Fast BSS Transition) and IEEE 802.11ai (Fast Initial Link Setup), these bridges dramatically reduce disconnection time during access point transitions. When an access point goes down or a device roams to a new coverage area, the bridge quickly jumps to the strongest available connection without missing a beat.

The adjustable roaming threshold gives you control over when devices begin searching for stronger signals, allowing you to optimize performance for your specific facility layout and RF environment. This prevents unnecessary roaming in areas with temporary signal fluctuations while ensuring timely handoffs when truly needed.

POWERFUL RADIO PERFORMANCE THAT EXCEEDS EXPECTATIONS

The BR-500AC incorporates powerful dual-band radios that significantly exceed the capabilities of many embedded Wi-Fi solutions found in medical devices. These enterprise-grade radios provide extended range and coverage for reliable connectivity throughout large hospital facilities, superior signal penetration through walls and medical equipment, and enhanced performance in high-density environments where multiple devices compete for wireless resources.

This radio performance advantage means your medical devices can maintain reliable connectivity in situations where built-in Wi-Fi modules might fail—from basement storage areas to upper floors with challenging coverage.

INTELLIGENT TRAFFIC PRIORITIZATION

Understanding that not all network traffic is equally important in your healthcare environment, the BR-500AC incorporates Wireless Multimedia Extensions (WME) support as part of its Quality of Service capabilities. This feature enables automatic prioritization of critical medical data over less time-sensitive traffic, ensuring that vital signs monitoring, alarm notifications, and other life-critical communications receive priority transmission even during periods of high network utilization.

FLEXIBLE DEPLOYMENT OPTIONS FOR ANY CONNECTIVITY CHALLENGE

Every hospital connectivity challenge is unique, and our bridges adapt to your specific requirements through flexible operating modes.

Single Client Mode provides completely transparent bridging where your connected device's MAC address passes directly through to the wireless network. This ensures your existing network policies, device tracking systems, and security configurations continue working exactly as designed—the bridge becomes virtually invisible to your infrastructure.

Multi-Client Mode transforms a single BR-500AC into a wireless hub supporting up to 16 devices through an Ethernet switch. This mode proves ideal for equipment clusters in busy hospital units or when creating mobile connectivity for entire medical carts loaded with multiple devices.

ENTERPRISE-GRADE SECURITY THAT REDUCES RISK AND COMPLEXITY

Hospital networks face unique security challenges—hundreds of medical devices from dozens of manufacturers, each potentially representing a different vulnerability vector. The BR-500AC addresses these challenges by providing a unified security platform that simplifies management while strengthening your overall security posture.

WPA3 ENTERPRISE SECURITY ACROSS ALL CONNECTED DEVICES

The BR-500AC and SD-330AC-1402 support the latest WPA3 encryption alongside WPA2 Enterprise and Personal modes, ensuring compatibility with both current infrastructure and future security requirements. Every device connected through these bridges benefits from the same enterprise-level security standard, regardless of the original device's built-in security capabilities.

This unified approach solves a critical problem: instead of managing different security standards across devices from multiple manufacturers, you can standardize your entire hospital on one consistent, enterprise-grade security implementation.

REDUCED ATTACK SURFACE THROUGH VENDOR CONSOLIDATION

Traditional hospital networks often include hundreds of Wi-Fi-enabled devices from dozens of different manufacturers, each representing a potential security vulnerability. Our bridge solutions provide protection by consolidating connectivity through single, trusted platforms that you control and monitor centrally. Instead of 100 different devices each creating their own potential entry points into your network, you can channel connectivity through bridges that provide fewer vulnerability vectors to monitor, simplified security policy enforcement, centralized security monitoring, and consistent security standards regardless of underlying device capabilities.This approach provides several critical security advantages:

- **Fewer vulnerability vectors** to monitor and protect
- **Simplified security policy enforcement** across all connected devices
- **Centralized security monitoring** instead of tracking multiple device types
- **Consistent security standards** regardless of underlying device capabilities

STREAMLINED INCIDENT RESPONSE AND MANAGEMENT

When security incidents occur in complex, multi-vendor environments, response time is often delayed by the need to coordinate with multiple vendors, understand different device behaviors, and manage various security protocols. The BR-500AC and SD-330AC-1402 simplify incident response through vendor consolidation and standardized security protocols.

In the event of a security issue, having fewer vendor relationships simplifies communication and coordination, speeding up containment and resolution. Your IT team can more effectively manage and enforce security policies, conduct security audits, and monitor network activity when working with a consistent, well-understood platform.

ADVANCED AUTHENTICATION AND ACCESS CONTROL

The BR-500AC and the SD-330AC-140 integrates seamlessly with your existing security infrastructure through:

- **IEEE 802.1X authentication** that works with your current certificate-based systems
- **MAC address filtering** for additional device-level access control
- **Multiple encryption options** to accommodate diverse security requirements
- **Device access password protection** for additional authentication layers

These features ensure our bridges fit into your existing security framework while providing the flexibility to adapt to evolving security requirements.

FIPS COMPLIANCE FOR GOVERNMENT AND HIGH-SECURITY HEALTHCARE ENVIRONMENTS

For healthcare organizations serving government agencies, veterans' affairs facilities, or other high-security environments, cryptographic compliance isn't optional—it's mandatory. Silex Technology addresses these requirements through our comprehensive FIPS (Federal Information Processing Standards) portfolio and forward-looking investment in next-generation security standards.

The SD-330AC-1402, which provides FIPS 140-2 validated cryptographic modules. This certification ensures that cryptographic operations meet the rigorous security requirements established by the National Institute of Standards and Technology (NIST) for protecting sensitive but unclassified information.
FIPS compliance delivers several critical advantages for healthcare organizations:

- **Government mandate compliance** for federal agencies and contractors, including Veterans Affairs hospitals
- **Enhanced cryptographic security** through validated encryption algorithms and key management
- **Audit readiness** with documented security controls that meet federal standards
- **Future-proofed investment** as we prepare for evolving compliance requirements

For healthcare IT teams managing government contracts or serving populations requiring the highest levels of security assurance, our FIPS-validated solutions provide the compliance foundation necessary for regulatory approval and operational security.

We've also got an eye toward the future—we're one of the only connectivity solutions manufacturers developing FIPS 140-3 validated cryptographic modules. You'll be ready for the 2026 sunset of FIPS 140-2[5].

[5] "FIPS 140-3 Transition Effort," National Institute of Standards and Technology, U.S. Department of Commerce

CENTRALIZED ADMINISTRATION ACROSS YOUR ENTIRE BRIDGE NETWORK

AMC Manager® provides single-pane-of-glass management for your entire bridge deployment. Whether you have ten bridges or hundreds, you can configure, monitor, and maintain them all from one central console. This centralized approach eliminates the need to manage individual devices separately and ensures consistent configuration across your facility.

Key management capabilities include:

- **Unified configuration management** for consistent settings across all bridges
- **Real-time monitoring** of bridge performance and connectivity status
- **Remote troubleshooting** without disrupting patient care areas
- **Centralized reporting** for network performance and security compliance

RAPID BULK DEPLOYMENT WITH BR KITTING UTILITY

The BR Kitting Utility, integrated into AMC Manager®, enables rapid bulk configuration of multiple units—invaluable when you need to deploy wireless connectivity for new hospital wings, connect numerous medical devices simultaneously, or standardize configurations across your facility.

You can configure device settings, security parameters, and network policies centrally, then deploy pre-configured bridges efficiently without requiring individual device setup. This approach significantly reduces deployment time and ensures consistency across your installation.

AUTOMATED CERTIFICATE MANAGEMENT FOR SECURITY COMPLIANCE

Certificate management represents one of the most complex aspects of healthcare network security. The BR-500AC and SD-330AC-1402 streamline this process through AMC Manager®'s support for both SCEP (Simple Certificate Enrollment Protocol) and EST (Enrollment over Secure Transport).

As hospitals move toward shorter certificate lifecycles for enhanced security—with many organizations now changing certificates multiple times per year instead of annually—automated certificate management becomes essential. AMC Manager® handles certificate enrollment, renewal, and distribution automatically, reducing administrative overhead while maintaining compliance with security policies. This automation is particularly valuable during certificate updates, where manual processes could result in device downtime or connectivity interruptions that impact patient care.

AVOID FDA RECERTIFICATION WITH LOW-POWER DESIGN

One of the most overlooked challenges in healthcare technology deployment is navigating FDA certification requirements. When medical device manufacturers modify their products or integrate new components it can trigger the need for FDA recertification—a process that can take six months to a year and requires specialized regulatory expertise that many organizations lack.

The BR-500AC and BR-330AC-LP feature flexible power designs that help you avoid this regulatory burden entirely. While these devices ship with standard AC adapters, they can also be powered by 5-volt DC through optional USB cable connections. This low-power design approach keeps the bridges classified as network infrastructure rather than medical device modifications, eliminating FDA certification requirements.

A COMPREHENSIVE SOLUTION PURPOSE-BUILT FOR HEALTHCARE

Our Wi-Fi bridge products are designed to address the unique reliability, security, and management challenges that healthcare facilities face. In the next chapter, we'll explore why Silex Technology's approach to healthcare connectivity goes beyond providing products to delivering the partnership and expertise that modern healthcare demands.

Learning from Europe's Most Demanding Healthcare Environment

Consider the complexity you manage daily, then imagine scaling that challenge across one of Europe's largest university hospitals. That's exactly what our partners at Charité - Universitätsmedizin Berlin face every day. Operating across four campuses with more than 100 departments, Charité's IT team manages over 20,000 staff members and approximately 12,000 wireless clients daily. Their infrastructure spans more than 450 network nodes, 4 data centers, and over 35,000 active devices—a scale that would challenge any wireless solution.

When Charité needed to transition their LAN-based medical device network to a secure 5GHz wireless infrastructure with enterprise-grade 802.1x authentication, they discovered what you've likely experienced: solutions that work well in corporate environments often fall short of healthcare's demanding requirements. Their existing network partners couldn't meet their strict EAP-TLS authentication requirements, leaving them searching for alternatives that could handle both the technical complexity and security standards essential to their operations.

The breakthrough came when they tested our BR-4600WAN Ethernet-to-Wi-Fi bridge. What impressed their IT team wasn't just that it worked—it was how quickly they could validate that it would meet their specific requirements. This rapid deployment capability reflects something we hear consistently from our healthcare partners: you need solutions you can implement quickly when patient care depends on connectivity.
But this isn't a short-term technology relationship. Over more than a decade, they've grown with us through four generations of our bridges—from the original SX-BR-4600WAN to today's BR-500AC. Each transition reflected evolving security requirements and advancing technology standards, exactly the kind of changes you navigate regularly in your own environment.

When Germany's Federal Office for Information Security mandated an upgrade from TLSv1.0 to TLSv1.2—the type of compliance challenge that can derail operations if not handled properly—we provided immediate firmware updates and continued support. Charité's infrastructure remained compliant without disruption, allowing their team to focus on patient care rather than scrambling to address connectivity failures.

UNDERSTANDING WHAT PARTNERSHIP REALLY MEANS IN HEALTHCARE

This is what partnership looks like in healthcare connectivity: understanding your unique challenges, anticipating your evolving needs, and delivering solutions that support your mission of exceptional patient care. When you choose Silex Technology, you're not just purchasing connectivity hardware—you're gaining a technology partner who recognizes the critical nature of your work and shares your commitment to keeping life-saving operations connected, secure, and operational when it matters most.

Building the Connected Healthcare Infrastructure Your Patients Deserve

Throughout this white paper, we've explored the critical connectivity challenges that define your daily work—from ensuring life-critical medical devices maintain uninterrupted network access to managing complex security requirements across hundreds of connected devices. We've examined how these challenges directly impact patient safety, regulatory compliance, and operational efficiency in ways that simply don't exist in other industries.

The solution isn't to accept these challenges as inevitable complexities of modern healthcare. Instead, it's about choosing wireless infrastructure partners and technologies that are purpose-built for your unique environment. What sets Silex Technology apart isn't just our technical capabilities—it's our understanding that successful healthcare connectivity requires more than good products. It requires a partner who understands the unique pressures you face, the constraints you work within, and the patient care outcomes that drive every decision you make.

READY TO TRANSFORM YOUR HEALTHCARE CONNECTIVITY?

The challenges facing healthcare connectivity won't solve themselves, and the demands on your wireless infrastructure will only continue to grow. We invite you to explore how a partnership with Silext Technology can address your specific connectivity challenges. Whether you're dealing with legacy equipment integration, security management complexity, or the need for rapid deployment capabilities, we're here to help you build the wireless infrastructure that supports exceptional patient care. Connect with our team today to discover how we can solve your wireless infrastructure challenges while supporting the exceptional patient care that defines your organization.