Xerox® Share Patient Information App

Security Guide

xerox™

Xerox® Healthcare MFP Solution

Document Version: 1.0 (May 2019).

Contents

Preface

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 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).

Purpose

The purpose of the Security Guide is to disclose information for Xerox Share Patient Information 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 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 Share Patient Information App does not establish security for any network environment.

This document does not provide tutorial level information about security, connectivity or Share Patient Information App 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 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.

Description and Details

Overview

The Xerox Share Patient Information App is an accessory that can be added to some Xerox® ConnectKey® devices. The purchase of the accessory includes a Kno2 license, allowing the MFP to be enabled in the Kno2 system. When combined 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.

The Share Patient Information App supports three primary workflows after logging into the Share Patient Information App using their Kno2 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.

App Hosting

The Share Patient Information App consists of two key components, the device weblet and the cloud-hosted web service. The device weblet is a ConnectKey / EIP web app that 1) presents the device user a view of the functionality that is executed in the cloud, and 2) interfaces with the device via the EIP API to initiate device functionality such as document scanning.

The weblet communicates with the cloud-hosted web service, which executes the business logic of the app, including the selection of message recipients, association of scanned documents with patient information and sending/uploading of the scanned document files through the Kno2 system.

Kno2: Interoperability as a Service™ platform

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,

In order for the app to communicate and interact with the Kno2 system, it utilizes the authentication dialog provided by Kno2, which prompts the user for their Kno2 login credentials. The Kno2 system can optionally require a two-step authorization process.

Once authorization has been established, an OAuth login token is returned to the device from the storage service. This token is used for further interactions. The device does not store the account credentials.

Single Sign On via Xerox Workplace Suite/Cloud and SSO Manager

In order to improve user experience by removing the need to log in to the Kno2 system 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 login information 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 content saved in the vault.

For a full description, please review the Xerox Workplace Suite/Cloud Information Assurance Disclosure:

https://security.business.xerox.com/en-us/products/xerox-workplace-suite/

Device Webservice Calls

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

Security

Hosting

The Xerox Share Patient Information consists of two parts; a weblet installed on the Xerox device and the cloud-based web service with which the weblet communicates. The 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 new international cloud privacy standard, ISO 27018. 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.

Microsoft Azure Security Highlights

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, please follow the link:
https://docs.microsoft.com/en-us/azure/security/azure-network-security

Secure Web Communications

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 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.

The Share Patient Information App requires the user to provide proper/valid credentials in order to gain access to the Kno2 system. Authenticated users are allowed to scan and send or upload documents using HTTPS.

At launch, the app must get an authentication/session token from the Kno2 authentication process. The token is used for that session of the app.

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 user credentials securely stored and automatically applied during subsequent app launches.

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.

Local and Cloud Storage

No user-specific data is stored locally on the device. Recently used usernames are stored locally on the device for simplifying user login. Recently used recipient fax numbers are stored locally on the device for simplifying the non-PHI fax workflow. All locally stored data is encrypted with AES 256.

To use the Share Patient Information App, a user must log in to their Kno2 account. The app invokes the Kno2 OAUTH dialog, which requires the user to enter their existing username and password and returns an authorization token that can be used for future access.

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 user credentials securely stored and automatically applied during subsequent app launches.

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

The content 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.

Xerox Workplace Suite/Cloud and Single Sign On

The Xerox Workplace Suite/Cloud server accepts credential storage requests from the App via the SSO Manager Service (the App retrieves a vault key from the SSO Manager and uses it to retrieve login credentials from the XWS/C service). 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.

Components

Printer with Xerox® Healthcare MFP

This is an EIP capable device capable of running ConnectKey Apps from the Xerox App Gallery. In this case, the printer has the Share Patient Information App installed. Xerox Share Patient Information App is installed via the Gallery and must be licensed on the Kno2 system.

Xerox Share Patient Information Web Service

The Xerox Share Patient Information Web Service is a service hosted on the Microsoft Azure Cloud System. The service is responsible for hosting the web pages, which are displayed on the UI of the printer 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. 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. Users will be routed to the closest server geographically (based on network speed).

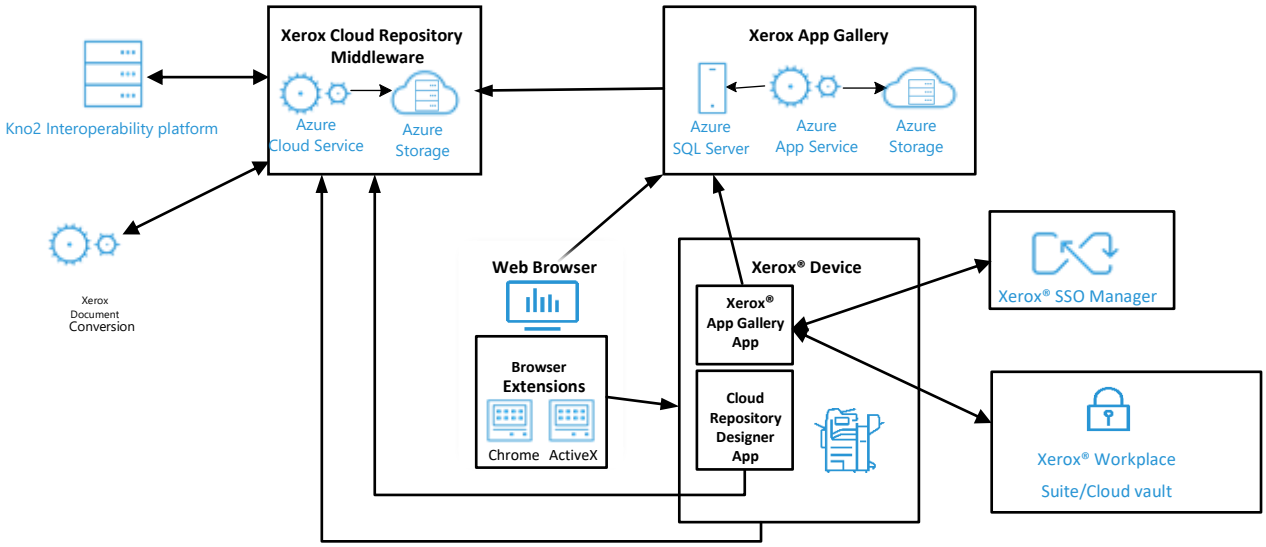
Kno2 Interoperability as a Service Platform

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 provides the integration with various EHR repositories. The Share Patient Information App never communicates directly with an EHR, only through Kno2 as a proxy.

Workflow and Data Flow Overview



Share Patient Information Workflow

Step 1: User launches the App at the Device

Step 2: User authenticates to the Kno2 system. (If first login, user can agree to save credentials to XWS/C storage for future use. On subsequent logins, credentials are 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 App at the Device

Step 2: User authenticates to the Kno2 system. (If first login, user can agree to save credentials to XWS/C storage for future use. On subsequent logins, credentials are 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 App at the Device

Step 2: User authenticates to the Kno2 system. (If first login, user can agree to save credentials to XWS/C storage for future use. On subsequent logins, credentials are 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).