Kno2®

Security Overview

Last Updated: November, 2018

KNO2 SECURITY OVERVIEW

Kno2® is a cloud-based healthcare solution that facilitates interoperable patient document exchange between providers across the care continuum. The communication that Kno2 provides must maintain the confidentiality, integrity and availability of electronic protected health information (PHI) to be trusted for use in patient care. To that end, the protection and security of patient information is of utmost importance and incorporated into the design, engineering, deployment and operation of the Kno2 application.

This document is intended to provide a high-level overview of the security capabilities and overall management of security program for Kno2.

Information Security Program Management

Kno2 maintains a formalized Information Security program lead by a CISO and built upon best-practice security practices. Kno2 uses HIPAA/HITECH as the primary framework for the security program structure and incorporates NIST 800-171 security controls into company operations. HIPAA security risk assessments are performed annually to review and remediate findings discovered in systems and operational procedures. Weekly meetings with Kno2 management are held to communicate Information Security program status and remediate any immediate risks to the Kno2 environment.

The Kno2 Security Culture

Kno2 fosters an open security culture where employees are reminded weekly through informal communication about current security topics. Staff members are encouraged to identify security issues and report them for remediation.

Kno2 staff are required to attend annual training on the requirements of the Health Information Portability and Accountability Act (HIPAA) and the protection of PHI. This training includes coverage of Kno2 Information Security policies and procedures, as well as current security trends. Records of this training is electronically maintained with the employee's file. New employees receive training as a part of their orientation with the company and all employees receive weekly security reminders on current security issues.

Kno2 requires a criminal history check for all full-time, part-time and temporary employees upon hire once a conditional offer of employment has been extended by the hiring manager. An offer of employment may be extended to an applicant prior to the completion of the criminal conviction check. However, the applicant's first day of work in the position must not be prior to the satisfactory completion of the criminal conviction check.

Vendor/Partner Management

Kno2 performs formalized risk assessments on potential vendors or partners that may be used to process, store or transmit PHI within the Kno2 application. These assessments consider the security controls and features offered by the vendor/partner product and attempt to determine the maturity of their overall information security program. Vendors/partners with inadequate security capabilities may not be considered unless documentation of successful remediation activity is accepted by Kno2.

Protection of Data at Rest and In Transit

All communications with Kno2 are conducted using best-practice encryption standards. Kno2 follows current security threats involving cryptography and compliance requirements, and adjusts the use of ciphers and protocols accordingly, including deprecation of support as necessary. Encryption is implemented using FIPS-140-2 compliant algorithms and a 2048-bit RSA key using Perfect Forward Secrecy exceeding HIPAA requirements and protecting against future cryptographic breakthroughs.

Kno2 utilizes an open-standards based authentication framework to enable third party applications to securely access the Kno2 API Services. Included within this framework are specific technical security requirements for establishing communication with Kno2. These include, but are not limited to:

- The Kno2 Generated & Managed App ID
- The Kno2 Assigned API Client Key & Secret
- Whitelisted IP Addresses for Token Generation

Kno2 can also accept HL7 interface data over industry standard IPSEC encrypted VPN tunnels. This provides a secure option for clinical data exchange for legacy applications that cannot use the Kno2 secure API services. This VPN service supports AES 256-bit encryption and SHA256 based hashing algorithms.

Data Center and Hosting Security

Kno2 utilizes Microsoft® Azure® services for all application infrastructure components and data storage. This first-tier IaaS/PaaS platform provides Kno2 with a secure base infrastructure and high degrees of resiliency and scalability. The Azure SLA guarantees that the critical components of the Kno2 application will be available 99.9% of the time.

Microsoft Azure is a cloud security leader and maintains compliance with the majority of legal and regulatory information security frameworks in existence today including HIPAA/HITECH, HITRUST, ISO/IEC 27001, NIST 800-171, PCI-DSS, FedRAMP, and FISMA. These frameworks provide for a robust set of controls to help ensure the privacy and security of Kno2 confidential data housed in the Microsoft data centers.

Physical access to the Microsoft data center facilities is guarded by outer and inner perimeters with increasing security at each level, including perimeter fencing, security officers, locked server racks, multi-factor access control, integrated alarm systems, and extensive 24x7 video surveillance from the operations center. No Kno2 employees have the need for physical access to these data center facilities.

All Kno2 data is stored in a database instance hosted on Microsoft Azure which provides for transactional integrity. Kno2 application servers are protected using Microsoft BitLocker® full disk encryption to prevent against data theft at the drive level. The Kno2 database implements an additional step to further secure confidential data by using field level AES encryption on high-risk data elements. Testing and troubleshooting take place within the secure hosted environment and no system data, including PHI, is stored or copied locally without authorization and appropriate security controls.

Kno2 utilizes Microsoft Azure network security features that allow for granular firewall controls to whitelist communications between backend servers. Multiple private virtual networks are used to further separate environments and application servers from each other and from public Internet access. This prevents random reconnaissance network probing and greatly reduces the options for lateral movement within the environment should an attacker ever penetrate beyond the external security defenses.

Kno2 utilizes Azure Services instead of full virtual servers wherever possible to reduce the attack surface area of the Kno2 application. An attacker has far fewer options when only targeting a specific Azure Service that is lacking the underlying server operating system and the inherent vulnerabilities. These services also allow for geographic diversity across multiple Microsoft data centers in order to increase business continuity capabilities. The remaining virtual servers that are used in the Kno2 infrastructure are automatically configured to meet the Center for Internet Security (CIS) configuration templates. This ensures that best-practice security measures are in place for all virtual machines without requiring manual configuration and eliminating configuration errors.

System Access – Minimum Necessary

Administrative access to the Kno2 applications servers hosted within the Microsoft Azure environment is limited to only a small number of individuals with very specific job roles involving the maintenance of the system. No other Kno2 employees have any access to the Kno2 environment. Security controls for those team members requiring remote access to the Kno2 system include individual user accounts with strong passwords and dual-factor authentication. Any individual needing access to the Kno2 system for maintenance or troubleshooting must also formally request the access through a supervisor for approval and auditing purposes.

The Kno2 application supports several customer-configurable options for user access based on organizational security requirements. Organizational administrator accounts require identity-proofing before activation and require dual-authentication. Strong passwords are required for standard user accounts by default, but the organizational administrator can also require dual-factor authentication if desired. All customer access is logged and directly accessible within the application to allow for user-level audits of organizational activity.

Monitoring

The Kno2 system is monitored using both Microsoft Azure and external third-party cloud-based systems. This allows for visibility into specific Kno2 application internals as well as traditional system utilization monitoring. Automated alerts are sent to system administration staff when key elements of the Kno2 application are outside of normal parameters. Web application errors are logged for review to distinguish between normal web server errors and potential threats to the system.

Security Testing Procedures

Kno2 uses a multilayered approach to security testing. The security team is included in sprint reviews to help conduct threat modeling for new application features and requests and static code analysis is performed early in the development lifecycle. Any serious issues identified during code analysis can be prioritized for validation and remediation before code is released to the next environment. Kno2 uses commercially available static code analysis tools to perform this testing.

The Kno2 web application is tested again once it has been staged to production web servers with commercial web application security testing tools. These automated tests are conducted using authenticated access to the application to provide maximum insight into potential security issues. These tests evaluate the application for the 2017 OWASP Top 10Application Security Risks including:

A1. Injection

A2. Broken Authentication

A3. Sensitive Data Exposure

A4. XML External Entities (XXE)

A5. Broken Access Control

A6. Security Misconfiguration

A7. Cross-Site Scripting (XSS)

A8. Insecure Deserialization

A9. Using Components with Known Vulnerabilities

A10. Insufficient Logging & Monitoring

Kno2 additionally uses commercial network vulnerability scanning tools to test all publicly available services for misconfiguration or other security issues. These tests are performed weekly and the results analyzed by security staff. Any services identified as high risk are reported and prioritized for remediation.

Finally, Kno2 contracts with a third-party firm to perform annual penetration and web application security testing. This testing includes an exhaustive review of the Kno2 technology stack and internal processes and procedures as related to HIPAA/HITECH standards. Any security findings are prioritized for remediation based on severity and logged as a support ticket for progress tracking.

Security Reviews & Industry Certifications

Kno2 has undergone and continues to pursue security reviews and appropriate industry certifications, including:

- HIPAA/HITECH regulatory compliance
- Surescripts® validation for use/connectivity to their accredited Health Information Network
- IHE (Integrated Health Enterprise) Certification 3 years running
- Drummond 2014 Modular EHR Certification