



WHITEPAPER

Imprivata Identity Verification

How modern identity
proofing improves security
and streamlines access





Introduction

Imprivata provides identity verification capabilities and identity assurance across a wide range of organizational workflows. This service enables validation of a person's identity using document analysis, biometric comparison, liveness detection, and contextual evaluation. By offering this as a shared service within the Imprivata portfolio, customers gain a unified approach that reduces complexity and supports secure, efficient identity proofing across Imprivata products and customer use cases. This is particularly valuable in healthcare, where identity assurance is critical to patient safety and clinical efficiency, is a regulatory requirement for workflows such as controlled substance prescribing and patient access, and plays a key role in reducing fraud and misidentification. Imprivata is committed to customer data protection by applying technical and administrative controls designed to safeguard identity data throughout its lifecycle.

How identity verification works

Modern identity verification combines document analysis, biometric comparison, and data validation within an orchestrated decisioning workflow that strengthens privacy and security while removing unnecessary friction for authorized users. The service determines which verification checks are required based on the requesting product or workflow, ensuring each verification session applies the appropriate level of assurance, according to NIST guidelines, without requiring users to understand the underlying complexity. This approach aligns with industry best practices and widely recognized standards for digital identity assurance.



Document capture and analysis

Users capture images of a government-issued identity document using a standard camera on a desktop or mobile device. The service evaluates:

- Image quality checks for blur, glare, cropping, and legibility
- Document security feature to identify tampering or forgery
- Document structure and layout against expected formats of the issuing authority
- Key identity attributes, including name, date of birth, and document number

Where available, extracted data is validated against authoritative sources, such as motor vehicle records for U.S. drivers' licenses in participating states through the American Association of Motor Vehicle Administrators (AAMVA).

Selfie capture and liveness detection

Users capture a selfie or short video clip as part of the verification process. The service evaluates:

- Passive liveness signals to confirm the presence of a real human
- Biometric similarity between the selfie and the portrait extracted from the identity document
- Quality indicators such as lighting, occlusion, and image clarity

These signals produce similarity and quality indicators that inform the verification decision.

Supplementary documents for higher-assurance workflows

Some workflows require higher levels of identity assurance, such as those aligned with NIST Identity Assurance Level 2 (IAL2). IAL2 outlines requirements for verifying a claimed identity using validated evidence, anti-spoofing controls, and strong fraud mitigation. Many healthcare workflows, including Electronic Prescribing of Controlled Substances (EPCS), require identity proofing at an IAL2-equivalent level. This level of assurance can also help patient populations assert their identity when enrolling for care and services remotely.

When authoritative database checks are unavailable or insufficient, users may be asked to provide supplementary evidence, including:

- Bank statement
- Utility bills
- Employment records
- Other approved secondary documents used in combination with a government-issued ID



Supplementary evidence strengthens confidence in the asserted identity when primary signals alone are insufficient. Imprivata applies these requirements based on workflow risk, providing an additional layer of validation where needed without adding unnecessary steps to lower-risk workflows.

Decisioning

Verification results are evaluated against configured policy thresholds, producing one of the following outcomes:

- Approved – verification meets organization assurance requirements
- Rejected – verification fails, with clear reasoning provided



Data capture, use, and storage

Identity verification involves several categories of data.

What data is stored and how is it used

Imprivata's identity verification service processes data during verification, and stores only the structured audit information required for long-term compliance.

Once verification is completed, the service returns a structured audit record containing only the verification outcome, reason codes, and workflow metadata. This approach limits long-term data retention while preserving the information needed for auditing and compliance.

The identity verification service processes:

- Document images used for document analysis
- Selfie images used for biometric comparison and liveness detection
- Extracted identity attributes such as name, date of birth, and address
- Session and device metadata such as browser type and approximate IP address-inferred location, used to support fraud detection and risk evaluation
- Verification outputs including match scores, quality metrics, timestamps, and reference IDs

Where the data is stored

The identity verification service stores identity data within a secure cloud infrastructure. This environment is designed for regulated use cases and aligns with industry-standard security and compliance frameworks.

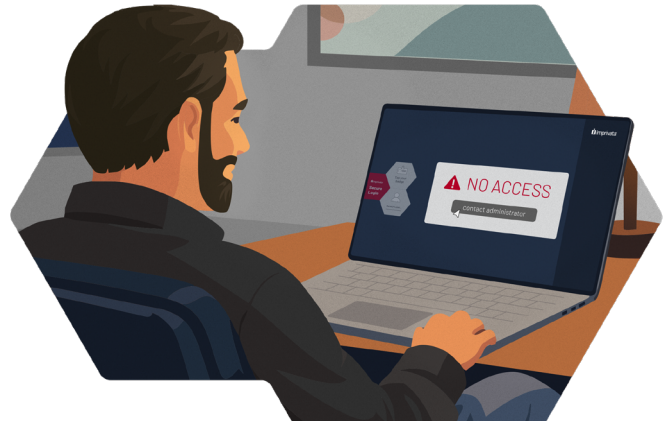
Identity data is encrypted at rest and in transit using industry-standard cryptography. Access is protected by strong authentication, role-based access controls, and comprehensive audit logging. Physical and logical safeguards provided by the underlying cloud infrastructure are designed to protect against unauthorized access.

Data privacy and security

How long identity verification data is stored

Identity verification data is retained only for the limited period required to complete verification and support short-term troubleshooting. Retention policies are applied to ensure data is not retained longer than necessary:

- Data associated with an individual verification session is deleted after a short period (e.g., 96 hours after a verification decision)
- Any remaining account-level data is deleted after a limited retention window (e.g., 30 days)



When a customer terminates use of Imprivata services, identity verification data associated with that customer is deleted as part of the deprovisioning process in accordance with Imprivata's data retention policies.

How identity verification data is secured

Imprivata applies technical and administrative controls designed to protect identity data throughout its lifecycle:

- Encryption of data in transit using TLS 1.2 or higher and at rest using strong encryption such as AES-256
- Logical tenant separation, ensuring customer data is isolated and not commingled across tenants
- Governance controls that enforce minimum-necessary access, role-based permissions, and separation of duties
- Continuous auditing and monitoring of verification activity
- Ongoing evaluation and improvement of document, biometric, and liveness protections

Imprivata is committed to customer data protection. Any third parties who may process customer data on our behalf are bound to adhere to appropriate technical and organizational measures.

Identity verification accuracy

Identity verification accuracy reflects how effectively users are verified while suspected fraudulent attempts are detected and denied. Unlike single-modality biometric authentication, identity verification incorporates multiple signals, including document authenticity checks, biometric comparison, and liveness detection.

Mitigating false positive scenarios

To reduce the risk of incorrect approvals, the identity verification service incorporates protection measures including:

- Advanced anti-spoofing techniques such as passive liveness detection to help prevent the use of printed photos, digital replays, or masks
- Document authenticity checks that evaluate holograms, fonts, layouts, and tamper indicators
- Biometric comparison safeguards that account for image quality and mismatch indicators

Together, these measures help protect against impersonation and maintain the integrity of the verification process.

Notice: Customers are responsible for making their own independent assessment of the information contained in this document. This document is provided for informational purposes only and reflects current Imprivata product direction, capabilities, and practices as of the date of publication, all of which may change without notice. It does not create commitments, warranties, or assurances from Imprivata or its affiliates, suppliers, or licensors. The rights and obligations of the parties are governed solely by applicable agreements with the customer, and this document does not amend or form part of any such agreement.



Imprivata delivers simple and secure access management solutions for healthcare and other mission-critical industries to ensure every second of crucial work is both frictionless and secure. The Imprivata platform of innovative, interoperable access management and privileged access security solutions enables organizations to fully manage and secure all enterprise and third-party identities to facilitate seamless user access, protect against internal and external security threats, and reduce total cost of ownership.

For more information, please contact us at:

Global headquarters USA
Waltham, MA
Phone: +1 877 663 7446
www.imprivata.com

European headquarters
Uxbridge, England
Phone: +44 (0) 208 744 6500
www.imprivata.com/uk

Germany
Langenfeld
Phone: +49 (0) 2173 99 385 0
www.imprivata.com/de

Australia
Melbourne
Phone: +61 3 8844 5533

Copyright © 2026 Imprivata, Inc. All rights reserved. Imprivata is a registered trademark of Imprivata, Inc. in the U.S. and other countries. All other trademarks are the property of their respective owners.