Identify Proofing Requirements

July 28, 2023

IDENTIFY PROOFING REQUIREMENTS

Published by
Surescripts, LLC

WWW.SURESCRIPTS.COM

Table of Contents

Section 1: Overview

1.1 Common Terms

Term	Definition
e-prescribing	Includes all E-Prescribing services.
Practice System Administrator	The individual responsible for assigning access to e-prescribing functionality. They are either with the application vendor or within a practice or hospital.
Prescriber Participants	Health Technology Vendors, hospitals, clinics, aggregators, or other VARs who own and operate a system or application which connects to the Surescripts network for the purpose of e-prescribing.
Verified User	A user who has achieved ID proofing based on the applicable tier.
NIST Identity Resolution & Evidence Collection (Strength of Evidence)	SP 800-63A: Identity Resolution and Evidence Collection (nist.gov)

1.2 Document Purpose and Scope

This document presents requirements for all Prescriber Participants connecting to the Surescripts® network for e-prescribing transactions. Surescripts has three identity (ID) proofing requirement tiers which vary according to the Prescriber Participant's 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.

All requirements in the tier applicable to a given Prescriber Participant must be met before a Prescriber Participant can access the Surescripts production network.

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

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 business model within each e-prescribing product or service.
- ID proofing applies only to non-controlled substances. EPCS must conform to the DEA requirements.

1.3 Overview of ID Proofing Tiers

The tiers are characterized by the relationship between the organization's application and potential users that will be ID proofed.

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). Tier 1 also applies to organizations where the EHR or stand-alone e-prescribing module is downloadable through the internet, is available for free, or is available through a free trial (e.g. applies to telemedicine e-prescribing purposes).

Tier 2 applies to organizations where the identity verification process must be **performed in person** within the specific practice organization by individual(s) designated by the Prescriber Participant. This individual may serve in a system administrator role but must be a verified user who is ID proofed to Tier 1 standards. If the practice organization is a physician group practice, **it must be a legally formed organization** and cannot be a professional association, independent practice association, or otherwise.

Tier 3 applies to organizations where the identity verification process is performed in-person within the organization by a department that is directly responsible for hiring, credential management, and controls access to the application (e.g. applies to hospital or institutional organizations).

1.4 Compliance Requirements

- For new Prescriber Participants who are implementing ID proofing as part of their initial network implementation, compliance is required for all prescribers added to the applicable application.
- For existing Prescriber Participants, compliance is required for new prescribers added to the application after implementing ID proofing.
- Surescripts highly recommends ID proofing existing prescribers as part of annual audits to maintain the security of the network and participating members.
- Entities that meet Surescripts requirements for a non-EHR/EMR can reference the Exceptions section of this document for exception requirements.

1.5 Appeal Process

Surescripts will review the Prescriber participant’s 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 Prescriber participant does not agree with the decision, it can be appealed.

1.6 Document References

Please reference the following documents when reading these requirements.

Document Title
NIST Special Publication 800-63-3 – Digital Identity Guidelines
NIST Special Publication 800-63A – Enrollment and Identity Proofing
NIST Special Publication 800-63B – Authentication and Lifecycle Management
SP 800-63A: Identity Resolution and Evidence Collection (nist.gov)

Section 2: Tier 1 IDP Requirements

All Prescriber Participants under Tier 1 must comply with the following steps:

Step	Requirements	Actions
1	*Collect demographic information about each individual prescriber*	**The following data will be needed for most verification methods:** • 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	*Verify individual and issue credentials electronically*	**Successfully complete verification, ID evidence NIST IAL2 or greater** a. One piece of SUPERIOR or STRONG evidence depending on strength of original proof and validation with issuing source *-or-* b. Two pieces of STRONG evidence *-or-* c. One piece of STRONG evidence plus two pieces of FAIR evidence Notification sent to individual that identify proofing has been completed per NIST requirements (i.e., sent to verified phone number or address of record) Please refer to the NIST Special Publications for more information on evidence conformance requirements and the notional strength of evidence types.

Notes and 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 and validation must contain matching individual names.
- Approved third-party endorsers include:
    - Kantara (http://kantarainitiative.org/idassurance/)
    - DirectTrust (https://directtrust.org/)
    - IDManagement.gov (https://www.idmanagement.gov/)

Section 3: Tier 2 IDP Requirements

All Prescriber Participants under Tier 2 must comply with the following steps.

Step	Requirements	Actions
1	*Collect and confirm physician group practice information*	**Record, and validate with a third-party source, both of the following:** a. The physician group practice NPI *-and-* b. The physician group practice tax identification number (TIN) **The physician group practice must be a legally formed organization and cannot be a professional association, independent practice association, or otherwise.**
2	*Confirm employed physician representative*	**Record physician prescriber representative:** Physician group practice shall identify, and Prescriber participant shall record, an employed physician representative to undergo the IDP process on behalf of the physician group practice.
3	*Validate employed physician representative*	**Successfully complete verification, ID evidence NIST IAL2 or greater** a. One piece of SUPERIOR or STRONG evidence depending on strength of original proof and validation with issuing source *-or-* b. Two pieces of STRONG evidence *-or-* c. One piece of STRONG evidence plus two pieces of FAIR evidence Notification sent to individual that identify proofing has been completed per NIST requirements (i.e., sent to verified phone number or address of record) Please refer to the NIST Special Publications for more information on evidence conformance requirements and the notional strength of evidence types.

Step	Requirements	Actions
4	*Verified physician may assign system administrator for physician group practice*	**Enable system administrator rights to access the application:** Physician may assign the role of system administrator for the e-prescribing functionality to designated employee(s) of the physician group practice.
5	*Verify Credential Authority*	Credential Authority: For e-prescribing functionality, a credential authority may only issue credentials to individuals within their organization. ◦ If remote, the department lead or system administrator must be ID proofed to NIST 800-63A IAL2 equivalency and be able to provide evidence of such upon Surescripts request. If in person, standard legal requirements and best practices for employee verification, such as I9 Form, are currently acceptable.

Notes and conditions for Tier 2:

- Remote Access Permitted: Health Technology Vendor 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 and have provided Form I9 documentation or equivalent
    -or-
  - Contractors or agents authorized to act on behalf of the physician group practice who have ID proofed to NIST 80063A IAL2 equivalency and ability to provide evidence of such upon Surescripts request
- If in person, standard legal requirements and best practices for employee verification, such as I9 Form, are currently acceptable
- Changes in System Administrator:
  - For initial implementation, the system administrator should be ID proofed at a NIST 800-63A IAL2 equivalency
  - System administrator role may be transferred to anyone who had previously been ID proofed by the prior system administrator

Section 4: Tier 3 IDP Requirements

All Prescriber Participants under Tier 3 must comply with the following steps.

Step	Requirements	Actions
1	*Collect and confirm healthcare entity information*	**Record, and validate with a third-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 or hospital*	**Enable administrative rights to access the e-prescribing functionality.** Prescriber participant shall ensure there is a credentialing authority, such as an IT department or individual designated as the system administrator, in accordance with the terms and conditions set forth below (e.g. employees and contractors).
3	*Verify Credential Authority*	Credential Authority: For e-prescribing functionality, a credential authority may only issue credentials to individuals within their organization. ◦ If remote, the department lead or system administrator must be ID proofed to NIST 800-63A IAL2 equivalency and be able to provide evidence of such upon Surescripts request. ◦ If in person, standard legal requirements and best practices for employee verification, such as I9 Form, are currently acceptable.

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.
- 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 and have provided Form I9 documentation or equivalent.
      -or-
    - Contractors or agents authorized to act on behalf of the physician group practice who have ID proofed to NIST 80063A IAL2 equivalency and ability to provide evidence of such upon Surescripts request.
- If in person, standard legal requirements and best practices for employee verification, such as I9 Form, are currently acceptable
- Changes in System Administrator:
    - For initial implementation, the system administrator should be ID proofed at a NIST 800-63A IAL2 equivalency.
    - System administrator role may be transferred to anyone who had previously been ID proofed by the prior system administrator.

Section 5: Exceptions

Exceptions can be requested from Surescripts for entities that do not fit the roles outlined in the Requirements for a variation of ID verification and are subject to individual review and additional audit. Exceptions should be directed to IDP@surescripts.com.