Security Guide

Xerox® Share Patient Information App

Xerox® Share Patient Information App

Document Version: 2.1 (August 2021)

REVISION HISTORY

Version	Date	Details
1.0	March 2019	Initial Version
2.1	August 2021	Branding updates • Changed App name to “Share Patient Information” • Authentication enhancements

.

Contents

1. Preface

The Xerox® Share Patient Information app provides an easy path for health care industry users to scan patient records and distribute them via the Kno2: Interoperability as a Service™ platform. After a one-time registration of the device with their Kno2 account, users can walk up to a Xerox printer, log in to the Xerox® Share Patient Information app, and scan one or more documents. The scanned images can be sent using Kno2 messaging to selected recipients (e.g., other health care providers) or uploaded by Kno2 into an integrated Electronic Health Record system (EHR).

The Xerox® Share Patient Information app is only available to USA-based Xerox App Accounts.

The Xerox® Share Patient Information app can be installed on Xerox multifunction devices which support ConnectKey technology. In order to use the app, a person must purchase a Kno2 license, allowing the MFP to be enabled in the Kno2 system. When the Kno2 system is accessed with the Xerox® Share Patient Information app, users are able to scan documents and send them via the Kno2 system to other providers or organizations that are part of the Kno2 system.

Purpose

The purpose of the Security Guide is to disclose information for the Xerox® Share Patient Information app with respect to device security. Device security, in this context, is defined as how data is stored and transmitted, how the product behaves in a networked environment, and how the product may be accessed, both locally and remotely. This document describes design, functions, and features of the Xerox® Share Patient Information app relative to Information Assurance (IA) and the protection of customer sensitive information. Please note that the customer is responsible for the security of their network and the Xerox® Share Patient Information app does not establish security for any network environment.

This document does not provide tutorial level information about security, connectivity or Xerox® Share Patient Information features and functions. This information is readily available elsewhere. We assume that the reader has a working knowledge of these types of topics.

Target Audience

The target audience for this document is Xerox field personnel and customers concerned with IT security.

It is assumed that the reader is familiar with the Xerox® Share Patient Information app; as such, some user actions are not described in detail.

Disclaimer

The content of this document is provided for information purposes only. Performance of the products referenced herein is exclusively subject to the applicable Xerox Corporation terms and conditions of sale and/or lease. Nothing stated in this document constitutes the establishment of any additional agreement or binding obligations between Xerox Corporation and any third party.

2. General Security Protection

Data Protection Overview

To use the Xerox® Share Patient Information app a user must log in.

The SPI app informs Kno2 that authentication is required by a configured Identity Provider. (Kno2 is the default Identity Provider.) The Identity Provider presents the MFD user with a log in dialog. The user supplies credentials for the user's account with the Identity Provider. When 2-Factor authentication enabled with the identity provider, the Identity Provider will interact with the user to obtain the user-supplied code. For a successful log in, the Identity Provider returns an authCode which the SPI app exchanges for authorization tokens with Kno2. When Kno2 acts as the Identity Provider, the user will supply their Kno2 username and password.

If the customer environment includes an Authentication solution (e.g., Xerox® Workplace Suite/Cloud) with Single Sign On (SSO) functionality enabled, the user can agree to have their Refresh token securely stored and automatically applied during subsequent app launches.

Once authenticated, the user proceeds with specifying the associated patient record information, scanning, and reviewing the message to be sent. After user-approval, the app uploads the image files to the Kno2 system using the Kno2 API. Each invocation of the API is authorized by the user's Access Token. After transmission of patient information (or cancellation), all cloud-based and device-based storage of the images is deleted.

User Data Protection within the products

DOCUMENT AND FILE SECURITY

File content is protected during transmission by standard secure network protocols at the channel level. Since document source content may contain Personally Identifiable Information (PII) or other sensitive content, it is the responsibility of the user to handle the digital information in accordance with information protection best practices.

HOSTING - MICROSOFT AZURE

The Share Patient Information web service is hosted on the Microsoft Azure Network. The Microsoft Azure Cloud Computing Platform operates in the Microsoft® Global Foundation Services (GFS) infrastructure, portions of which are ISO27001-certified. Microsoft has also adopted the ISO 27018 international cloud privacy standard. Azure safeguards customer data in the cloud and provides support for companies that are bound by extensive regulations regarding the use, transmission, and storage of customer data.

The service is scalable so that multiple instances may be spun up/down as needed to handle user demand. The service is hosted both in the US and Europe. Under normal conditions all SPI traffic is routed to US servers. However, if the US server fails; the Azure Traffic Manager settings can be manually revised to route traffic to the EU server instead.

These Security highlights are relevant to the App Gallery system:

General Azure security

- Azure Security Center

- Azure Key Vault
- Log Analytics

Storage security

- Azure Storage Service Encryption
- Azure Storage Account Keys
- Azure Storage Analytics

Database security

- Azure SQL Firewall
- Azure SQL Connection Encryption
- Azure SQL Always Encryption
- Azure SQL Transparent Data Encryption
- Azure SQL Database Auditing

Identity and access management

- Azure Role Based Access Control
- Azure Active Directory
- Azure Active Directory Domain Services
- Azure Multi-Factor Authentication

Networking

- Network Security Groups
- Azure Traffic Manager

For a full description of Azure security, please follow the link: https://docs.microsoft.com/en-us/azure/security/azure-network-security

KNO2

Kno2's Interoperability as a Service platform serves as a communications proxy, enabling access to health care providers and EHR repositories via cloud faxing, Direct secure messaging, and patient and provider search.

Kno2 supports authentication for the Share Patient Information App. Authentication employs an 'oAuth' method hosted by an Identity Provider. The Identity Provider can optionally require a two-step authorization process. Once authorization has been established, the Kno2 system provides an Access token for use in the current session. For Devices configured with SSO, Kno2 also provides a Refresh token which may be used for future sessions. The Refresh token is stored in the SSO vault, as described below.

The Kno2 application is hosted in Microsoft Azure. For scale or redundancy some resources may be deployed to multiple regions inside the US.

For more information about Kno2 security, see: https://kno2.com/wp-content/uploads/2020/03/Kno2-Security-Overview_FINAL_March2020.pdf.

XEROX® WORKPLACE SUITE/CLOUD AND SSO MANAGER

In order to improve user experience by removing the need to log in to their Identity Provider each time, Xerox offers an optional Single Sign-On (SSO) capability. Users can log into the printer and are then able to launch the app without the need to provide additional credentials.

The Single Sign-On feature integrates with the Xerox® Workplace Suite/Cloud authentication solution to store user access information for SSO-compatible Xerox Gallery Apps. After the user

enters their storage service credentials the first time, the XWS/C solution acts a storage vault where the user's Refresh Token is securely stored.

All content to be stored in the vault is encrypted with AES 256 by the SSO Manager server before being given to the SSO vault that resides on the XWS/C solution. This ensures that the SSO vault can never view or use the contents being stored in the vault. Only the SSO Manager infrastructure knows how to decrypt the content stored in the vault and only the App knows how to use it.

The SSO Manager Service manages the encryption key exchange required for secure communications and encrypts/decrypts the credential content saved in the vault.

For a full description, please review the Xerox® Workplace Suite/Cloud Information Assurance Disclosure at: https://security.business.xerox.com/en-us/products/xerox-workplace-suite/

User Data in transit

DEVICE WEBSERVICE CALLS

During standard usage of the Xerox® Share Patient Information app, calls to the device web services are used to initiate and monitor scan functions and retrieve device information using the EIP interface.

The web pages for the Xerox® Share Patient Information app are deployed in a Microsoft Azure App Service. All web pages are accessed via HTTPS from a Web Browser. All communications to and from the Xerox® App Service are over HTTPS. Data is transmitted securely and is protected by TLS security for both upload and download. The default TLS version used is 1.2.

KNO2

The Xerox® Share Patient Information app requires authentication in order to gain access to the Kno2 system. Authenticated users are allowed to scan and send or upload documents using HTTPS.

All communication is done via HTTPS and the data is transmitted securely and is protected by TLS security. The default TLS version used is 1.2. Xerox® App Gallery supplies a link to a Certificate Authority root certificate for validation with the cloud web service. It is the responsibility of the customer to install the certificate on their devices and to enable server certificate validation on the devices.

XEROX® WORKPLACE SUITE/CLOUD AND SINGLE SIGN ON

If the customer environment includes an Authentication solution (e.g., Xerox® Workplace Suite/Cloud) with Single Sign On functionality enabled, the user can agree to have their Kno2 Refresh Token securely stored and automatically applied during subsequent app launches.

All communication is via HTTPS and the data is transmitted securely and is protected by TLS security. The default TLS version used is 1.2. The credentials stored in the XWS vault are encrypted using AES 256.

3. Share Patient Information – Xerox® ConnectKey® App

Description

OVERVIEW

The Xerox® Share Patient Information ConnectKey app supports three primary workflows after a person has authenticated with their credentials:

• Share Patient Information – Users may scan patient records to be sent to recipients within the Kno2 directory. Users will be allowed to select the recipient(s) of a message based on their organization, search for or enter patient information, attach scanned documents, review and send.

• Scan to EHR – Users may scan patient records to be uploaded to an Electronic Health Records system integrated with their Kno2 system. Users will be allowed to search for or enter patient information, associate visits, orders, and reviewers, attach scanned documents (scanned files), review and upload to the EHR.

• Simple (non-PHI) Fax – Users may scan documents that do not contain patient health information and send them via the Kno2 fax feature to fax numbers within the Kno2 directory. Users will be allowed to select the recipient(s) of a fax based on their organization, attach scanned documents, review and send.

ConnectKey App

The Xerox® Share Patient Information app weblet may be installed on Xerox ® Devices from the Xerox® App Gallery. The purpose of the SPI App is to provide access to the Kno2 cloud service.

The ConnectKey App allows users, at the device, to authenticate; and share patient information with other providers, store patient information to an EHR repository, or to fax non-patient information.

Table 1. ConnectKey App user benefits

Application	What can I do?
ConnectKey App	• Share Patient Information • Scan to EHR • Fax (non-PHI) Workflow

APP HOSTING

The ConnectKey App depends heavily on cloud hosted components. A brief description of each can be found below.

ConnectKey App

The ConnectKey App consists of two key components, the weblet installed on the Xerox MFD and the cloud-hosted web service. The device weblet enables the following behavior on a Xerox ® Device:

1. Presents the user with an application UI that executes functionality in the cloud.
2. Interfaces with the EIP API to initiate scan operations at the Device.

The Share Patient Information weblet communicates with the Share Patient Information cloud-hosted web service, which executes the business logic of the app.

Xerox Extensible Interface Platform® Web Services

During standard usage of the ConnectKey App, calls to the device web services are used to initiate scan operations on the device.

COMPONENTS

MFD

The MFD is an EIP capable device capable of running ConnectKey App weblets installed from the Xerox App Gallery. In this case, the printer has the Xerox® Share Patient Information app weblet installed.

Share Patient Information – App weblet

The Xerox® Share Patient Information app weblet is installed on the MFD via the Xerox® App Gallery and must be licensed on the Kno2 system.

Share Patient Information – Web Services

The Xerox® Share Patient Information Web Service is hosted on the Microsoft Azure Cloud System. The service is responsible for hosting the web pages, which are displayed on the UI of the MFD and provide the basis for user interaction with the Xerox® Share Patient Information app. The web service interacts with the Kno2 platform using the Kno2 APIs.

Xerox® Workplace Suite/Cloud and SSO Manager

The optional Single Sign-On feature integrates with the Xerox® Workplace Suite/Cloud authentication solution to store user access information for SSO-compatible Xerox Gallery Apps. After the user enters their storage service credentials the first time, the XWS/C solution acts a storage vault where the Kno2 refresh token is securely stored.

The Xerox Workplace Suite/Cloud server accepts credential storage requests from the Share Patient Information web service via the SSO Manager Service (the SPI web service retrieves a vault key from the SSO Manager; and uses it to retrieve the Kno2 refresh token from the XWS/C service).

Kno2

The Kno2 cloud hosted platform provides a programmatic (API) interface to the Kno2 methods allowing for the creation and sending of Kno2 messages.

Electronic Health Records (EHR) Repository

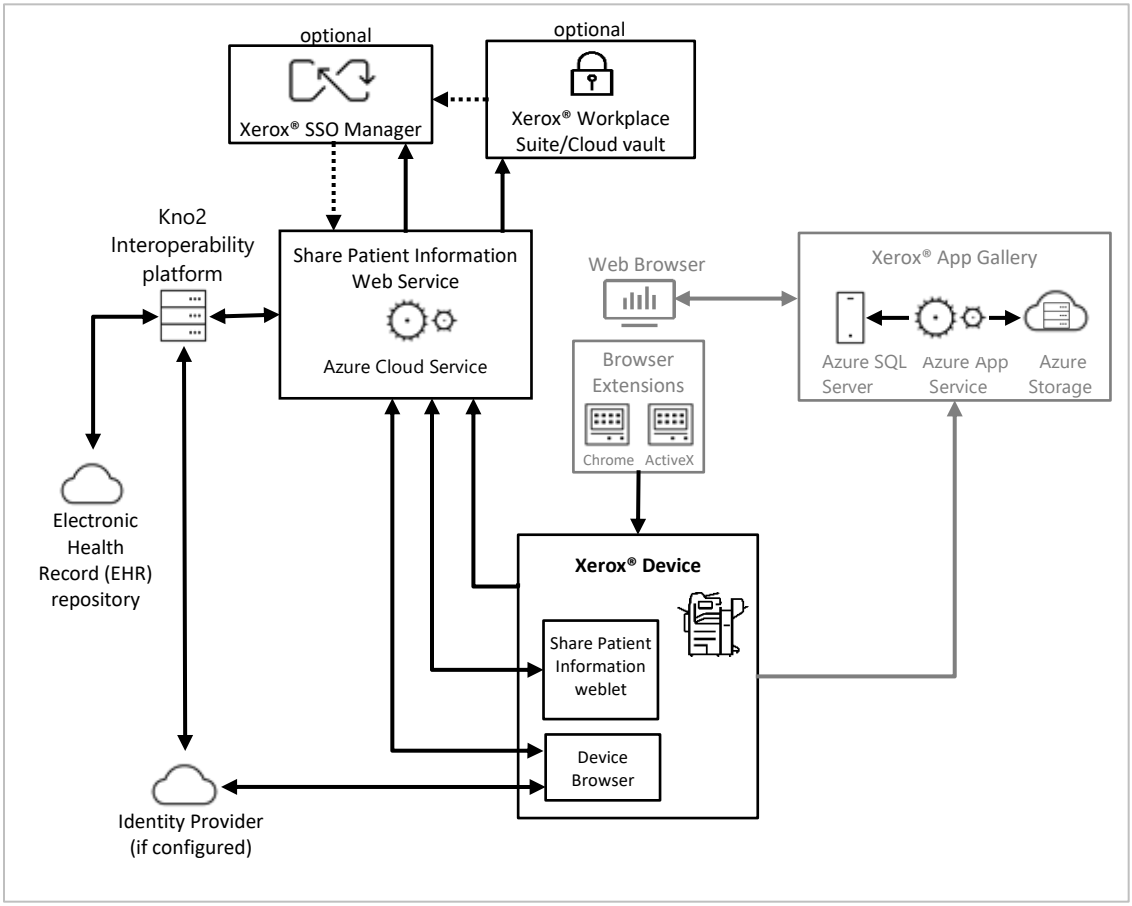
The Kno2 platform integrates with various EHR repositories. The Xerox® Share Patient Information app never communicates directly with an EHR, only indirectly through Kno2 as a proxy.

Identity Provider

Depending on customer requirements, a 3rd party Identity Provider may be configured in the Kno2 system to authenticate a Share Patient Information user. In this case, the Identity Provider will directly interact with the user via the Device browser during the authentication process. This user interaction is via redirection; and does not involve the Share Patient Information app. Kno2 itself can be configured to be the identity provider.

ARCHITECTURE AND WORKFLOWS

Architecture Diagram



Workflows – ConnectKey App

Share Patient Information Workflow

Step 1: User launches the Share Patient Information App weblet at the Device

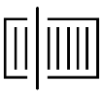
Step 2: User authenticates. (If first login, user can agree to save Refresh Token to XWS/C storage for future use. On subsequent logins, Refresh Token is automatically retrieved and applied.)

Step 3: User selects the Share Patient Information feature to create a new message.

Step 4: User selects one or more Recipients from the Kno2 recipient directory.

Step 5: User either searches for a Patient in the Kno2 patient directory or manually enters Patient demographic information.

Step 6: User modifies the scanning options (i.e., single sided, resolution, etc.).



Step 7: User selects the Scan button and the document is scanned and attached to the message. Multiple documents may be scanned and attached.

Step 8: User reviews the message parameters and selects the Send button.

Step 9: The message is sent to the Kno2 inbox of the specified Recipient(s).

Scan to EHR Workflow

Step 1: User launches the Share Patient Information App weblet at the Device

Step 2: User authenticates. (If first login, user can agree to save Kno2 Refresh Token to XWS/C storage for future use. On subsequent logins, Refresh Token is automatically retrieved and applied.)

Step 3: User selects the Scan to EHR feature to create a new message.

Step 4: User either searches for a Patient in the Kno2 patient directory or manually enters Patient demographic information.

Step 5: User selects or specifies Visit, Order, and Reviewer information associated with the document.

Step 6: User modifies the scanning options (i.e., single sided, resolution, etc.).

Step 7: User selects the Scan button and the document is scanned and attached to the message. Multiple documents may be scanned and attached.

Step 8: User reviews the message parameters and selects the Send button.

Step 9: The message is sent to the Kno2 platform.

Step 10: The metadata and attachments are uploaded to the EHR repository.

Fax (non-PHI) Workflow

Step 1: User launches the Share Patient Information App weblet at the Device

Step 2: User authenticates. (If first login, user can agree to save Kno2 Refresh Token to XWS/C storage for future use. On subsequent logins, Refresh Token is automatically retrieved and applied.)

Step 3: User selects the non-PHI Fax feature to create a new message

Step 4: User selects one or more Recipient fax numbers from the Kno2 recipient directory.

Step 5: User modifies the scanning options (i.e., single sided, resolution, etc.).

Step 6: User selects the Scan button and the document is scanned and attached to the message. Multiple documents may be scanned and attached.

Step 7: User reviews the message parameters and selects the Send button.

Step 8: The message is sent to the Kno2 platform.

Step 9: The Kno2 platform forwards the content via cloud fax to the specified Recipient fax number(s).

User Data Protection

APPLICATION DATA STORED IN THE XEROX CLOUD

User data related to the categories below are stored in cloud storage:

- Refresh Token (if SSO is enabled)
- Document Images

After image file transmission (or cancellation), all cloud-based and device-based storage of the images is deleted.

LOCAL ENVIRONMENT

Application data transmitted

Application data is protected during transmission by standard secure network protocols at the channel level. Since document content may contain Personally Identifiable Information or other sensitive content, it is the responsibility of the Kno2 user to handle the scanned documents in accordance with information protection best practices.

It is recommended that the Device Administrator enable the “verify server certificates” feature at the device to validate the networking chain of trust.

Application data stored on the Xerox ® Device

The following app data is stored on the device, in persistent storage, until the App is uninstalled from the device.

- The Share Patient Information weblet
- Recently used fax numbers at the device (not specific to a particular user)
- Saved Settings (specific to the logged in user at the device).
  The user is identified by an Kno2-provided ID which does not contain any personally identifiable information. These Saved Settings do not follow the user from device to device.
- Scratchpad data storage

All locally stored data is encrypted with AES 256.

4. Additional Information & Resources

Kno2 Security

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.

For more information about Kno2 security, see: https://kno2.com/wp-content/uploads/2020/03/Kno2-Security-Overview_FINAL_March2020.pdf.

Security @ Xerox

Xerox maintains an evergreen public web page that contains the latest security information pertaining to its products. Please see https://www.xerox.com/security.

Responses to Known Vulnerabilities

Xerox has created a document which details the Xerox Vulnerability Management and Disclosure Policy used in discovery and remediation of vulnerabilities in Xerox software and hardware. It can be downloaded from this page: https://www.xerox.com/information-security/information-security-articles-whitepapers/enus.html.

Additional Resources

Security Resource	URL
Frequently Asked Security Questions	https://www.xerox.com/en-us/information-security/frequently-asked-questions
Bulletins, Advisories, and Security Updates	https://www.xerox.com/security
Security News Archive	https://security.business.xerox.com/en-us/news/

Table 2 Additional Resources