IDENTITY PROOFING REQUIREMENTS

Date: October 28, 2014

IDENTITY PROOFING REQUIREMENTS

PUBLISHED BY
SURESCRIPTS®, L.L.C.
920 2ND AVENUE S.
MINNEAPOLIS, MN 55402
PHONE: 866-267-9482
FAX: 651-855-3001

2800 CRYSTAL DRIVE
ARLINGTON, VA 22202
PHONE: 866-797-3239
FAX: 703-921-2191
WWW.SURESCRIPTS.COM

Document Change Log

The table below tracks significant changes made to the document since it was last published.

Pub. Dt.	Sec #	Title	Change Description	Reason
10/28/14	First publication.			

This page intentionally left blank.

TABLE OF CONTENTS

This page intentionally left blank.

SECTION 1 OVERVIEW

DOCUMENT PURPOSE

This document presents requirements for **all prescriber participants** connecting to the Surescripts® network for e-prescribing transactions. Surescripts offers a choice of three identity (ID) proofing requirement tiers. Participants must select the tier that meets their business model. Surescripts requires adoption of these requirements to meet the National Institute of Standards and Technology (NIST) standards, as well as signed contracts.

The requirements defined in this document consist of procedural and technical steps that can be implemented to support ID Proofing to align with the NIST standards.

These requirements are in addition to those requirements that are product/service-specific and are mandated in specific Surescripts product implementation guides.

All of the requirements in the participant's chosen tier must be met in order for a participant to access the Surescripts production network.

Key Points of ID-Proofing:

- ID proofing *may not* be determined based on an organization's prior relationship with an individual.
- Entities choose the tier they will certify against, based on tier definition and business model within each e-prescribing product/service.
- Apply only to non-controlled substances. E-prescribing of Controlled Substances (EPCS) must conform to the DEA requirements.
- The tiers are characterized by the relationship between the organization's application and potential users that will be ID proofed.

OVERVIEW OF ID PROOFING TIERS

Tier 3 applies to organizations where the identity verification process is performed in-person, within the organization, by a department that is responsible for hiring and credential management.

Tier 2 applies to organizations where the identity verification process must be performed in person, by individual(s) designated by the prescriber (verified user), within the specific practice organization. This verified user may serve in a system administrator role.

Tier 1 applies to organizations where the identity verification process for new user registration is performed remotely via the system, for example, through an online web registration form, and/or where the EHR/stand-alone e-prescribing module is downloadable through the internet and/or is available for free or through a free trial.

DOCUMENT SCOPE

This document is intended to be used for e-prescribing products. These requirements are in addition to those requirements that are product/service-specific and are mandated in Surescripts product implementation guides. Vendors can choose whether to extend the requirementss to all components of the Electronic Health Record (EHR)/Electronic Medical Record (EMR).

The requirements in this document do not directly meet EPCS requirements; however, the Knowledge Based Authentication (KBA) section of this document can support the foundation for those (EPCS) requirements. Participants currently ID proofing at a certified EPCS level are following NIST level 3 two-factor authentication requirements, which supersede the requirements set forth in this document.

COMPLIANCE REQUIREMENTS

For new Surescripts participants implementing ID proofing as part of their initial network implementation, compliance is required for all prescribers added to the applicable application.

For existing Surescripts network participants, compliance is required for new prescribers added to the application after implementing ID proofing.

Surescripts highly recommends ID proofing existing prescribers during annual audits, where possible.

APPEAL PROCESS

Surescripts will review the participants' implementation of the ID proofing process against the published requirements. Surescripts will not approve any application that does not meet the ID proofing requirements as specified in this document. If a participant does not agree with the decision they can appeal it.

TERMS

Term	Definition
e-Prescribing	Includes all e-prescribing services.
Practice System Administrator	The individual, either within a practice/hospital or at the vendor level responsible for assigning access to e-prescribing functionality.
Verified User	A user who has achieved ID proofing based on one of the 3 tiers.

DOCUMENT REFERENCES

Please reference the following documents when reading these requirements.

Document Title
NIST Special Publication 800-63-2 – Electronic Authentication Guideline
Surescripts Network Operations Guide and Service Level Agreements

This page intentionally left blank.

SECTION 2 TIER 3 IDP REQUIREMENTS

All vendors and aggregators under Tier 3 must comply with the following Steps 1 and 2.

Step	Requirements	Actions
1	*Collect and confirm healthcare entity information*	**Record and validate with a 3rd party source either (a) or (b) below, as applicable.** a. For hospitals, the hospital state license number. *-or-* b. For physician group practices, i. The physician group practice NPI *-and-* ii. The physician group practice tax identification number (TIN).
2	*Assign system administrator for practice/hospital*	**Enable administrative rights to access the e-prescribing functionality.** Vendor shall ensure there is a credentialing authority, such as an IT department or an individual designated as the system administrator in accordance with the terms and conditions set forth below (e.g., employees and contractors).

Notes and conditions for Tier 3:

- Recording of information: After verification of information has been performed, the record of that information may be kept in any format so long as it can be presented in the event of an audit request.
- Remote access permitted: Applications may enable remote capabilities for authorized users of the e-prescribing functionality.
- Credential Authority: For e-prescribing functionality, a credential authority may only issue credentials to individuals within their organization.

This page intentionally left blank.

SECTION 3 TIER 2 IDP REQUIREMENTS

All vendors and aggregators under Tier 2 must comply with the following Steps 1-4.

Step	Requirements	Actions
1	*Collect and confirm physician group practice information*	**Record and validate with a 3rd party source both of the following:** a. The physician group practice NPI *-and-* b. The physician group practice tax identification number (TIN).
2	*Confirm employed physician representative*	**Record physician prescriber representative:** Physician group practice shall identify, and vendor shall record an employed physician representative to undergo the IDP process on behalf of the physician group practice.
3	*Verify employed physician prescriber and issue credentials*	a. **Physician prescriber verification:** Complete all of steps 1-3 for Tier 1 IDP Requirements for the identified employed physician representative as set forth below. b. **Credential issuance/confirmation:** The credential issuance or confirmation shall be issued to a *physician group practice location* address of record (not the physician's home address of record).
4	*Verified physician may assign system administrator for physician group practice*	**Enable system administrator rights to access the EHR/EMR:** Physician may assign the role of system administrator for the e-prescribing functionality to designated employee(s) of the physician group practice. Vendor and physician group practice should determine appropriate workflows for transitions to system administrators for the e-prescribing functionality of the EHR/EMR.

Notes and conditions for Tier 2:

- Remote Access Permitted: Applications may enable remote e-prescribing capabilities for authorized users.
- e-Prescribing Functionality System Administrators:
  - System administrators for e-prescribing functionality may only issue credentials to individuals within their organization who are:
    - physician group employees authorized to use e-prescribing functionality

    –or-
    - contractors/agents authorized to act on behalf of the physician group practice.
- Changes in System Administrator:
  - For initial implementation, the system administrator should be ID proofed at a Tier 1 requirement level.
  - System administrator role may be transferred to anyone who had previously been ID proofed by the prior system administrator.
  - Legal entity requirement: The physician group practice must be a legally formed organization and cannot be a professional association, independent practice association, or otherwise.

This page intentionally left blank.

SECTION 4 TIER 1 IDP REQUIREMENTS

All vendors and aggregators under Tier 1 must comply with Step 2 and select one of Steps 3(A-C) below. Step 1 is conditional for step 3A.

Step	Requirements	Actions
1	*Collect demographic information about each individual prescriber*	***The following data is mandatory:*** • Full name • Date of birth • Telephone number • Home address
2	*Verify prescriber is appropriately licensed*	**Record and validate Medical license number (or its equivalent).**
3(A)	*Verify individual and issue credentials electronically, with confirmation mailed to home address of record or texted to cell phone # of record*	**1. Knowledge-Based Authentication (KBA)** Successfully complete knowledge-based authentication or knowledge-based ID proofing (collectively, KBA), provided that: a. KBA is endorsed by either Kantara, SAFE BioPHARMA, or IDManagement.gov as meeting or exceeding LOA 2 (see links below); *-or-* b. Surescripts has independently reviewed the KBA product and added the product to an approved KBA product list (to be updated on a periodic basis). **Note:** If the KBA product you plan to use is not listed, contact your Surescripts Compliance representative. **2. Credential Issuance** a. Issue credentials electronically; *-and-* b. Either (i) or (ii): i. Send confirmation letter to the home address of record (e.g., credit agency; governmental agency, if permitted; Verizon; Experian; Equifax; or other non-public source). *-or-* ii. Send a message via text message to a confirmed phone number of record. Phone number must be confirmed through records search and cannot rely solely on applicant-provided unverified phone number.
3(B)	*Verify individual and issue credentials to home address of record*	**1. Credit Card Validation** Collect individual credit card number and, after a 2-3 day waiting period, either charge the credit card a pre-determined amount (can range from nominal amount to subscription or other start-up fee charge) or conduct a credit authorization hold. Pre-paid credit cards are prohibited. **2: Credential Issuance** Issue credentials to an individual home address of record (e.g., credit agency; governmental agency, if permitted; Verizon; Experian; Equifax; or other non-public source). Credentials cannot be issued to a phone number of record, an e-mail address, or otherwise provided electronically.

Step	Requirements	Actions
3(C)	*Verify individual and issue credentials electronically, with confirmation of home address of record*	**1: Financial Account Verification** Collect one (1) of the following and validate with a 3rd party, non-public source (e.g., credit agency, Verizon, Experian, or other non-public source): a. Loan numbers (e.g. student loan, mortgage, automobile loan); *-or-* b. Savings account number; *-or-* c. Public utility account number (electric, water, etc.). **2: Credential Issuance** Issue credentials electronically and send confirmation letter to the home address of record (e.g., credit agency; governmental agency, if permitted; Verizon; Experian; Equifax; or other non-public source). **Note:** Credit card or checking account verification for ID proofing is prohibited under this option.

Notes & Conditions for Tier 1:

- Prior relationships insufficient:
  - Prior relationships with users do not qualify as sufficient ID proofing.
- System administrators must complete ID Proofing of all new users before creating accounts.
- Matching names: All forms of identification/validation must contain matching individual names.
- Free use: Applications that offer free use while capturing credit card or other payment method should use 3 (B) as its form of ID proofing at a minimum.
- KBA failures: If a prescriber cannot pass the KBA as laid out in step 3(A), select one of the other methods.
- Approved third-party endorsers include:
  - Kantara (http://kantarainitiative.org/idassurance/)
  - SAFE BioPharma (http://www.safe-biopharma.org/SAFE_Trust_Framework.htm)
  - IDManagement.gov (http://www.idmanagement.gov/approved-identity-providers)
  - See also the approved KBA Vendor List available on at http://surescripts.com/idproofing Password: $ureIDP2013