Key Source International

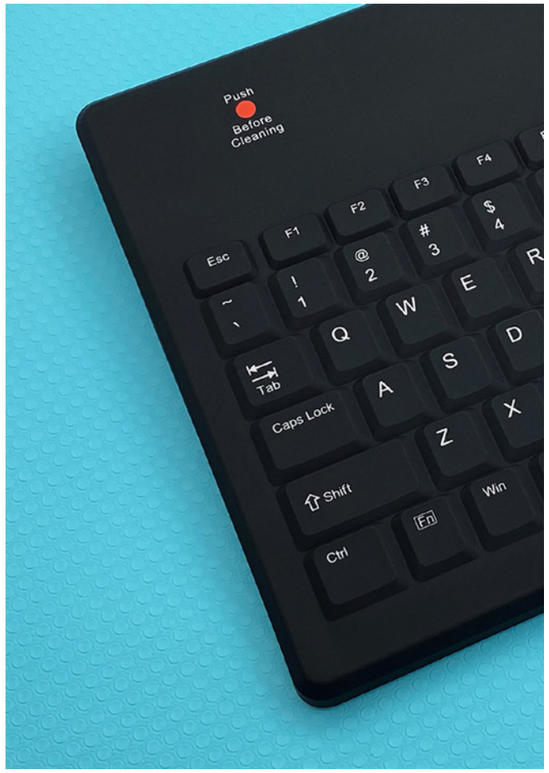
Protecting Patient Safety with Endpoint Security and Infection Control at the Desktop

Kevin Krause,
VP of Sales

In 2023, the threat of internal data breaches at healthcare facilities is still prevalent, and staying ahead of the curve to protect confidential patient information remains a necessity. Hospital-acquired infections, as well, are a growing concern as hospitals continue the fight against new and ever-virulent bacteria, viruses, and fungi that cause severe illness and death.

First, the desktop computer remains a primary tool for healthcare professionals, and unsecured keyboards are a weak link in the security chain. While it's true outsider threats to hospital IT security via hacking and ransomware attacks are on the rise and widely discussed, internal threats to endpoints are often overlooked. Recent statistics indicate the healthcare industry continues to experience significant internal data breaches caused by employees. One reliable study found over 90 percent of healthcare organizations experienced at least one data breach in the past two years, with a substantial slice caused by staff negligence or malicious intent. Stories of hospital chains suffering breach of confidential patient data caused by an insider who deliberately accessed and shared the information still abound in our news feeds.

Further, as clinicians continue vigilance in the fight against deadly environmental pathogens, keyboards remain high-touch surfaces and known vectors for cross-contamination. The crucial need still exists for clinicians to access all available tools to prevent infections that compound patient illness, prolong hospital stays, and impact a hospital's bottom line. In March 2023, CDC epidemiologist Dr. Meghan Lyman stated about Candida auris, a dangerous yeast fungus now circulating in US hospitals, "The rapid rise and geographic spread of cases is concerning and emphasizes the need for continued surveillance and adherence to proven infection prevention and control."



The product engineers at KSI recognized long ago that its keyboards could offer a robust solution for healthcare organizations looking to strengthen a hospital's endpoint security and desktop infection control measures.

In the words of Kevin Krause, vice president of sales at KSI, "KSI medical-grade keyboards are uniquely designed to meet the specific needs and rigorous standards of healthcare."

KSI integrates top-brand mix-and-match security components into its keyboards. Customers can choose an HID 500 dpi biometric fingerprint reader, rfIDEAS WaveID® Plus dual band (125kHz and 13.56Mhz) contactless card reader, or both. The combination of both offers multifactor authentication in one device and provides an additional layer of security to keep confidential patient data safe, as well as a compact solution that deters desktop clutter. KSI security components are compatible with popular Single Sign-On (SSO) platforms used in hospitals, including BIO-key, Identity Automation, Identiv, Omnikey, and Imprivata.

Compatibility with Imprivata software is of particular importance as it includes OneSign, the company's SSO, and its Confirm ID platform that enables DEA ePrescribe compliance and convenient hands-free mobile authentication. Imprivata, a leading healthcare IT security solution, is widely used in hospitals across the country and overseas. KSI keyboards offer seamless integration with Imprivata software, allowing healthcare workers to securely access patient data and comply with ePrescribe regulations while maintaining the highest level of multifactor security.

Just as important is integration of KSI's award-winning, patented LinkSmart® cleaning button with accompanying San-a-Key® software. LinkSmart with San-a-Key provides for fast and easy surface disinfection of KSI keyboards, aiding in prevention of cross-contamination with use of hospital-approved germicidal wipes.

> "KSI medical-grade keyboards are uniquely designed to meet the specific needs and rigorous standards of healthcare"

One press of the bright red LinkSmart button temporarily disables keys and triggers San-a-Key software to display an onscreen, animated keyboard schematic that guides end user keyboard surface disinfection. The schematic depicts the keyboard being disinfected synonymous with the user wiping the keyboard surface in real-time—one key or one region at a time until all keys are wiped clean. User-defined San-a-Key allows hospital administrators to establish keyboard disinfection schedules and send popup cleaning reminders to all desktops. Hospitals can now track tthe who, when, and where of KSI keyboard cleaning across the enterprise.

KSI keyboards come in a range of form factors and feature low-profile, full-travel keys that speed workflow. KSI 1700 series hard-shell keyboards and 2000 series silicone-covered keyboards are full-sized, while KSI 1800 series silicone-covered keyboards are compact and designed for mobile carts and workstations with limited space. KSI 1900 series pods feature the same security components and compatibilities as KSI keyboards for those customers seeking a standalone solution.

By choosing KSI keyboards, healthcare organizations safeguard confidential data, reduce the risk of internal data breaches, meet key compliances, and create a safer environment for patients and clinicians. ES