Oloid Face Vault v2.0

DEA EPCS Biometric Subsystem Certification Test Report

Prepared for:

Oloid

440 N Wolfe Rd. Sunnyvale, CA 94085

Version 1.0
9 May 2025
Report #250509-iBetaBTR-v1.0

Trace to Standards
21 CFR Part 1311.116

Test Results in this report apply to the biometrics system configuration tested. Testing of biometric systems that have been modified may or may not produce the same test results. This report shall not be reproduced, except in full.

iBeta Quality Assurance is DEA approved for Biometric System Testing.

Date of publication:
22 May 2025

This report is made public as of the above date.
*It will be maintained at **http://www.ibeta.com** for a period of 2 years from that date.*

Date of expiration:
22 May 2027

Copyright © iBeta Quality Assurance, all right reserved.
No portion of this report may be reproduced without written permission from iBeta

2675 S. Abilene Street, Suite 300, Aurora, Colorado, 80014

Version History				
Ver #	**Description of Change**	**Author**	**Approved by**	**Date**
v0.1	Certification Report for Oloid	Otto Marxhausen	Ryan Borgstrom	5/9/2025
v1.0	Final Certification Report	Otto Marxhausen	Ryan Borgstrom	5/22/2025

TABLE OF CONTENTS

1 Executive Summary

This report contains the results and conclusions of the iBeta Quality Assurance assessment that resulted in the certification of the biometric subsystem consisting of Oloid Face Vault v2.0 from Oloid. The biometric subsystem was validated and certified against the applicable requirements of 21 CFR Part 1311.116 for its inclusion as a built-in subsystem in an Electronic Prescription of Controlled Substance (EPCS) Application.

The Oloid biometric system is a facial recognition-based technology that acquires images of the face, converts the images using a proprietary algorithm, and matches those images to their reference (enrollment) templates.

The Oloid Face Vault v2.0 biometric system was validated to operate at a False Match Rate (FMR) of 0.001 or lower, accessed via the native Chrome browser on an iPad Pro 12.9” M1. The operating point corresponding with the False Match Rate described in 1311.116(b) was tested so that there was at least 95% confidence that the False Match Rate was equal to or less than the required value. To validate the False Match Rate requirement of 0.001 or lower as cited in 1311.116(b), iBeta found that the biometric system meets the requirement.

The application utilized for testing is consistent on all platforms with compatible browsers; however, iBeta only tested the Oloid Face Vault v2.0 biometric solution on a single iPad Pro 12.9” M1.

The Oloid biometric subsystem was tested to the DEA EPCS regulations with 21 CFR Part 1311.116. All other EPCS requirements are out of scope of this report.

This report is publicly available and available upon request from Oloid. This report will be maintained on the iBeta website during the period of certification from the issuance of this report 22 May 2025 through certification expiration date 22 May 2027).

1.1 *Biometric System Identification*

The Oloid Face Vault v2.0 acquisition components and cloud-based solution for matching are described in Section 4.1 Submitted Biometric Subsystem Identification and 4.2 Biometric System Test Environment. The application used for testing was accessed via the native Chrome browser on an iPad Pro 12.9” M1.

1.2 *Disclosure*

This report consists of the publicly available assessment and test results made between the independent test organization, iBeta Quality Assurance LLC and the vendor. This report is made public in accordance with DEA requirements and is located at www.ibeta.com.

Information and data not disclosed outside of the testing lab include:

- Technology Test data used to determine the FMR;
- Test Design Procedures; and
- Test Case templates and as-run Test Cases.

2 Introduction

This report was generated to document iBeta Quality Assurance’s assessment and testing of a biometric subsystem for the purpose of that subsystem’s inclusion in an Electronic Prescription of Controlled Substances (EPCS) system. This report addresses the testing of the Oloid applications to the 21 CFR 1311.116 regulations. The results were for Oloid’s Oloid Face Vault v2.0 facial biometric recognition application with the associated Oloid Face Vault v2.0 matching algorithm and cloud-based server. Subjects first performed a single enrollment, followed by 5 genuine verification transactions.

The purpose of this document is to provide an overview of the certification testing and findings. The complete list of the system names, major subsystems, version numbers and any interfacing devices is contained in Section 4 Biometric System Identification. Additional details of the design, structure, and processing capabilities are identified in the Section 5 Biometric System Overview.

Testing was conducted at the iBeta Quality Assurance facility in Aurora, Colorado.

Certification testing was performed in compliance with the requirements of 21 CFR 1311.116. All test executions and reviews included the record of requirements that were satisfactorily and unsatisfactorily completed. No deficiencies were noted during the test effort.

The requirement of 21 CFR 1311.116(b) is that the biometric subsystem operate at a False Match Rate (FMR) of 0.001 or lower. Technology testing for the FMR requirement was performed using ISO/IEC 19795-1 and ISO/IEC 19795-2 as guidance documents in the generation and execution of test cases.

iBeta Quality Assurance, a limited liability company, is located in Aurora, Colorado. The company is a full-service software testing laboratory providing Quality Assurance and Software Testing for the business and interactive entertainment communities.

2.1 *Internal Documentation*

The documents identified below are iBeta internal documents used in certification testing.

Table 2-1 Internal Documents

Version #	Title	Abbreviation	Date	Author (Org.)
01	DEA EPCS Biometric Subsystem Certification – Oloid	Contract	8 July 2024	iBeta Quality Assurance
01	iBeta Biometric NDA – Oloid	NDA		iBeta Quality Assurance
iBeta Procedures				
2.0	Biometric Deliverable Receipt Procedure		12 April 2017	iBeta Quality Assurance
7.0	Biometric Security Procedure		12 March 2024	iBeta Quality Assurance
1.0	Biometrics Configuration Management Procedure		14 May 2024	iBeta Quality Assurance
1.0	DEA-EPCS Biometric Assessment Procedure		21 May 2013	iBeta Quality Assurance
1.0	Biometric Training and Training Records Procedure		14 May 2024	iBeta Quality Assurance
iBeta Project Documents				
1.0	DEA-EPCS-Biometric-Assessment-Oloid		24 March 2025	iBeta Quality Assurance
1.0	Pre-Certification Letter		18 March 2025	iBeta Quality Assurance
1.0	DEA-EPCS-Cert-Oloid		22 May 2025	iBeta Quality Assurance

2.2 *External Documentation*

The documents identified below are external resources used in certification testing.

Table 2-2 External Documents

Version #	Title	Abbreviation	Date	Author (Org.)
2017	ISO/IEC 17025: 2017 – General requirements for the competence of testing and calibration laboratories	ISO/IEC 17025: 2017	29 November 2017	ISO/IEC

Version #	Title	Abbreviation	Date	Author (Org.)
2023	ISO/IEC 17043:2023 – International Standard: Conformity assessment – General requirements for proficiency testing	ISO/IEC 17043:2023	May 2023	ISO/IEC
2021	ISO/IEC 19795-1:2021 Information technology — Biometric performance testing and reporting — Part 1: Principles and framework	ISO 19795-1:2021 Or 19795-1	1 May 2021	ANSI ISO
2007	ISO/IEC 19795-2:2007 Information technology — Biometric performance testing and reporting — Part 2: Testing methodologies for technology and scenario evaluation	ISO 19795-2: 2007 Or 19795-2	1 February 2007 (ANSI adoption)	ANSI ISO
12 April 2025	21 CFR Part 1311.116 Additional Requirements for Biometrics	Regulations	12 April 2025	Drug Enforcement Administration (DEA) Department of Justice, Office of Diversion Control
31 Mar 2010	21 CFR Parts 1300, 1304, 1306, and 1311 Electronic Prescriptions of Controlled Substances	Interim Final Rule	Effective Date 1 June 2010	Drug Enforcement Administration (DEA) Department of Justice, Office of Diversion Control
19 Oct, 2011	Docket No. DEA-360 Clarification and Notification		19 Oct, 2011	DEA Office of Diversion Control

2.3 *Test Report Contents*

The contents of this Test Report include:

- Section 1: The Executive Summary identifies a brief summary of results and conclusions of the certification testing.
- Section 2: The Introduction identifies the scope of certification testing.
- Section 3: The Certification Test Background identifies the process for certification testing.
- Section 4: The Biometric Subsystem Identification identifies the system configuration including hardware, software, and the technical documentation.
- Section 5: The Biometric Subsystem Overview identifies the subsystem functionality capabilities.
- Section 6: The Certification Review and Test Results are the methods and results of the testing effort.
- Section 7: The Opinions and Recommendations section identifies the certification and limitations of that certification based upon the results of Section 6.

Detailed Results and Data Analysis are in Attachment 1: Detailed Technology Assessment Results.

3 Certification Test Background

As a background for this biometric subsystem certification, under 21 CFR 1300, 1304, 1306 and 1311, the DEA Office of Diversion Control specifies and regulates the operation of Electronic Prescription of Controlled Substances (EPCS) applications. The regulations require 2-factor authentication of individuals to a system that electronically prescribes controlled substances. The regulations allow for two of three factors to be used for authentication. One of those factors may include a biometric from the individual claiming an identity.

Certification testing of Oloid's Oloid Face Vault v2.0 Biometric Subsystem included Security Assessment and Operating Point to provide 0.001 False Match Rate or better.

3.1 *Terms and Definitions*

The Terms and Definitions identified below are used in this test report.

Table 3-1 Terms and Definitions

Term	Abbreviation	Definition
Authentication	Auth	The process whereby a claimant provides evidence to a system that the claimant is in fact the person claimed and not an imposter.
Biometric characteristic		A specific type of physical attribute associated with an individual that may be used to establish identity. Examples are fingerprint, iris, facial, hand geometry, vein print, vein pattern, gait, and signature.
Biometric Sample	biometric	Information obtained from a biometric sensor, either directly or after further processing
Biometric Subsystem		As viewed from the perspective of an overall prescription signing system or application, the biometric subsystem is that portion of the system used to provide the biometric authentication when a biometric is used as one of the two factors of authentication.
Biometrics Identification	BID	The anonymous 6-digit subject identification of biological characteristics
Built-In		iBeta's DEA approved process describes a 'built-in' biometric subsystem as a subsystem that is primarily enclosed by the overall EPCS system. It therefore relies on the enclosing system to satisfy most or all of the DEA regulations for EPCS.
Claimant		Person claiming to have an identity for which the biometric subsystem will validate the claim
Commercial Off-the-Shelf	COTS	Commercial Off-The-Shelf; An item that is both commercial and sold in substantial quantities in the commercial marketplace
Confidence Interval	CI	Confidence intervals consist of a range of values (interval) that act as good estimates of the unknown population parameter. In the context of this report and ISO 19795, the confidence interval is purely statistical in estimation.
Conformance Test Software	CTS	A test program utilized to provide data such as biometric data to the IUT and automatically obtain results (such as a similarity score) in response to a particular challenge.
Drug Enforcement Agency	DEA	The United States Department of Justice Drug Enforcement Agency. The Office of Diversion Control specifically handles the regulations discussed in this report.
Detection Error Trade-off	DET	A graphical plot of error rates for binary classification systems, plotting false reject rate vs. false accept rate
Distortion		A measure of the inability of an image to reproduce parallel lines when parallel lines are presented at a target.
Electronic Medical Record	EMR	Overall system which is subject to DEA-EPCS regulations and which digitally signs and transmits electronic prescriptions
Electronic Prescription of Controlled Substances	EPCS	Program allowing physicians and their agents to electronically transmit prescriptions to a dispensary such as a pharmacy.
Enrollee		Person enrolling in the EMR

Term	Abbreviation	Definition
Factor		In authentication, one of the pieces of evidence that is used to support the identity claim of the claimant.
False Match Rate	FMR	Probability that the system incorrectly matches the input pattern to a non-matching template in the database
False non-match rate	FNMR	Probability that the system fails to detect a match between the input pattern and a matching template in the database
Failure to acquire	FTA	Failure to capture and/or extract usable information from a biometric sample
Failure to enroll	FTE	Failure to create a proper template from an input for a number of specified attempts (governed by NIST SP800-76-1)
Implementation under test	IUT	That which implements the standard(s) being tested
Institutional Review Board	IRB	A committee that has been formally designated to approve, monitor, and review biomedical and behavioral research involving humans
Independent Test Lab	ITL	Lab accredited by NIST to perform certification testing of biometric systems.
Logically Shred		To overwrite data in memory or disk locations enough times to mitigate the probability that the information can be retrieved by unauthorized persons
National Voluntary Laboratory Accreditation Program	NVLAP	Part of NIST that provides third-party accreditation to testing and calibration laboratories.
New England Independent Review Board	NEIRB	An independent institutional review board, ensuring the rights and welfare of research study participants
Operating point		Biometric systems can utilize a variety of algorithms and techniques to reach a decision as to whether a challenge biometric matches a previously enrolled biometric. The sum of all of these configuration parameters including some similarity score cutoff corresponds to the operating point of the system.
Principal Investigator	PI	Person responsible for the oversight of their research and ultimately responsibility for the conduct of those to whom they delegate responsibility
Personally Identifiable Information	PII	Any personal information about an individual, maintained by an agency, including, but not limited to an individual’s name; social security number; date of birth; mother’s maiden name; biometric records; education; financial transactions; medical history; criminal or employment history; and information which can be used to distinguish or trace an individual’s identity
PDF file	PDF	File format for all releases of the Report
Resolution		Used in the context of this report, refers only to the pixel width and height of a digitized image produced by a camera.
Software Development Kit	SDK	Set of software development tools which allows for the creation of application for a software package
Spatial Frequency Response	SFR	Estimation of the spatial frequency response of an imaging device based on an image of a slanted edge and line-spread-function of that image.
System under test	SUT	The computer system of hardware and software on which the implementation under test operates
Technology Testing		Refers to the acquisition of a corpus of biometric records that are used to enroll and challenge a

Term	Abbreviation	Definition
		biometric system to determine statistics such as false-match rate and false-non-match rate
Vendor		Biometric subsystem manufacturer

3.2 *DEA-EPCS Certification*

3.2.1 Definition of Test Criteria

The test criteria determined the configuration and test cases for execution. The Oloid biometric application configurations were established in collaboration with the vendor.

The test requirements are established in the DEA Final Interim Rule specifically in 21 CFR 1311.116(b) and (h)(4) that require that the biometric subsystem operate at a point with 95% confidence that the False Match Rate is 0.001 or lower. iBeta utilized the test methods defined in ISO/IEC 19795-1 and ISO/IEC 19795-2 to acquire biometric data and used it to test the technology of the biometric subsystem to validate an operating point that met this requirement.

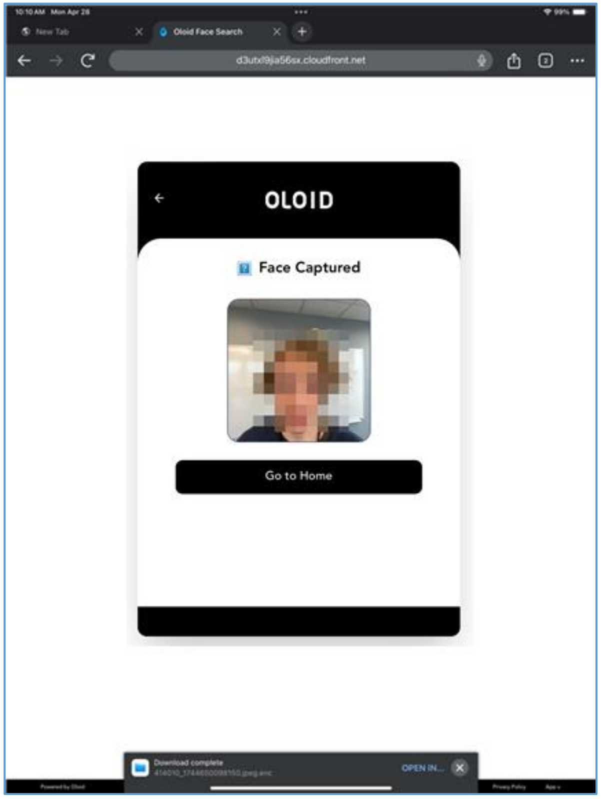
3.2.2 Test Environment Setup

For this test effort, iBeta located all equipment in the Biometrics Lab of the iBeta facility.

A test dry run was conducted prior to full data collection. On 25 February 2025, four iBeta employees provided Personally Identifiable Information (PII) and a prototype test of the data collection test case was conducted. Each subject completed an enrollment as a single image capture in normal office lighting (between 250 and 700 LUX) and performed five genuine verifications. The data analysis was conducted online without any errors.

Data acquisition was done using a single device, an Apple iPad Pro 12.9” M1.

Picture 3-1: Biometric Acquisition with the Oloid EPCS app



Subjects’ data were associated with a BID. Vendor agreed to delete all subject data within 45 days of the publication date of this report. Each subject provided their self-declared ethnicity, their birthday month and year, and gender.

3.2.3 Test Execution

Test enrollment or data collection was conducted from 27 March through 14 April 2025. Collection practices followed the same procedure as the prototype test. Acquisition of Technology Testing corpus data was acquired in an office type of environment consistent with the expected environment for prescribing practitioners: The collection environment was conducted in normal office lighting (between 250 and 700 LUX), at 16% humidity and 72° Fahrenheit.

Following the DEA Regulations 21 CFR Part 1311, 100 subjects were enrolled and included iBeta employees and non-employees as per the iBeta DEA-EPCS Biometric Test Protocol approved by the New England Independent Review Board.

Subject biographical data was recorded in a Microsoft Excel document. Only an identifier, the Biometric ID (BID), connected the subject biographical data to the acquired biometric data.

The collection device consisted of an Apple iPad Pro 12.9” M1, its factory-installed camera, and the installed Chrome browser, through which Vendor’s application was accessed.

The Oloid application provided either successful or unsuccessful enrollments and verifications for subjects for online FMR testing. As described in Section 3.2.2, subjects were presented to the Oloid mobile application and online results were immediately available to testers.

During this data collection, iBeta recorded zero Failure to Acquires (FTAs) instances, in which the application was unable to recognize the subjects. A Failure to Enroll (FTE) rate not to exceed 15% was assumed in the data collection planning. iBeta observed zero FTEs during testing, resulting in an FTE rate of 0% for the test effort.

Subsequent algorithmic testing was conducted offline. Offline results were received from Vendor’s servers via an automatically-generated CSV file that populated data after matches were attempted, then used for the assessment of the FMR and FNMR.

Oloid Face Vault v2.0 FMR testing and analysis was conducted offline that utilized a backend matching algorithm. Each challenge was reported as a true match (tm_i), true non-match (tn_i), false match (fm_i) or false non-match (fn_i). If there were then M challenges that were expected to not match, a pair of numbers can be calculated. In each case, a challenge was considered to be a transaction with one of the results above reported.

$$FMR = \frac{\sum_{i=1}^{N} fm_\text{i}}{N} \qquad (3.2.3-1)$$

Equation 3.2.3-1 is the calculated (or observed) FMR; however, the DEA EPCS regulations require a statistical 95% Confidence Interval for the operating point of the system.

A single False Match was recorded during offline testing. iBeta used bootstrapping as defined in ISO 19795-1:2021: “The bootstrap values allow a direct approach for constructing 100(1 - α) % confidence limits: choosing *L* (lower limit) and *U* (upper limit) such that only a fraction α/2 of bootstrap values are lower than *L*, and α/2 bootstrap values are higher than *U.* At least 1000 bootstrap samples should be used for 95% limits.”

3.2.3.1 *Deviations and Exclusions*

In accordance with iBeta Standard Operating Procedures, any deviations from or exclusions to the test method are documented, technically justified, authorized and accepted by the customer.

There was a single abnormality in the testing process: while iBeta attempted to enroll 100 subjects, enrollment data for only 96 subjects appeared on Vendor's servers. These four missing instances were not enumerated as Failures to Enroll, as iBeta was unable to definitively determine whether they were due to application errors or tester failure to note that the application had not completed its submission before proceeding. The enrollment data for 100 subjects did remain locally on the device and were therefore available for use during offline testing.

4 Biometrics System Identification

The Oloid Face Vault v2.0 application as specified in Table 4-1 and 4-2 were tested for this certification.

4.1 *Submitted Biometrics System Identification*

Table 4-1 contains the elements of the Oloid application.

Table 4-1 Biometrics System Name and Version

Biometric System Name	Version	Description
Oloid Face Vault	2.0	Name and version of full system, including GUI and backend server component with proprietary matching algorithm.

For the test effort, Oloid did modify the backend configuration during testing due to the testing device having communication issues with the server during enrollment and having cropping issues with the image to be used for enrollment from the sensor, but stated that this change did not impact the matching algorithm.

4.2 *Biometrics System Test Environment*

The Biometric Subsystem Test Environment identifies the specific hardware and software that was used in the test environment in Tables 4-3 and 4-4, respectively.

Table 4-2 Biometrics System Test Hardware

Hardware	Firmware, Operating System & Version	Description
Apple iPad Pro 12.9" M1	iOS: 15.5 Model Number: A2378 Serial Number: FJWMHH5P63	Device used for data collection, via installed Chrome browser

Throughout the test effort, iBeta utilized other software, hardware and materials as warranted to support the testing, analysis, and reporting.

Table 4-3 Other Software, Hardware, and Materials

Material	Material Description	Use in the Biometrics System
Multiple desktop and laptop PCs	A variety of PCs running Microsoft operating systems	Supplied by iBeta: Preparation, management and recording of test plans, test cases, reviews, and results
Vendor servers	Separate servers for storage of testing data and application of matching algorithm	Supplied by Vendor. Used to store data and provide matching results via an exported CSV file.
Microsoft Office 2010	Excel and Word software and document templates	Supplied by iBeta: The software used to create and record test plans, test cases, reviews, and results
SharePoint Online	TDP and test documentation repository	Supplied by iBeta: Vendor document and test documentation repository and configuration management tool

Material	Material Description	Use in the Biometrics System
Other standard business application software	Internet browsers, PDF viewers email	Supplied by iBeta: Industry standard tools to support testing, business, and project implementation
Traceable® Digi-Sense Light Meter	Ambient light meter S/N: 181729938	Ambient light measurements were taken prior to biometric data acquisition on a per day basis or when conditions change
AcuRite Humidity Monitor	Humidity and temperature measure Model 00309SBDI	Ambient temperature and humidity were taken prior to biometric data acquisition on a per day basis or when conditions change

4.2.1 Biometrics Test Environment – Technology Test

The technology test was performed on Vendor's servers; the last day of testing was April 24, 2025. As the technology test was performed, the results were populated into a CSV file that was available to iBeta personnel.

4.2.1.1 *Processing and Post-processing*

Online results were recorded by iBeta testing personnel. Offline results were calculated by iBeta's Subject Matter Expert from the results provided in the CSV file referenced above. Raw results were submitted to both Optimal and Non-Optimal Bootstrapping, as described in Section 3.2.3 Test Execution and Section 6.3 False Match Rate Review.

5 Biometrics System Overview

The Oloid biometric subsystem consists of the Oloid Face Vault v2.0 mobile application and its matching algorithm.

The test conducted for DEA EPCS certification consisted of a data collection application that drove the sensor for image capture. Additional functionality of the biometric subsystem was reviewed to verify additional requirements of the DEA EPCS regulations in addition to the FMR (1311.116(b)) requirement.

As tested, the enrollment and verification subsystem accessed the records through the file system. iBeta was not able to review any other functionality associated with a specific implementation of the biometric subsystem as it might interface to an EPCS certifiable system.

iBeta only reviewed the functionality of this system as it relates to the DEA EPCS regulations as it pertained to those described in this report and specifically to the 1311.116 section.

6 Certification Review and Test Results

The results and evaluations of the certification are identified below.

6.1 *Limitations*

The results and conclusions of this report are limited to the specific Implementation under Test (IUT) applications and versions described in Section 1.1 and Section 4.1.

It was the responsibility of Oloid to provide iBeta with the application and documentation for certification which are representative of those systems and devices produced for the consumer. iBeta used a device from our equipment inventory to conduct the online test effort.

These results represent usage of falsification testing methodology. Testing can only demonstrate non-conformity, i.e., if errors are found, non-conformance of the IUT shall be proven, but the absence of errors does not necessarily imply the converse. These results are intended to provide a reasonable level of confidence and practical assurance that the IUT conforms to the regulations. Use of these results will not guarantee conformity of an implementation to the regulations; that normally would require exhaustive testing, which is impractical for both technical and economic reasons.

During pre-engagement and pre-assessment analyses, iBeta determined that the Oloid biometric subsystem could be built into an EPCS system. The interface to the device is an API, however, iBeta tested the Oloid Face Vault v2.0 application through a standard Chrome browser. Much of this configuration could vary in a final EPCS implementation. The interface to the file system of enrollment records also depends on physical and logical security of the overall system.

The scope of this iBeta report and certification is solely for the Oloid biometric subsystem using images acquired using the Oloid system. The evaluation and testing certifies that the Oloid system meets the DEA biometric regulations and can be incorporated into an EPCS application which can then be certified to meet the full DEA EPCS regulations.

6.2 *DEA Biometric Subsystem Review*

6.2.1 Oloid Component Results

There was a single point of uncertainty in testing as described in section 3.2.3.1 Deviations and Exclusions, but otherwise there were neither deviations from the DEA approved test method nor any test setup that varied from the standard protocol.

False Match Rate results are given in Section 6.3.

6.2.1.1 *Exceptions*

There were no exceptions taken to the test method.

6.3 *False Reject and False Match Rate Review*

The False Reject Rate (FRR) was calculated with offline testing, using Genuine Comparisons, the number of offline matches between each subject and that subject's verification images.

Table 6-1 False Reject Rate Review

	Genuine Comparisons
Number of Comparisons	491
False Rejects	0
Rule of 3 False Reject Rate	0.611%

As no False Rejects were observed, the FRR was calculated using the Rule of 3, as defined in ISO 19795-1:2021: "The Rule of 3 addresses the question "What is the lowest error rate that can be statistically established with a given number *N* of independent identically distributed comparisons?" This value is the error rate *p* for which the probability of zero errors in *N* trials, purely by chance, is (for example) 5%. This gives:

$$p \approx 3/N \qquad (3.2.3\_ 2)$$

for a 95% confidence level."

As described in the Test Environment Setup Section 3.2.2 above, the False Match Rate (FMR) was calculated based on results from approximately 9,504 imposter comparisons of optimal bootstrapping, with 100 subjects enrolled.

Table 6-2 False Match Rate Review with Bootstrapping

	Imposter Comparisons – Optimal Bootstrap	Imposter Comparisons – Non-Optimal Bootstrap
Number of Comparisons	9504	48591
False Match	1	0
False Match Rate	0.02978%	0.00643%

“Optimal Bootstrap” in the table above is the DEA EPCS-relevant metric, which utilizes only one verification transaction per subject, for maximum independence of samples. “Non-Optimal Bootstrap” utilizes all verification transactions per subject; it is included for context and is a valid FMR to be used for marketing purposes of the system.

With a target False Match Rate of 0.10%, the Optimal Bootstrap result of 0.02978% indicates a conformance result with the DEA EPCS standard.

iBeta obtained the Age (Table 6-1), Gender (Table 6-2), Ethnicity (Table 6-3), and Facial Attributes (Table 6-4) demographics reported below.

Table 6-3 Age Demographics

Age (Years)	Count	Percentage
<18	0	0.0%
18 – 35	31	31%
36 – 52	38	38%
53 - 70	31	31%
70>	0	0.0%

Table 6-4 Gender Demographics

Gender	Count	Percentage
Male	45	45%
Female	53	53%
Non-Binary	2	2%

Table 6-5 Ethnicity Demographics

	Count	Percentage
White	55	55%
African American	20	20 %
Hispanic	11	11%
Asian	9	9%
Other	5	5%

6.3.1 Exceptions

The Oloid biometric subsystem is certified effective on the published date of this report. Per 21 CFR 1311.300(a)(2), this certification expires 2 years from that date. Also per that requirement, the assessments and testing for certification applies only to the subsystem tested and documented within this report. Any alterations to that subsystem invalidate this certification.

The data supporting these certification results are found in Attachment 1.

6.4 *Other EPCS Biometric Subsystem Requirements*

Table 6-6 Testing of Biometric Subsystem Requirements

Requirement Reference	Requirement	Details of level of iBeta Assessment	✓
1311.116(a)	If one of the factors used to authenticate to the electronic prescription application is a biometric as described in § 1311.115, it must comply with the following requirements.	The purpose of this report is to allow that the facial biometric as obtained and described herein meets the other subsystem requirements for use in a DEA EPCS system.	☑

Requirement Reference	Requirement	Details of level of iBeta Assessment	✓
1311.116(b)	The biometric subsystem must operate at a false match rate of 0.001 or lower.	As described in section 6.3, the application and device meet this requirement.	☑
1311.116(c)	The biometric subsystem must use matching software that has demonstrated performance at the operating point corresponding with the false match rate described in paragraph (b) of this section, or a lower false match rate. Testing to demonstrate performance must be conducted by the National Institute of Standards and Technology or another DEA-approved government or nongovernment laboratory. Such testing must comply with the requirements of paragraph (h) of this section.	The purpose of this report is to validate the threshold required to produce a FMR or 0.001 or lower. iBeta is a DEA-approved nongovernment laboratory. The system certifying agency must verify that the algorithm operates at the threshold defined above.	☑
1311.116(d)	The biometric subsystem must conform to Personal Identity Verification authentication biometric acquisition specifications, pursuant to NIST SP 800–76–1 as incorporated by reference in § 1311.08, if they exist for the biometric modality of choice.	Not Applicable	☑
1311.116(e)	The biometric subsystem must either be co-located with a computer or PDA that the practitioner uses to issue electronic prescriptions for controlled substances, where the computer or PDA is located in a known, controlled location, or be built directly into the practitioner's computer or PDA that he uses to issue electronic prescriptions for controlled substances.	The biometric device (browser-capable smartphone or tablet) is expected to be co-located with the practitioner's smartphone.	□
1311.116(f)	The biometric subsystem must store device ID data at enrollment (i.e., biometric registration) with the biometric data and verify the device ID at the time of authentication to the electronic prescription application.	Oloid was able to show that the subsystem is storing the device ID data during enrollment and verifying the device ID at authentication; however, this requirement will need to be fully tested in the overall EPCS system.	☑
1311.116(g)	The biometric subsystem must protect the biometric data (raw data or templates), match results, and/or non-match results when authentication is not local. If sent over an open network, biometric data (raw data or templates), match results, and/or non-match results must be: (1) Cryptographically source authenticated; (2) Combined with a random challenge, a nonce, or a time stamp to prevent replay; (3) Cryptographically protected for integrity and confidentiality; and (4) Sent only to authorized systems.	The scanned copy of the data (facial image) is stored on the mobile device. The data is transmitted to Oloid's servers in an encrypted form. Full examination of the encryption is outside the scope of iBeta's certification and must be tested by the entity certifying or auditing the overall EPCS system.	☑

Requirement Reference	Requirement	Details of level of iBeta Assessment	✓
311.116(h)	Testing of the biometric subsystem must have the following characteristics: (1) The test is conducted by a laboratory that does not have an interest in the outcome (positive or negative) of performance of a submission or biometric. (2) Test data are sequestered. (3) Algorithms are provided to the testing laboratory (as opposed to scores or other information). (4) The operating point(s) corresponding with the false match rate described in paragraph (b) of this section, or a lower false match rate, is tested so that there is at least 95% confidence that the false match and non-match rates are equal to or less than the observed value. (5) Results of the testing are made publicly available.	(1) iBeta is independent of Oloid and does not have an interest in the outcome of the performance of this testing. (2) Test data were destroyed at the conclusion of testing and during testing, test data were transmitted to vendor's servers only in encrypted form. (3) The Oloid Face Vault v2.0 application was connected to a cloud-based service where the matching algorithm was hosted with iBeta having programs to perform comparisons and obtain results. (4) Oloid set an operating point of a 90% match score or more on their system in order to be considered a match. iBeta's process and procedures to test the FMR at 95% confidence have been approved by the DEA. (5) This report is available at https://www.ibeta.com/dea-epcs-biometrics-certification-test-reports/	☑

6.4.1.1 *Exceptions*

The 21 CFR 1311.116(g) requirements were tested through partial document review, as iBeta only had access to the matching algorithm and no means to connect that algorithm to a system that might operate like an EPCS-approvable system. iBeta was able to see that the system was able to store and transmit images in an encrypted form, through saving the encrypted images from the system and then being given a program from Oloid to unencrypt the images to verify them after the testing was completed. The remainder of the requirements was evaluated from Oloid documentation. iBeta verified that the Oloid Face Vault v2.0 could be incorporated into an enclosing or encompassing Electronic Health Record application that would then meet the requirements. Full examination of the encryption was not within the scope of iBeta's certification and must be tested by the entity certifying or auditing the overall EPCS system

7 Opinions and Recommendations

7.1 *Recommendations*

iBeta Quality Assurance has completed the testing of the Oloid Face Vault v2.0 biometric subsystem. In our opinion the acceptance requirements of 21 CFR Parts 1311.116 have been met as delineated in Table 7-1 and its Notes.

iBeta Quality Assurance certifies the Oloid Face Vault v2.0 application to the requirements of 21 CFR Parts 1311.116(b) and 1311.116(h)(4). Other requirements assessed are also included below in Table 7-1.

The following table (Table 7-1) contains the 21 CFR 1311 requirements that were found to be in compliance with the regulation. Requirements checked (☑) were found to be in compliance. Requirements not checked (☐) were not within the scope of iBeta's certification and must be tested by the entity certifying or auditing the overall EPCS system as described in the Notes. However, in all cases, iBeta believes this system can be incorporated into an EPCS certified system to meet all requirements for that system.

Table 7-1 Requirement in Compliance

Requirement	Description	Approved
1311.116(a)	If one of the factors used to authenticate to the electronic prescription application is a biometric as described in §1311.115, it must comply with the following requirements.	
1311.116(b)	Biometric subsystem must operate at a false match rate of 0.001 or lower	☑
1311.116(c)	The biometric subsystem must use matching software that has demonstrated performance at the operating point corresponding with the false match rate described in paragraph (b) of this section, or a lower false match rate. Testing to demonstrate performance must be conducted by the National Institute of Standards and Technology or another DEA-approved government or nongovernment laboratory. Such testing must comply with the requirements of paragraph (h) of this section.	☑
1311.116(d)	The biometric subsystem must conform to Personal Identity Verification authentication biometric acquisition specifications, pursuant to NIST SP 800–76–1 as incorporated by reference in § 1311.08, if they exist for the biometric modality of choice. *This standard does not apply to the system under test.	☑
1311.116(e)	The biometric subsystem must either be co-located with a computer or PDA that the practitioner uses to issue electronic prescriptions for controlled substances, where the computer or PDA is located in a known, controlled location, or be built directly into the practitioner's computer or PDA that he uses to issue electronic prescriptions for controlled substances.	□
1311.116(f)	The biometric subsystem must store device ID data at enrollment (i.e. biometric registration) with the biometric data and verify the device ID at the time of authentication to the electronic prescription application.	☑

1311.116(g)(1)
1311.116(g)(2)
1311.116(g)(3)
1311.116(g)(4)
	The biometric subsystem must protect the biometric data (raw data or templates), match results, and/or non-match results when authentication is not local. If sent over an open network, biometric data (raw data or templates), match results, and/or non-match results must be:
	Cryptographically source authenticated, combined with a random challenge, a nonce, or a time stamp to prevent replay, cryptographically protected for integrity and confidentiality; and sent only to authorized systems.
		☑

1311.116(h)(1)	The test is conducted by a laboratory that does not have an interest in the outcome (positive or negative) of performance of a submission or biometric.	☑
1311.116(h)(2)	Test data are sequestered.	☑
1311.116(h)(3)	Algorithms are provided to the testing laboratory (as opposed to scores or other information).	☑
1311.116(h)(4)	The operating point(s) corresponding with the false match rate described in paragraph (b) of this section, or a lower false match rate, is tested so that there is at least 95% confidence that the false match and non-match rates are equal to or less than the observed value.	☑

All other 21 CFR 1311 requirements that may be applicable to an installed biometrics subsystem were outside of the scope of testing of this subsystem in the absence of its containing system. All other requirements must be tested for the overall enclosing system.

Notes on the 1311.116 requirements:

(a) 1311.116(a) is a rollup requirement mandating the other requirements for biometrics subsystem

(e) The tested biometric subsystem has the capability to meet this requirement but it must be tested for the overall system. See Table 6-1 for details.
(f) The tested biometric subsystem has the capability to meet this requirement, but it must be implemented and tested for the overall system. See Table 6- for details.
(g) The tested biometric subsystem has the capability to meet this requirement especially when operated locally. See Table 6-1 for details.

7.1.1 Limitations

As described in Section 6.1 Limitations, iBeta has tested what it believes to be a representative sample of the commercially available system and used the appropriate test methods to test conformance to the regulations. Device or system behavior which falls outside of the scope of this testing is not certified. iBeta cannot extrapolate the results of the testing to include devices other than those listed in Table 1-1.

Because the biometric subsystem does not sign or receive electronic prescriptions, it was found to not be subject to other requirements of the 21 IFR Part 1311 such as auditing and records maintenance. These are the responsibility of the overall system since the biometric subsystem only returns a successful/unsuccessful response to one of the two factors used for authentication prior to signing a prescription.

As shown in Table 6.2, the FMR requirement of 0.001 at a 95% Confidence Interval is met with an Operating Point of 90% Match Score.

One of the purposes of this report is to evaluate the threshold or operating point at which the biometric authentication method meets the 0.1% FMR mandated by the DEA EPCS regulations. The regulations specify the use of 95% confidence interval applied to the observed measurements. There may be other sources of measurement error over which iBeta had no control. Most likely, these sources would affect FNMR to a greater extent than FMR.

7.1.2 Exceptions

There were no exceptions other than those listed in Section 6.3.1.

7.2 *Opinions*

The vendor-supplied documentation was acceptable for iBeta to produce a software test suite built upon the vendor's application.

The Oloid Face Vault v2.0 system operated as expected.

7.3 *Responsible Test Laboratory Personnel*

The responsible test laboratory person and the contact information for the New England IRB appointed Principal Investigator for this test effort:

Ryan Borgstrom
iBeta Quality Assurance Director of Biometrics
(Responsible test lab contact)
RBorgstrom@ibeta.com
303.627.1110 extension 182

David Yambay
iBeta Quality Assurance Director of Biometrics
(IRB-appointed Principal Investigator)
DYambay@ibeta.com