USE CASE | *HEALTHCARE*

KSI Multifactor Authentication Helps Healthcare Meet EPCS Compliance

KEY BENEFITS of KSI EPCS PRODUCTS:

- Compatibility with Imprivata® Confirm ID platform
- Embedded HID® Crossmatch® biometric authentication
- Hands-free BLE mobile authentication enabled
- Two-factor authentication, meeting DEA requirements
- Multiple functions routed through one USB
- Minimization of workflow disruption
- Reduction of password use and management
- Protection against unauthorized access to PHI
- Component integration unclutters the desktop
- FIPS-201 and HIPAA compliant
- Option to layer security with added RFID
- Optional LinkSmart® keyboard cleaning button

Studies indicate so-called doctor shoppers obtain, on average, 32 prescriptions from 10 different doctors. Moreover, nearly 90% of handwritten opioid prescriptions may contain errors.

With the dangerous and illicit activity of doctor shopping having become a pervasive problem, the Drug Enforcement Agency (DEA) set forth Electronic Prescribing for Controlled Substances (EPCS) regulation designed to minimize the use of controlled substances and overdose related to over-prescribing. New York state practitioners are already in compliance with the new electronic standard that eliminates paper prescriptions. Many other states are now in process of adopting their own versions of New York's I-STOP. Soon, EPCS ePrescribe will be standard protocol within United States healthcare facilities.

The DEA outlines specific requirements to which healthcare providers, pharmacies, and technology vendors must adhere, one being a mandate that prescribers use two-factor authentication when signing electronic prescriptions.

CHALLENGE: EPCS compliance, strong authentication, port conservation, and increased efficiency

The state legislature has just passed EPCS regulation that mandates all prescribers become compliant within two years. Leadership of a regional health system has directed its IT team to prepare a plan for the looming deadline.

The team dismisses a token solution due to its overall goal of eliminating use of burdensome passwords. Hard tokens have proven to be expensive, often misplaced, and difficult to manage. Soft tokens present potential security risks and administrative headaches.

Along with adoption of the Imprivata® Confirm ID authentication platform to help meet compliance, locating compatible hardware is top priority. The IT team seeks FIPS-201 and HIPAA compliant security peripherals that are compatible with Confirm ID, in order that the DEA's two-factor authentication requirement is met.

Thin clients in operation on the vast majority of the health system's desktops present their own challenge – complying with EPCS threatens to make managing limited available ports even more difficult. Examining the bigger picture, the team recognizes that, over time, the hospitals' workstations have become unruly and inefficient. Security peripherals clutter provider workspaces and increasingly go missing.

The health system needs a comprehensive solution that addresses compliance while gaining efficiencies.

The DEA mandates providers use two factors of authentication when signing an electronic prescription

KSI embedded BLE used in mobile authentication, combined with integrated FIPS 201 fingerprint biometrics, meet compliance of EPCS two-factor identity modalities

FACTOR 1: KSI embedded BLE supports Confirm ID hands-free mobile authentication

ePrescribe is enabled with two-factor identification and the Confirm ID platform

Imprivata
ID

FACTOR 2: KSI fingerprint biometrics provides the second required factor of identity

KSI hardware and use of Confirm ID puts healthcare in compliance with EPCS

SOLUTION: Simple, efficient ePrescribe workflow via integrated two-factor authentication, through one USB port

After careful research, the IT team realizes KSI is the only company offering the range of all-in-one solutions needed to resolve each issue it confronts in: 1) meeting DEA and healthcare strong authentication regulations, 2) eliminating passwords and password management, and 3) streamlining workstations.

KSI's integration of hardware components meets the two-factor identity modalities required by the DEA, using:

- Bluetooth® Low Energy module
- FIPS 201 compliant biometric fingerprint reader

The team's selection of top-ranked Imprivata® Confirm ID ensures an auditable chain of trust for the entire EPCS process – from identity proofing and credential enrollment, to integration with EHR and prescription signing applications. KSI embedded low-energy Bluetooth® supports utilization of Confirm ID by enabling hands-free mobile authentication that saves time for health system providers, secures the desktop, and provides the first factor of DEA-mandated authentication.

The second factor, provided by an embedded 500 dpi HID® Crossmatch® biometric fingerprint reader, eliminates the need for a separate device that untidies the workspace. KSI's biometric component is high quality, FIPS 201 compliant, and compatible with leading Single Sign On applications used by healthcare.

KSI EPCS SOLUTIONS

KSI-1700 CFFFB Keyboard
KSI-1802R CFFFB Keyboard
KSI-1900 CFFFB Security Pod
And many more; please inquire

Use of KSI dual-factor authentication products offered a robust, HIPAA-compliant solution, and allowed the IT team to comply with the new mandate. Prescribers and administrators saved time, with the need for passwords and cumbersome password management significantly reduced. Electronic prescription workflow was made simple using KSI hardware in conjunction with Imprivata® Confirm ID. Upon identity proofing and credentialing, a quick fingerprint scan and convenient mobile authentication was all it took to securely access PHI and ePrescribe applications. Health system leaders were assured that doctor shopping and internal fraud were now much less likely due to strong authentication implemented at every desktop. With all security functions routed through a single USB port, thin client ports were freed up for other uses, and provider workstations were made more orderly.

The IT team went further by adding yet another layer of protective security to every KSI device. Embedded RFID card readers provided fast, contactless prescriber identity without impact to workflow. At the request of Infection Control, the optional, patented LinkSmart® cleaning button was added to each KSI keyboard to allow clinicians fast disinfection of keyboard surfaces with germicidal wipes throughout the day.

In KSI technology, the IT team found an all-in-one, compatible EPCS solution that complies with DEA and healthcare regulations, prevents doctor shopping, conserves ports, and increases efficiency. Health system providers are now saving time better spent devoted to patient care.