



## EyeVerify Eyeprint ID™

# DEA EPCS Biometric Subsystem Certification Test Report

Prepared for:  
Wells Fargo Bank, N.A.  
420 Montgomery Street  
San Francisco, CA 94101

Version 2.0  
22 May 2015  
Report #150522-iBetaBTR-v2.0

**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:**  
May – 22 – 2015

*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:**  
May – 22 – 2017

*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
V1.0	Initial Draft Certification Report for EyeVerify® and Well Fargo configuration review	Gail Audette	Kevin Wilson	15 May 2015
V2.0	Final Certification Report for EyePrint ID™ Biometric Subsystem	Gail Audette	Kevin Wilson	22 May 2015

## TABLE OF CONTENTS

<b>1</b>	<b>EXECUTIVE SUMMARY</b> .....	<b>4</b>
1.1	BIOMETRIC SUBSYSTEM IDENTIFICATION .....	4
1.2	DISCLOSURE.....	4
<b>2</b>	<b>INTRODUCTION</b> .....	<b>5</b>
2.1	INTERNAL DOCUMENTATION.....	5
	Table 2-1 Internal Document .....	5
2.2	EXTERNAL DOCUMENTATION.....	6
	Table 2-2 External Documents .....	6
2.3	TECHNICAL DOCUMENTS .....	7
2.4	TEST REPORT CONTENTS.....	7
<b>3</b>	<b>CERTIFICATION TEST BACKGROUND</b> .....	<b>8</b>
3.1	TERMS AND DEFINITIONS .....	8
	Table 3-1 Terms and Definitions.....	8
3.2	DEA-EPCS CERTIFICATION .....	10
3.2.1	<i>Definition of Test Criteria</i> .....	10
3.2.2	<i>Test Environment Setup</i> .....	10
	Picture 3-2: Biometric Acquisition Application.....	11
	Picture 3-3: Biometric Acquisition with EyeVerify App on HTC One M9 sensor .....	11
	Table 3-2 Claimed versus Measured Error Rates.....	13
3.2.3	<i>Test Execution</i> .....	13
<b>4</b>	<b>BIOMETRICS SYSTEM IDENTIFICATION</b> .....	<b>15</b>
4.1	SUBMITTED BIOMETRICS SYSTEM IDENTIFICATION .....	15
	Table 4-1 Biometrics System Name and Version .....	15
	Table 4-2 Biometrics System Components .....	15
4.2	BIOMETRICS SYSTEM TEST ENVIRONMENT .....	15
	Table 4-3 Biometrics System Test Hardware .....	16
	Table 4-4 Biometrics System Test Software.....	16
	Table 4-5 Biometrics System Technical Documents .....	16
	Table 4-6 Other Software, Hardware and Materials .....	16
	Table 4-7 Mobile Device camera characteristics (front facing camera) .....	17
4.2.1	<i>Biometrics Test Environment – Technology Test</i> .....	17
<b>5</b>	<b>BIOMETRICS SYSTEM OVERVIEW</b> .....	<b>18</b>
<b>6</b>	<b>CERTIFICATION REVIEW AND TEST RESULTS</b> .....	<b>19</b>
6.1	LIMITATIONS.....	19
6.2	DEA BIOMETRIC SUBSYSTEM REVIEW .....	19
6.2.1	<i>EyeVerify Component Results</i> .....	19
6.3	FALSE MATCH RATE REVIEW .....	19
	Table 6-1 Age Demographics .....	20
	Table 6-2 Gender Demographics .....	20
	Table 6-3 Thresholds to meet 95% Confidence Interval of 0.001 FMR .....	20
	Table 6-4 Thresholds for the case with and without eyeglasses. ....	21
6.3.1	<i>Exceptions</i> .....	21
6.4	OTHER EPCS BIOMETRIC SUBSYSTEM REQUIREMENTS.....	21
	Table 6-5 Testing of Biometric Subsystem Requirements.....	21
<b>7</b>	<b>OPINIONS AND RECOMMENDATIONS</b> .....	<b>24</b>
7.1	RECOMMENDATIONS.....	24
	Table 7-1 Requirement in Compliance .....	24
7.1.1	<i>Limitations</i> .....	25
7.1.2	<i>Exceptions</i> .....	25
7.2	OPINIONS.....	25
7.3	RESPONSIBLE TEST LABORATORY PERSONNEL .....	26

# 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 Eyeprint ID™ from EyeVerify. 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 EyePrint ID™ biometric subsystem was validated to operate at a False Match Rate (FMR) of 0.001 or lower on three smartphone installations. 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.

The EyeVerify biometric subsystem is an Eyeprint (conjunctival, episcleral, and periocular) recognition system. iBeta tested and certified the built-in matching algorithm.

The EyeVerify biometric subsystem was tested on an iPhone 6, Samsung Galaxy S5, and HTC M9 One. Other devices are not subject to this certification.

The EyeVerify Eyeprint ID™ 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 Attachment 1 is available upon request from Wells Fargo. This report will be maintained on the iBeta website during the period of certification from the issuance of this report (22 May 2015) through the certification expiration date (22 May 2017).

## 1.1 *Biometric Subsystem Identification*

The EyeVerify Eyeprint ID™ core acquisition components are described in Section 4.1 Submitted Biometric Subsystem Identification and 4.2 Biometric Subsystem Test Environment. Two applications were provided by EyeVerify – an iOS version for the iPhone and an Android version for the HTC and Samsung smartphones.

## 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](http://www.ibeta.com).

Additional results are proprietary and not made public but disclosed to the vendor:

- Attachment 1: Detailed Technology Assessment Results

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 subsystems' inclusion in an Electronic Prescription of Controlled Substances (EPCS) system. This report addresses the testing of the EyeVerify Eyeprint ID™ application to the 21 CFR 1311.116 regulations. The results were generalized by running the FMR tests on both Apple and Android operating systems.

The EyeVerify applications were used to acquire the dataset used to evaluate the FMR results. The purpose of this document is to provide an overview of the certification testing and findings. The complete list of the systems 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 Copernicus Group Independent Review Board (CGIRB) reviewed iBeta DEA-EPCS Biometric Test Protocol application and granted unconditional approval on 22 September 2014 (approval: IBE1-114-437) for the following):

- Test Protocol Version 2.0 dated 12 September 2014
- Biometrics Security Procedures (Version 3.0) dated 5/20/13
- DEA-EPCS Biometric Subsystem Assessment Procedure (Version 4.0) dated 21 May 2013
- Biometrics Testing Disclaimer (Version 1.0)
- Brochure - 'Biometrics Testing Lab'
- Informed Consent Form (Form A)

The certification test effort was conducted in full compliance with the IRB approved study protocol.

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 Document**

Version #	Title	Abbreviation	Date	Author (Org.)
	Mutual Confidential Disclosure Agreement	NDA	April 24, 2014	iBeta Quality Assurance
01	EPCS Pre-Certification Testing Services Contract		April 24, 2014	iBeta Quality Assurance
	Mutual Non-Disclosure Agreement Doc ID 178826		December 3, 2014	Wells Fargo
	Limited Services Agreement ID 179873	MSA	2/6/15	Wells Fargo
SOW ID 179874	Wells Fargo EPCS Certification of the EyeVerify	SOW	2/6/15	Wells Fargo

Version #	Title	Abbreviation	Date	Author (Org.)
	EyePrint Verification software Statement of Work			
	Wells Fargo			
<b>iBeta Procedures</b>				
1.0	Biometric Deliverable Receipt Procedure		6/1/11	iBeta Quality Assurance
3.0	Biometric Security Procedure		5/20/13	iBeta Quality Assurance
1.0	Biometrics Configuration Management Procedure		6/9/11	iBeta Quality Assurance
4.0	DEA-EPCS Biometric Assessment Procedure		21 May 2013	iBeta Quality Assurance
1.0	Biometric Training and Training Records Procedure		6/1/11	iBeta Quality Assurance
<b>iBeta Project Documents</b>				
1.0	DEA-EPCS-Biometric-Assessment-EyeVerify		5/4/2015	iBeta Quality Assurance
1.0	EyeVerify DEA EPCS Pre-Certification Letter		4/10/15	iBeta Quality Assurance
1.0	DEA-EPCS-TestCases-EyeVerify		5/8/2015	iBeta Quality Assurance

## 2.2 External Documentation

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

**Table 2-2 External Documents**

Version #	Title	Abbreviation	Date	Author (Org.)
2005	ISO/IEC 17025: 2005 – General requirements for the competence of testing and calibration laboratories	ISO/IEC 17025: 2005	2005-05-15	ISO/IEC
2010	ISO/IEC 17043:2010 – International Standard: Conformity assessment – General requirements for proficiency testing	ISO/IEC 17043:2010	2010-02-01	ISO/IEC
2006	ISO/IEC 19795-1:2006 Information technology — Biometric performance testing and reporting — Part 1: Principles and framework	ISO 19795-1 Or 19795-1	Aug 17, 2007 (ANSI adoption)	ANSI ISO
2006	ISO/IEC 19795-2:2006 Information technology — Biometric performance testing and reporting — Part 2: Testing methodologies for technology and scenario evaluation	ISO 19795-2 Or 19795-2	Feb 01, 2007 (ANSI adoption)	ANSI ISO
1	Evaluation of measurement data — Guide to the expression of uncertainty in measurement	JCGM:100	September, 2008	JCGM (Joint Committee for Guides in Metrology)
31 Mar 2010	21 CFR Part 1311.116 Additional Requirements for Biometrics	Regulations	31 Mar 2010	Drug Enforcement Administration (DEA) Department of Justice, Office of Diversion Control

Version #	Title	Abbreviation	Date	Author (Org.)
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
1472G	MIL-STD-1472G Department of Defense Design Criteria Standard Human Engineering		11 January 2012	Department of Defense

## 2.3 Technical Documents

The Technical Documents submitted by HT Systems for this certification test effort are listed in Section 4 – Biometric Subsystem Identification.

## 2.4 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 5.

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 the EyeVerify Eyeprint ID™ Biometric Subsystem included Security Assessment and Operating Point to provide 0.001 false match rate or better. Frequency status reports were sent to EyeVerify and Wells Fargo certification management staff and iBeta project test staff. These reports included project activity status, issues, and other relevant information

#### 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 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 Image Discrimination	BID	The statistical analysis of biological characteristics
Biometric ID	BID	The six-digit code that is assigned to each test subject (crew) which identifies their reference and probe records, and anonymizes them from other personally identifiable information acquired during the test campaign.
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
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.
Copernicus Group Independent Review Board	CGIRB Copernicus Group IRB	An independent institutional review board, ensuring the rights and welfare of research study participants

Term	Abbreviation	Definition
Drug Enforcement Agency	DEA	The United States Department of Justice Drug Enforcement Agency. The Office of Diversion Control specifically handles the <a href="#">regulations</a> discussed in this report.
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
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 Match Count	FM	The actual number of false matches observed.
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
False non-match count	FNM	The actual number of false non-matches observed.
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)
Front-facing camera		The camera or associated lens that faces the same direction as the mobile device screen. Also known as the selfie camera.
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.
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

Term	Abbreviation	Definition
PDF file	PDF	File format for all releases of the Report
Software Development Kit	SDK	Set of software development tools which allows for the creation of application for a software package
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 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 EyeVerify Eyeprint ID™ 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.

As necessary to test the system, iBeta generated a semi-automated Conformance Test Software (CTS) to enroll and challenge the biometric subsystem with biometric data and record the results.

### 3.2.2 Test Environment Setup

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

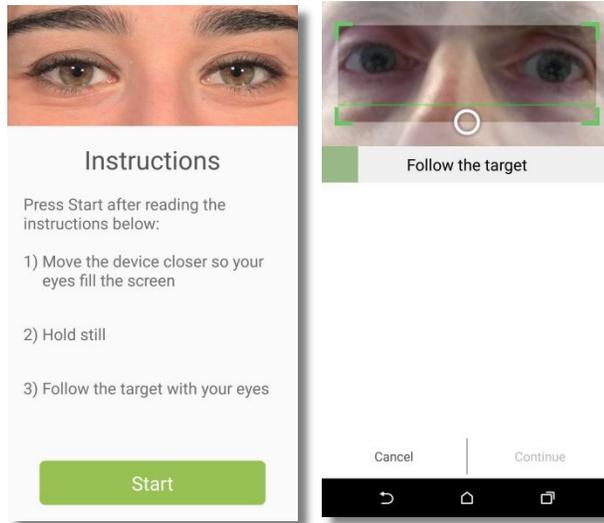
Subjects' data collection was only associated with anonymous Biometric Identification (BID) 6 digit number. Each subject provided their self-declared ethnicity, their birthday month and year, and gender. Data was also collected as to whether the subjects was wearing contacts. The iBeta Security Procedure was utilized to maintain biographical data separately from biometric data and access to both was restricted to appropriate personnel. Collection of biographical data is used only to prevent the inclusion of duplicate crew members.

In addition, all data collection was conducted in normal office (clinical and hospital) lighting environment and the illumination was recorded each day and verified to be within the Mil-Std 1472G office environment (per Table XXII stating the specific task illumination requirements for general office work to be illuminations a the preferred level of 755 lux with a minimum level of 540 lux).

During data collection, all of the smartphones were run either off of the internal battery or while charging. No smartphone was allowed to drop below a 50% battery level.

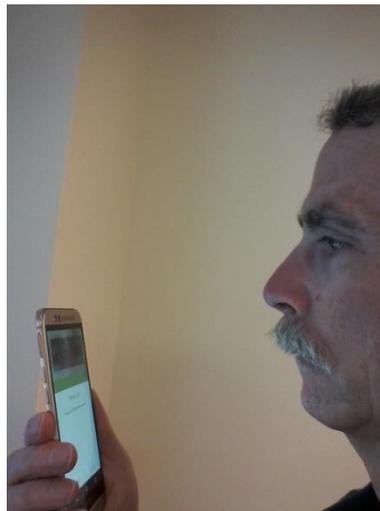
This test tool version was validated on 15-16 April 2015 by acquiring ten sets of data and verifying the data collection. The as-run technology test aggregate data and source code have been archived on a secure repository server.

A screen shot of the EyeVerify enroll and verify app (from the Samsung device) is provided below in Picture 3-2.



**Picture 3-2: Biometric Acquisition Application**

The Technology Test was implemented using EyeVerify provided demo apps which stored a reference (enrollments) and probe (verifications) image in a specified set of folders. EyeVerify also provided the software to perform the matching challenges. iBeta utilized one of the two applications (one Android, one iOS) in the devices specified in Table 4-2. The test environment for PII collection with the EyeVerify mobile device sensors is provided below in Picture 3-3.



**Picture 3-3: Biometric Acquisition with EyeVerify App on HTC One M9 sensor**

Data was collected on three devices as described in Section 4, two Android based, and one iOS based.

An encrypted database was created using TrueCrypt as listed in Table 4-7. The database of biometric data samples consisted of a series of enrollment or reference images, and two series of verification or probe images. Due to the possibility of overrunning storage, these images were offloaded from the devices periodically, especially during the first days of testing when iBeta was unsure of the amount of storage space required and the possibility that the devices would slow down after large numbers of images had been taken. In general, a typical reference consisted of sixteen (16) images, and a typical probe of six (6) images.

Glasses are a known modality-specific factor that might affect performance. For crew members who appeared or reported that they wore glasses, iBeta collected their biometric first with glasses (and recorded that collection by using their assigned BID but substituting the last digit with a '3'). iBeta then collected their biometric with their assigned BID and no glasses. No subjects indicated that they could not collect data without their glasses.

During post-processing, iBeta verified that all BIDs associated with a BID ending in 3 (i.e. only the last digit was changed to 3) wore glasses during their first data collection.

During the first day of testing, verifications (probes) were not collected for 55 individuals. iBeta has not determined whether this was tester error or a problem with the acquisition applications. Consequently, from that point forward, two probe sets of images were collected to supply the appropriate number of about 100 expected matches. These additional probes were not used during the testing of expected non-matches which leads to the FMR value.

EyeVerify supplied the matching algorithm application. The application ran on Linux. iBeta used an Oracle Virtual Machine (VM), Virtual Box, that had Ubuntu 14.10 64-bit version installed. The inputs to the application were 1) the main folder which contained the consolidated enrollments and verifications, and 2) the name of the output file which was produced in comma-separated value (CSV) format. The output consisted of

eBID, vBID, SN, EM, Score

where eBID is the reference, vBID is the probe, SN is the sequence number of the probe, expected match (EM) is the algorithm expectation of a match, and the Score is a floating point number. As described below, the EM in test runs was either "GENUINE" or "IMPOSTER" based on eBID being equal to the vBID; but in the actual test with real data, the EM always read "IMPOSTER" as the scores were being reported independent of the eBID and vBID relationship.

To meet the requirement of 1311.116(h)(3) that the algorithms are provided to the laboratory and not the scores, iBeta generated a C# application which renamed all the reference and probe images with a new BID, Sequence Number, and date of acquisition. The program generated a dictionary of input BID values to output BID values (obfuscated BIDs). Therefore, only the iBeta dictionary indicated whether a particular reference file should or should not match a particular probe file.

The number of subjects varied for each of the mobile devices, but was approximately 110. Those numbers are tabulated in Section 6 - Results.

The EyeVerify test application produced a matching score for each attempted match. The application tested all possible combinations of enrolled records against verification records. The EyeVerify generation of the test application was performed during the pre-certification stage and iBeta had previously tested and agreed to that application prior to testing.

iBeta's testing protocol does not include dependent matches. Thus, the match A x B where A and B are different BIDs and the matching is expected to not match, the corresponding match B x A is not performed. Thus, for n pairings there are expected to be  $n*(n-1)/2$  independent results. Given the EyeVerify results file, an iBeta application used the previously generated dictionary of actual BIDs to obfuscated BIDs to generate a new CSV file that contained the actual BIDs, the actual SN, and the actual EM as well as that corresponding score.

The biometric subsystem was configured to produce a similarity index for each attempted matching. The biometric system normally accepts a match only when the similarity index exceeds the operating point index. Therefore using the reported similarity index, iBeta calculated whether the challenge would be matched by the system at that operating point or not. Over a series of simulated operating points, and based on this calculation, each challenge was reported as a true match ( $tm_i$ ), true reject ( $tr_i$ ), false accept ( $fm_i$ ) or false reject ( $fr_i$ ).

$$FMR = \frac{\sum_{i=1}^N fm_i}{N} \quad (3.2.3 - 1)$$

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. Table 3-2 shows the values taken from Figure B.1 of INCITS/ISO/IEC 19795-1:2006[2007], which plots  $O/N$  = the Observed Error Rate and  $C/N$  = the Claimed Error Rate where  $N$  is the number of comparisons made. Here,  $O$  is the observed number of errors for the given  $N$  and  $C$  is the virtual number of errors that fall within the 95% confidence interval of the hypothesis that the FMR is 0.001 or better. While Figure B.1 of ISO 19795-1 has observed error rates as high as  $30/N$ , iBeta chose to use smaller values of  $N$  to lower the cost of testing (for any given claimed error rate).

To obtain the matches, iBeta challenged all enrollment (reference) records against all verify (probe) records. However the matching of  $I \times J$  was not repeated for the dependent case of  $J \times I$  where the first record is the enrollment (reference) and the second record is the verification (probe) record. Thus there are approximately  $N*(N-1)/2$  expected non matches and  $N$  matches if every reference has a corresponding probe associated with it.

**Table 3-2 Claimed versus Measured Error Rates**

<b>N x Observed Error Rate</b>	<b>N x Claimed Error Rate</b>	<b>Minimum N for an Error Rate of 0.001</b>
0	3.0	3000
1	4.8	4800
2	6.4	6400
3	7.9	7900
4	9.3	9300
5	10.6	10600
6	11.9	11900

Using methods and formulas documented in ISO/IEC 19795-1:2006, the variances of the above rates were calculated using Table 3-2.

### 3.2.3 Test Execution

Test data collection was conducted during the April 17 through 24, 2015 timeframe and the results are listed in Attachment 1.

Following the DEA Regulations 21 CFR Part 1311, subjects were enrolled and included iBeta employees and non-employees as per the iBeta DEA-EPCS Biometric Test Protocol approved by the Copernicus Group Independent Review Board on 22 September 2014, approval: IBE-14-437.

Subject biographical data was acquired on paper. Only an identifier, the Biometric ID (BID), connected the subject biographical data to the acquired biometric data. As of the publication of this report, the biographical data collected for this study has been destroyed except for the aggregate data reported herein.

The mobile devices enclose the biometric device, which consisted of the front-facing camera and the EyeVerify application. Acquisition of Technology Testing corpus data was acquired in an office type of environment consistent with the expected environment for prescribing practitioners.

The acquired data transfer was dependent on the mobile device. All devices were connected to a PC via their USB cable to download the data.

- iPhone (iOS) – The folder was available for copying in iTunes.
- Samsung and HTC (Android) – The folder was available as an automatically or semi-automatically mounted drive when plugged into the PC.

As above, the biometric data was transferred to the Technology Testing computer as per iBeta security procedures. During periods when the EyeVerify application was performing matching, the biometric data

was transferred to a USB drive. After the matching, the USB data was destroyed per the iBeta security procedures.

A Failure to Enroll (FTE) Rate not to exceed 15% was assumed in the data collection planning. Only one subject (with an eye tumor) and two subjects (who wore glasses and reported not being able to see the target for enrollment without their glasses) were noted as FTEs.

As per the iBeta security procedures and after completion of all testing, subject Personally Identifiable Information (PII) biographical data was logically overwritten as per a NIST SP800-88 approved method by using the Microsoft Sysinternals SDelete utility.

As described in section 3.2.2, the images were presented to the EyeVerify matching application and it performed all possible pair matches. During reverse analysis of that data, the iBeta application produced only the first expected non-match pairing, and not the second or any other pairings with dependent verification records.

Because verification records from approximately 55 subjects were not acquired, duplicate verification records were acquired from the remaining subjects. Thus, the FNMR value was based on fewer subjects than the FMR value, but approximately the same number of expected match (EM) attempts. That usage is consistent with ISO 19795-5 allowing up to five verification attempts per visit to produce FRR numbers. Thus, the iBeta application which sorted the EyeVerify results included all A x A expected matches even if there was more than one.

There were no issues that were identified in the review; therefore, there is no attached Discrepancy Report.

During this test effort, iBeta experienced no Failure to Acquire (FTA) instances.

Subjects who appeared for the test wearing eyeglasses were tested as two separate individuals. First, those individuals enrolled and verified wearing their glasses. Second, they enrolled and verified again with a different BID. However, those individuals were tracked within the subsequent data analysis which was performed a) without eyeglasses and b) all subjects with and without eyeglasses. For this certification, only results without eyeglasses are being considered; however, as delineated in Section 6.3, the wearing of eyeglasses did not significantly affect the FMR.

### **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 were no deviations or omissions from the standards.

## 4 Biometrics System Identification

The EyeVerify matching algorithm and three mobile device cameras 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 version of the EyeVerify algorithm tested. The smartphones' front facing cameras and corresponding EyeVerify application produced sRGB images.

Table 4-1 contains the elements of the EyeVerify EyePrint ID™ versions of the SDKs for iOS and Android that were tested within the data collection packages provide by EyeVerify.

The smartphones/application submitted and certified in this report capture and process images as documented in Table 4.7 below. Because the image size processed into a template and the smartphone camera resolution could affect the FMR, no other devices are being certified.

**Table 4-1 Biometrics System Name and Version**

Biometric System Name	Version/SHA256 Hash/size (bytes)
EyeVerify EyePrint ID™	iOS Version 2.3.1 Android Version 2.3.3
EyeVerify Data Collection.apk	4a54a840fe17af3f7ebe79d876f67373274f8def359bbfd8f7984d669d9e5c9c / 10974617
EVCClient_Data_Collector-4f041.ipa	fe3751fbce38746115f0a10d971af26ccd58956bd648e33beb6c3dbef99f1830 / 16785982

This Biometrics System includes the following:

**Table 4-2 Biometrics System Components**

Hardware	Firmware, Operating System & Version	Description
Samsung Galaxy S5	Kernel: 3.4.0-438554 dpi@SWDD6107#1 Build: LRX21T.G900R4VXU1BOC1 SE for Android: SEPF_sm-g900r4_5.0.0009 Hardware version: G900R4.02	SmartPhone with Android application installed used for data collection
iPhone 6	Model MG692LL/A S/N F73NC1KEGSMN Firmware 2.23.03 iOS Version 8.3 (12F70)	SmartPhone with iOS application installed used for data collection
HTC One M9	s/n: FA53VYJ07550 IMEI: 357227060662085 Android: 5.0.2 HTC Sense: 7.0 Software number: 1.32.617.30 Kernel: 3.10.49-gc715f59 ans@AABM#1 SMP PREEMPT	SmartPhone with Android application installed used for data collection

The USB charging cords supplied with each mobile device were used to acquire data from the devices.

### 4.2 Biometrics System Test Environment

The Biometric Subsystem Test Environment identifies the specific hardware and software that was used in the test environment.

iBeta enrolled and verified all subjects using the each smartphone and associated application.

Throughout the data collection, no application upgrades were introduced and no smartphone hardware failures occurred to prompt any change to the hardware.

**Table 4-3 Biometrics System Test Hardware**

Hardware	OS or Version	Manufacturer	Description
Gateway DX4860 Intel Core i5	Windows 7 Home Premium	Gateway/Acer	Generic PC

**Table 4-4 Biometrics System Test Software**

Software	Version	Manufacturer	Identify Hardware
TrueCrypt	7.1.a	TrueCrypt	All PC's and laptops
SDelete	1.61	Microsoft	All PC's and laptops
Oracle VM Virtual Box	4.3.26r98988	Oracle	Gateway DX4860
Ubuntu-64	14.10	Ubuntu	Gateway/Oracle VM AMD64 version
iTunes	12.1.2.27	Apple	All PC's and laptops
Andro Shredder	1.19	Apparillos.com	Android devices

**Table 4-5 Biometrics System Technical Documents**

Version #	Title	Abbreviation	Date	Author (Org.)
	Installing the EyeVerify iOS Demo App		4/25/14	EyeVerify
	EyeVerify Product Flow Diagram		2/9/15	EyeVerify
	Eyeprint Batch Verification Testing		4/22/15	EyeVerify Inc.

**Table 4-6 Other Software, Hardware and Materials**

Material	Material Description	Use in the Biometrics System
Other		
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
Repository servers	Separate servers for storage of test documents and source code, running industry standards operating systems, security and back up utilities	Supplied by iBeta: Documents are maintained on a secure network server. Source code is maintained on a separate data disk on a restricted server
Microsoft Office 2013	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 2010	TDP and test documentation repository	Supplied by iBeta: Vendor document and test documentation repository and configuration management tool
Other standard business application software	Internet browsers, PDF viewers email	Supplied by iBeta: Industry standard tools to support testing, business and project implementation
Visual Studio 2013 v.12.0.2.1005.1 (Microsoft)	Build and source code Integrated Development Environment	Supplied by iBeta: View source code
Beyond Compare 3 v.3.2.4 (Scooter Software)	Comparison utility	Supplied by iBeta: used to compare file/folder differences
WinDiff 5.1 (Microsoft)	Comparison utility	Supplied by iBeta: used to compare file/folder differences
Md5deep v4.4	Open Source	Hashing of executable code
Extech Easy View 30 Light Meter	Ambient light meter	Ambient light measurements were taken prior to biometric data acquisition on a per day basis or when conditions change

The front-facing camera characteristics are documented in Table 4-7. Despite the focal length differences in the cameras, the user feedback encouraged a user to fill the available width of the

feedback image with their pair of eye images. Thus, there was an approximate correlation between the image width and the area corresponding to an eye-white capture. The distance given in Table 4-7 was measured for a typical closest approach from the surface of the eye to the device surface, and in all cases is roughly +/- 0.25 in.

**Table 4-7 Mobile Device camera characteristics (front facing camera)**

Device	Mega-pixels	Image size (Width x Height)	f/#	Approx Distance (in)	Source
Samsung Galaxy S5	2.0	1080 x 1920	“wide angle lens”	6.00	<a href="http://samsung.com">samsung.com</a>
iPhone 6	1.2	960 x 1280	f/2.2	6.25	<a href="http://apple.com">apple.com</a>
HTC One M9	4.1*	1520 x 2688	f/2.0 26.8 mm	8.00	<a href="http://htc.com">htc.com</a> , size by inspection

\*Specification is in ultrapixels

## 4.2.1 Biometrics Test Environment – Technology Test

The devices listed in Table 4-3 indicate their functional purpose in the test effort. Three devices were used for test coverage, as described in Table 4-7.

### 4.2.1.1 Processing and Post-processing

The originally acquired images were stored in an encrypted mountable NAS drive connected only to an isolated network in the test lab. These images were transferred to a USB for testing in the Linux virtual machine. The results of that testing were offloaded to a Windows PC for further analysis.

## 5 Biometrics System Overview

The EyeVerify biometric subsystem consists of an EyeVerify mobile SDK and the front-facing camera of the mobile device.

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)).

The biometrics subsystem consist of the matching application and its corresponding enrollment and verification records. The EyeVerify provided a MatchTest utility as a standalone Linux or MacOS application.

The normal EyeVerify mobile SDK acquires enrollment images and associates them with the user ID and the device ID and stores the template locally on the device. At the time of authentication, the appropriate set of templates is looked up by user ID. Then, another set of images are acquired for the user. The templates from that authentication attempt are matched against the enrolled templates.

The EyeVerify app emulated this behavior by enrolling all the images in the enrollments folder, and then performed a match of those against the images in the verifications folder.

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. The primary goal of this certification was to verify the EyeVerify application could meet the 0.001 FMR requirements of the DEA EPCS.

## **6 Certification Review and Test Results**

The results and evaluations of the certification are identified below. Detailed data regarding the Acceptance/Rejection criteria, reviews and tests for FMR are found in Attachment 1 (not released publicly).

### **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 EyeVerify to provide iBeta with the names of the systems and devices for certification which are representative of those systems and devices produced for the consumer. iBeta used its own devices for the testing.

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.

The EyeVerify biometric subsystem operates only in verification mode (1:1). The following results from the technology test indicate the threshold for each device that must be used to meet the 0.001 FMR requirement.

The scope of this iBeta report and certification is solely for the EyeVerify biometric subsystem as listed in Section 4. The evaluation and testing certifies that the EyeVerify 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 EyeVerify Component Results**

There were neither deviations from the DEA approved test method nor any test setup that varied from the standard protocol. The results are reported in detail in Amendment -1 (not publicly available) to this report.

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 Match Rate Review**

As described in the Test Environment Setup Section 3.2.2 above, the False Match Rate (FMR) was calculated based on results from up to 5461 attempted matches of up to 118 enrolled subjects. Although there were no FTAs and the FTEs were consistent on all platforms, some of the subjects did not attempt data collection on all of the smartphones yielding between 116 and 118 subjects per platform.

iBeta obtained the Age (Table 6-1) and Gender (Table 6-2) demographics reported below.

**Table 6-1 Age Demographics**

Age (Years)	Samsung		iPhone		HTC	
	Count	Percent	Count	Percent	Count	Percent
<21	0	0.0%	0	0.0%	0	0.0%
21 - 30	23	19.5%	22	18.8%	23	19.8%
31 - 50	65	55.1%	65	55.6%	64	55.2%
51 - 70	30	25.4%	30	25.6%	29	25.0%
70>	0	0.0%	0	0.0%	0	0.0%

**Table 6-2 Gender Demographics**

Gender	Samsung		iPhone		HTC	
	Count	Percent	Count	Percent	Count	Percent
Male	64	54.2%	65	55.6%	63	54.3%
Female	54	45.8%	52	44.4%	53	45.7%
Undisclosed	0	0.0%	0	0.0%	0	0.0%

Table 6-3 summarizes the measured false match rate (FMR) and threshold for each of the three devices for subjects not wearing eyeglasses. The false match (FM) value is the count of false matches observed for that threshold and FMR. In the table, the minimum threshold that meets the DEA EPCS requirement is highlighted in green.

**Table 6-3 Thresholds to meet 95% Confidence Interval of 0.001 FMR**

Device	threshold	FM	FMR 95% CI
Samsung	3.161	0	0.000566
	2.978	1	0.000905
	2.969	2	0.001207
	2.945	3	0.001490
iPhone	3.917	0	0.000560
	3.030	1	0.000897
	3.000	2	0.001195
HTC	3.413	0	0.000570
	3.367	1	0.000912
	3.316	2	0.001216
	3.290	3	0.001501

The HTC device required the largest threshold to meet the 0.001 FMR requirement. If an overall threshold for all devices were to be chosen, the value of 3.367 would meet the requirement on the three device types tested.

For subjects wearing eyeglasses, the same numbers of false matches (FM) were observed for both wearing and not wearing the eyeglasses. In this test method, the number of expected matches and expected non-matches increased because every person wearing eyeglasses was counted twice, once without and once with the eyeglasses. This led to an additional three expected matches for those individuals and approximately one thousand additional expected non-matches. Because these additional expected non-matches were not independent (having come from the same individual), counting them would lower the FMR artificially. However, Table 6-4 shows that the number of false matches (FM) did not change at each threshold for each device. Therefore, the wearing of eyeglasses did not significantly affect the FMR in the region of 0.0006-0.0015 tested in this study.

**Table 6-4 Thresholds for the case with and without eyeglasses.**

Device	threshold	FM
Samsung	3.161	0
	2.978	1
	2.969	2
	2.945	3
iPhone	3.415	0
	3.030	1
	3.000	2
HTC	3.413	0
	3.367	1
	3.316	2
	3.290	3

### 6.3.1 Exceptions

The EyeVerify biometric subsystem is certified effective on the publish 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 6-5 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 state that the EyeVerify biometric as obtained and described herein meets the other subsystem requirements for use in a DEA EPCS system. However, as described below, some requirements were not testable or not applicable to the system iBeta tested.	<input type="checkbox"/>
1311.116(b)	The biometric subsystem must operate at a false match rate of 0.001 or lower.	As describe in section 6.3, the API and device meet this requirement if the appropriate threshold is set.	<input checked="" type="checkbox"/>
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.	<input checked="" type="checkbox"/>
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 §	Not Applicable	<input checked="" type="checkbox"/>

Requirement Reference	Requirement	Details of level of iBeta Assessment	✓
	1311.08, if they exist for the biometric modality of choice.		
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 has the capability to be co-located with the computer or PDA, but that determination was outside of the scope of this certification.	<input type="checkbox"/>
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.	iBeta observed source code indicating that the Device ID is used as one source of random data used to both obfuscate and encrypt the biometric enrollment records. Without the correct Device ID, the verification would fail.	<input checked="" type="checkbox"/>
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.	Authentication itself is local, and as such this requirement is not applicable to that portion of the subsystem. However, iBeta did not validate how that authentication might be communicated to any entity outside the mobile device. Therefore, even though the mobile device might be co-located with the rest of the system, if that system is external to the mobile device, it might not be considered to be local because it might not be within the security perimeter of the mobile device or overall prescribing system.	<input type="checkbox"/>
1311.116(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's process and procedures to test the FMR at 95% confidence interval have been approved by the DEA. This report will be available on the iBeta website for 2 years after publication.  (2) iBeta is independent of EyeVerify and Wells Fargo and does not have an interest in the outcome of the performance of this testing.  (3) Test data were destroyed at the conclusion of testing and test data were not provided to the vendor during testing.  (4) Algorithms in the form of an API and associated executables were tested.  (5) This report is available at <a href="http://www.ibeta.com/our-software-quality-services/epcs/reports/">http://www.ibeta.com/our-software-quality-services/epcs/reports/</a>	<input checked="" type="checkbox"/>

EyeVerify makes the following claims concerning EyePrint biometric matching in its online documentation:

1. Image Capture
2. Segmentation & Enhancement
3. Interest Point Detection & Feature Extraction
4. Chaff points added
5. Scramble Descriptors
6. Eyeprint key encoding
7. Matching
8. Eyeprint key decoding

iBeta observed source code corresponding to items 2 through 8 listed above, which included the use of the Device ID in items 4 and 5. Except for the use of the Device ID, iBeta did not observe that any of these steps are applicable to the DEA EPCS 21 CFR 1311.116 requirements.

#### **6.4.1.1 Exceptions**

The 21 CFR 1311.116(f) and (g) requirements were tested as described in Table 6-5. However the testing of the overall system is out of scope of this certification. This report complies with 1311.116(c) but not with 1311.300(a) except as they apply to the biometric subsystem tested.

## 7 Opinions and Recommendations

### 7.1 Recommendations

iBeta Quality Assurance has completed the testing of the EyeVerify 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 EyeVerify Eyeprint sensor 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. See also Table 6-5 for details of how each requirement was validated.

**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 to 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.	☑
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.	☑

Requirement	Description	Approved
1311.116(h)(2)	Test data are sequestered.	<input checked="" type="checkbox"/>
1311.116(h)(3)	Algorithms are provided to the testing laboratory (as opposed to scores or other information).	<input checked="" type="checkbox"/>
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.	<input checked="" type="checkbox"/>

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 6-5 for details.
- (g) iBeta did not test or validate this requirement, and it must be tested within the communication to the overall system.

iBeta did observe that in the case of eyeglasses, the FNMR was adversely effected by reflections of lighting sources in the eyeglasses. If this situation occurs during verification, then it may be overcome by turning the head or raising or lowering the head to minimize the reflection(s). However, if it occurs during enrollment, it may negatively impact the FNMR for all future verifications.

### 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 CFR Part 1311 such as auditing and records maintenance. These are the responsibility of the overall system since the biometric subsystem only returns a pass/fail response to one of the two factors used for authentication prior to signing a prescription.

As shown in Table 6-3, the Samsung Galaxy S5 and the iPhone 6 meet the FMR requirement of 0.001 with a threshold of 3.03. However the HTC One M9 required a higher threshold to meet the requirement. That result reinforces the conclusion that the FMR may depend on the optics of the device and therefore only the specific devices tested are approved by this report.

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. For example, iBeta observed that the matching score for an expected match for subjects wearing eyeglasses was always lower than for the same subjects not wearing eyeglasses. In this study, that difference in scores did not impact the results in the 0.1% range of FMR; however, only the non-glasses portion of the study is being used to certify the biometric subsystem.

### 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 collect and analyze the proprietary Eyeprint biometric authentication methods provided by EyeVerify.

The EyeVerify Eyeprint software and sensors operated as expected.

### **7.3 Responsible Test Laboratory Personnel**

The contact information for the Copernicus Group IRB appointed Principal Investigator for this test effort:

A handwritten signature in cursive script that reads "Kevin Wilson".

Kevin Wilson Ph.D.  
Director of Biometrics  
KWilson@ibeta.com  
303-627-1110 extension 177