Secure Methods of Documenting Positive Identification in a Pharmacy

Updated 5/20/2026

This document provides information for Ohio outpatient and institutional pharmacies on how to meet the Board's positive identification requirements. It may be applied to other terminal distributor license types who must also document certain records using positive identification.

The Ohio Board of Pharmacy (OBP) requires pharmacies to keep records in accordance with Chapter 4729. of the Ohio Administrative Code (OAC). Some records require documentation of the positive identification of the pharmacy personnel completing the task. For more information on positive identification requirements, please refer to the applicable inspection guide: www.pharmacy.ohio.gov/inspection.

Positive identification can be achieved through various routes. OBP has established minimum requirements to achieve compliance with positive identification.

To assist licensees in complying with positive identification requirements, the Board developed this frequently asked questions document that begins on the next page. If you need additional information, the most expedient way to have your questions answered will be to e-mail the Board office by visiting: www.pharmacy.ohio.gov/contact

77 S. High Street, 17th Floor
Columbus, OH 43215 U.S.A.

Phone: 614 | 466 4143
Fax: 614 | 752 4836

Frequently Asked Questions

Q1) What is positive identification?

“Positive identification" means a method of identifying a person that does not rely solely on the use of a private personal identifier such as a password. There must be a secure means of identification.

Positive identification includes security measures to ensure identification of the individual responsible for completing tasks requiring positive identification in the OAC.

IMPORTANT: ***Mandatory electronic requirements for pharmacies go into effect on January 15, 2027. For more information, visit: www.pharmacy.ohio.gov/positiveIDrequest.***

Q2) What are the primary factors to consider when implementing positive identification?

When working with your system(s), IT/informatics, and/or vendors, a pharmacy should determine when positive identification will be applied, and the method(s) to be used. Oftentimes, licensees implement a primary method and a back-up method. For more information on positive identification requirements, please refer to the applicable inspection guide: www.pharmacy.ohio.gov/inspection.

Application of positive identification can occur at any of the following points:

1. At log-in to the computer terminal/VPN/single sign-on system (SSO).
2. At log-in to the software/program.
3. At point of action of activity that requires positive identification.
4. At a later time (retrospective review/hard copy documentation that includes printing reports to be signed or signing off with electronic positive identification).
5. In real time with use of paper records (hard copy documentation).
    - This method should be limited and is often reserved for downtime procedures, compounding records, or ancillary services (e.g., immunization administration).

Methods that can be used to achieve positive identification include:

1. Electronic Positive Identification Methods
    a. Magnetic Card Reader **+** Private Personal Identifier
    b. Bar Code Reader **+** Private Personal Identifier
    c. Biometric Method
        i. Fingerprint
        ii. Facial Recognition
    d. Proximity Badge Reader **+** Private Personal Identifier
    e. Board approved system of randomly generated personal questions **+** Private Personal Identifier
2. Other effective methods that have been approved by the board
    a. Token **+** Private Personal Identifier
        i. Examples of tokens include: DUO, OKTA, and Google Authenticator
        ii. In order for a token to be utilized, it must meet Federal Information Processing Standards (FIPS-140-2), or the most recent standard.

3. Hard Copy Documentation/Non-Electronic Positive Identification Methods
    a. Manual signature (i.e., wet ink) on a hard copy record
    b. Printout of every transaction that is verified and manually signed (i.e., wet ink) within a reasonable period of time by the individual who performed the action requiring positive identification
        i. Reasonable period of time is within 30 days or as required by the licensee policies and procedures.
    c. Electronic review of transactions that is verified and electronic positive identification is applied within a reasonable period of time by the individual who performed the action requiring positive identification
        i. Reasonable period of time is within 30 days or as required by the licensee policies and procedures.

IMPORTANT: Effective January 15, 2027, hard copy documentation/non-electronic positive identification for pharmacies will only be permitted for downtime procedures, compounding records, and ancillary services. For more information, visit: www.pharmacy.ohio.gov/positiveIDrequest.

Q3) What are the permitted methods of positive identification?

The requirements outlined in this document are the minimum requirements for OBP positive identification. A licensee can be more restrictive and require additional methods (e.g., multi-factor authentication) for their systems.

When electronic record keeping is not available or cannot be maintained, positive identification can occur in real time with use of paper records with wet-ink signature/initials as a manual process (e.g., immunization administration, compounding records, downtime procedures). As a reminder, mandatory electronic requirements for pharmacies go into effect on January 15, 2027. For more information, visit: www.pharmacy.ohio.gov/positiveIDrequest.

1. Electronic Positive Identification Methods
    a. Magnetic Card Reader **+** Private Personal Identifier
    b. Bar Code Reader **+** Private Personal Identifier
        i. The bar code is to be provided by licensee. It is recommended to have the barcode associated with the personnel's employee ID or name badge. It is NOT recommended to have an employee print a barcode daily for use as electronic positive identification.
        ii. If the barcode is not provided by the licensee, it must be generated by a multi-factor authentication (MFA) method. The system must deactivate the previously generated barcode when a new barcode is generated. Reminder: Use of a barcode is not permitted for the electronic transmission of controlled substances for outpatients. Systems must be in compliance with 21 CFR 1311.
    c. Biometric Method
        i. A biometric is a measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition.
        ii. Permitted methods:
            1. Fingerprint
            2. Facial Recognition
    d. Proximity Badge Reader **+** Private Personal Identifier

e. Board approved system of randomly generated personal questions **+** Private Personal Identifier
    i. The licensee must develop a bank of 70 questions. Each user needs to answer 15 questions from the pool of 70 questions. Each question must have a unique answer.
    ii. Non-controlled drugs must be verified with one question + Private Personal Identifier
    iii. Controlled drugs must be verified with two questions + Private Personal Identifier
    iv. It is recommended questions are utilized as a back-up method and not the primary positive identification method.
        1. Reminder: Use of challenge questions is not permitted for the electronic transmission of controlled substances for outpatients. Systems must be in compliance with 21 CFR 1311.

2. Other effective methods that have been approved by the board
    a. Token **+** Private Personal Identifier
        i. Examples of tokens include: DUO, OKTA, and Google Authenticator
        ii. For a token to be used, it must meet Federal Information Processing Standards (FIPS-140-2), or recent standards.

3. Non-electronic Positive Identification Methods
    a. Manual signature (i.e., wet-ink) on a hard copy record
    b. Printout of every transaction that is verified and manually signed (i.e., wet-ink) within a reasonable period of time by the individual who performed the action requiring positive identification
        i. Reasonable period of time is within 30 days or as required by the licensee policies and procedures.
    c. Electronic review of transactions that is verified and electronic positive identification is applied within a reasonable period of time by the individual who performed the action requiring positive identification
        i. Reasonable period of time is within 30 days or as required by the licensee policies and procedures.

IMPORTANT: ***Mandatory electronic requirements for pharmacies go into effect on January 15, 2027. For more information, visit: www.pharmacy.ohio.gov/positiveIDrequest.***

Q4) How can a pharmacy ensure compliance with positive identification?

1. The pharmacy must have a system in place that can confirm the method of positive identification utilized.
    a. The licensee must review their system to determine if the electronic positive identification method(s) can be overridden by a user (i.e., user documents with no positive identification utilized). If the primary method can be overridden, the licensee must have a back-up method in place to obtain positive identification (i.e., electronic or hard copy method).
    b. The licensee must be able to detect if an override occurred or if there were downtime or technical issues.
        i. It is recommended if the back-up method is hard copy documentation due to downtime/technical issues, the system automatically generates the hard copy documentation.

2. All electronic systems must have a timeout of inactivity.
    a. A timeout of inactivity is also required when the hard copy documentation method is generated from the electronic record keeping system (e.g., end of day report, printed MAR).

3. Application of positive identification can be achieved in one of the following manners, with the minimum required electronic security measures:

    a. **At log-in to the computer terminal/VPN/single sign-on system (SSO)** that permits access to programs that document activities requiring positive identification.
        i. The system must be configured to prevent additional users from logging into programs with the use of the initial user's positive identification.

1. For example: The licensee utilizes a SSO process and applies positive identification during SSO. Only this user (User A) is able to log-in to the programs for documentation. Once User A authenticates with positive identification, User B cannot enter username/password to document in the system.
    a. The above is only allowable if the system requires re-authentication with an approved method of positive identification.

b. **At log-in to the software/program** that captures the documentation of the activity (e.g., pharmacy dispensing software, electronic medical record, program used for tracking).

c. **At point of action of activity** that requires positive identification.

d. **At a later time (retrospective review/hard copy documentation that includes printing reports to be signed)**, after electronic review of activities that require positive identification. Positive identification may be applied electronically or by wet-ink signature/initials.

   The OBP recognizes workflows sometimes require a retrospective review of documentation and application of positive identification (e.g., surgical/OR areas). This method is not preferred, and the licensee is to minimize the use of retrospective review. The licensee must develop SOPs to outline when and why the retrospective review option is required.

   This method may be used as a back-up method during down times when electronic positive identification cannot be achieved. It can include a printout of activities that is signed by the responsible individual. All time outs of inactivity outlined below are still required for a hard copy (i.e., paper) positive identification method.

4. System requirements

a. **Timeout of inactivity** refers to when the system/program "locks" and requires personnel to enter credentials (e.g., username/password) to continue working in the system/program. If positive identification is applied at log-in, the system will require the application of the positive identification. If positive identification is applied at any other point, the system must require some type of credential (e.g., password, PIN, badge scan) to continue working.
    i. This does not require complete close out of the system.

b. **Timeout of inactivity**:
    i. No more than five (5) minutes for all systems, except:
        1. Surgical/Procedural areas that utilize anesthesia medications: 60-minute timeout of inactivity
        2. Primary engineering control/Secondary engineering control compounding areas: 60-minute timeout of inactivity
    ii. Follow licensee specific policy for timeout of inactivity when positive identification is applied at point of action.

5. **Private Personal Identifier (PPI) Requirements**
    a. PPI can be a password or PIN.
    b. PPI must be updated per licensee policy.

Q5) Does the Board have recommended best practices?

The OBP recommends the following best practices to achieve positive identification:

a. The licensee has a security policy for electronic systems, and the policy is reviewed on a regular basis.
b. The licensee reviews recommendations and requirements of the Health Insurance Portability and Accountability Act.
c. The licensee has a quality assurance process to ensure positive identification methods are in place and work, including assessing overridability.
d. The licensee has a primary electronic positive identification method and an electronic back-up method when the primary fails (e.g., if the fingerprint does not work the person is provided challenge questions + personal private identifier). If a

second electronic positive identification method is not possible, a hard copy documentation method that is generated by the system is recommended.

e. The licensee should have SOPs that address logging out of the workstation at the end of the shift and when physically leaving the workstation.
f. The licensee should have an SOP regarding password/PPI recommendations. This should include frequency of updating passwords (e.g., 90 days) and repeatability (e.g., cannot use same password more than once in a calendar year).
g. If the PPI is a PIN, it is recommended:
    i. The minimum length is 4 digits.
    ii. The maximum number of repeating digits is 2 (e.g., 3774).
    iii. The maximum number of sequential digits is 3 (e.g., 1235).