imprivata®

WHITEPAPER

# Imprivata face recognition

How face authentication improves user experience and security

Imprivata has developed a facial recognition capability to address the evolving challenges of identity assurance and secure access within healthcare and other highly regulated environments. This biometric technology is designed to provide an accurate, frictionless authentication mechanism that both strengthens security posture and reduces operational inefficiencies associated with legacy credentials. By integrating facial recognition as a shared service across the Imprivata portfolio, we enable customers to deploy a unified and interoperable biometric framework that ensures consistent user experiences, simplifies administration, and supports compliance with stringent regulatory requirements. For healthcare, it also helps to mitigate patient safety issues and claims friction caused by misidentification.

## How face recognition works:

### Face matching

Imprivata face recognition uses shapes, contours, shading, and geometries in a combined snapshot to represent a person's face. Users of this technology consent to allow their image to be captured in a photo for enrollment and authentication provided by Imprivata systems. When a user enrolls their face, the technology captures the user's image or leverages an existing photo and determines that it is a good entry (i.e., that the image quality is acceptable, and there is in fact a human face in the photo) and creates a "template" of the face in the photo. A template is essentially a collection of data points (think of these as points in space) that represent the face.

## Key benefits

- **Enhanced security**
- **Convenience and user experience**
- **A "what you are" factor for MFA supporting compliance**
- **Scalability with widely available cameras**

During authentication, an image of the user is captured. The authentication image is translated to a template and matched against the enrolled face template for the user. If the comparison finds a match, the user is authenticated.

### Liveness detection

Imprivata employs a sophisticated, fully passive liveness detection process to verify the authenticity of images used for face recognition. This process is designed to detect and prevent various spoofing attempts, such as photos, videos, or 3D masks, enabling secure and reliable identity validation.

The passive liveness technology analyzes a single image frame captured during authentication. This approach minimizes user effort and enhances the verification process's efficiency. Using advanced AI algorithms, the liveness detection process examines various factors within the image to determine if it is taken in real-time. This includes assessing face sharpness, size, illumination, position, angle, and the presence of masks.

The system provides feedback to users, guiding them to adjust their positioning or lighting if necessary. This proactive approach helps in capturing high-quality images, reducing errors, and the need for repeated attempts.

## Data capture, use, and storage

### What data Imprivata stores and how is it used

Imprivata captures, uses, and stores the following data:

- An image is captured at enrollment and used to generate a face template. Imprivata stores the enrollment image and resulting template to enable seamless upgrades without the need for re-enrollment as biometric template algorithms evolve.

- A face image is captured during authentication. A template for the image is created and compared against the face template created during enrollment. The image captured for authentication is used for authentication and then deleted.

- The template generated during enrollment is a mathematical representation of the user's face, not the actual image. The face template cannot be reverse engineered to generate an image of a person's face.

### Where the data is stored

Imprivata stores face images and templates within the Imprivata Cloud Platform (ICP) hosted on Amazon Web Services (AWS). Face images are stored in Amazon S3 buckets, and the templates are stored in Amazon RDS. Each organization is configured in its own logical tenant. Data is stored separately and cannot be accessed by other customer organizations.

### Imprivata regional support for face recognition

Imprivata maintains data in the following AWS regions to meet regional requirements:

- US-East (United States) – supports all US states

- EU-West-1 (Ireland) – supports EU and UK

## Data security

### Use of face templates for privacy and security

The stored face template is a mathematical representation of the image. The template cannot be reverse engineered to an image. The face template is specific to the biometric matching service used by Imprivata and cannot be used with any other face recognition service.

### How long face data is stored

Imprivata retains the following data:

- Images used for comparison at authentication are stored during authentication. The images are deleted after the authentication is completed.

- If a customer terminates use of Imprivata services, all stored face data is deleted as part of the deprovisioning process.

- Enrollment images and templates can be deleted at any time by an administrator.

- Depending on the Imprivata service using face recognition, users may have direct self-service access to delete or re-enroll their face. In some cases, an administrator may be required for deletion.

- If a user account in Imprivata is deleted, their enrollment image and face template are also deleted.

### How data for face recognition is secured

Data at rest (enrollment images and templates) are secured with AES-256 encryption. The encryption keys are stored by AWS. In addition, the enrollment photo is encrypted with a customer tenant-specific key, which is managed by the Imprivata Cloud Platform and stored in AWS KMS.

Data in transit between components is secured by TLS 1.2+ server authentication.

## Face recognition efficacy

Face recognition efficacy is measured using a scale of false positive vs. false negative results. A false positive result indicates that the wrong person matches a stored biometric template. A false negative result indicates that no match was found for an enrolled person during authentication. Like all biometric capabilities, face recognition can be tuned to lower false positive results at the cost of increasing the number of false negative results, and vice versa. To measure face recognition efficacy, most vendors participate in third-party assessments by the **National Institute of Standards (NIST) Face Recognition Technology (FRT) process**. Vendors often conduct additional testing beyond the requirements defined by NIST.

Imprivata face recognition technology has undergone NIST FRT testing and benchmarked against additional standards.

### Accuracy

Imprivata is committed to the performance of its technology, whether home grown or third party. In testing, Imprivata face recognition capabilities were measured against a False Match Rate (FMR) of .000001 (1 false positive in 1,000,000 comparisons). When compared to the standard NIST Visa/Border test set, the testing showed a False No Match Rate (FNMR) of .0019 (19 false negative results in 10,000 comparisons). In independent testing at the same FMR of .000001, the solution generated an FNMR of .00024 (24 false negative results in 100,000 comparisons).

### Mitigating false positive scenarios for 1:1 scenarios

It is statistically unlikely that an organization will encounter a false positive scenario during facial authentication for 1:1 matching scenarios. Because facial authentication is probabilistic (the algorithm is determining how probable it is that the user is the associated identifier), Imprivata strongly recommends using face recognition technology as a part of an orchestrated authentication event/flow. This can occur in one of two ways.

1. Part of an MFA flow – face recognition can be used in combination with other authenticators to have high identity assurance as a part of an authentication flow.

2. In combination with risk signaling and/or behavioral analytics, face recognition can be combined with risk signaling and/or user behavioral analytics to drive higher levels of identity assurance during authentication.

In either scenario, organizations must determine the optimal solution for their individual needs.

### Compliance

Face recognition is a commonly used factor for biometric authentication. Many governmental regulations, such as DEA requirements for Electronic Prescribing of Controlled Substances in the United States, allow for biometrics as part of methods for achieving appropriate security and compliance. Imprivata face recognition capabilities are developed with these regulations in mind, ensuring proper notice, consent, monitoring for harmful bias, as well as other data privacy and security safeguards that align with government regulations and industry standards alike.

## Consent

Consent to use face recognition and other biometrics may be required by law. The Imprivata face recognition solution includes the ability to provide and revoke consent, allowing customers the ability to incorporate language to meet their compliance needs.

## Bias

Historically, face recognition systems have shown demographic performance differences (bias) across different demographics.

To address bias concerns, face recognition technology is developed and tested using diverse training data. The system is continuously tested across different demographic groups to identify and address performance disparities, with neural network architectures that are specifically designed to minimize demographic bias.

The embedded face matching technology has been recognized for achieving high accuracy with minimal demographic bias in independent testing, including NIST evaluations where they've demonstrated some of the lowest differential error rates across demographic groups.

Imprivata monitors the algorithmic outputs and analyzes any trends to address issues at the forefront.

To learn more about Imprivata face authentication capabilities, **contact us**.

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