 **ONC §170.315(d)(13)**

Multi-Factor Authentication (MFA) – Evidence Package

Product: **Pace + / Content Distributor**

Version: 4.1.0

1 Criterion Summary

Regulatory Requirement:

The Health IT must support multi-factor authentication for user access control.

System must:

- Require at least two authentication factors
 - Enforce MFA when enabled
 - Prevent bypass
 - Protect against brute-force OTP attacks
 - Log authentication events
-

2 MFA Use Case Statement

Multi-Factor Authentication (MFA) is required for all user access to protected functionality within the Pace Plus system. MFA is enforced immediately after successful username and password validation and prior to granting access to any system resources.

MFA is required in the following scenarios:

- All user login attempts to the application
- Access to protected clinical and administrative data
- Execution of sensitive operations, including data export, user management, and system configuration
- Any session where MFA is enabled at the user or system level

The authentication process requires two factors:

1. Knowledge Factor – Username and password
2. Possession Factor – Time-based One-Time Password (TOTP) generated via an authenticator application

Users are not granted access until both factors are successfully validated. The system prevents bypass by restricting access to all protected resources until MFA verification is complete.

To ensure security, the system enforces:

- Limited OTP attempts with temporary lockout on repeated failures
- Protection against brute-force attacks
- Logging of all MFA-related events for audit and compliance

3 Enrollment Process (New Users)

When user logs in and no MFA row exists:

- Row inserted in tblUserMfaSettings
- Unique Base32 secret generated (32 chars)
- QR code generated locally
- Manual key shown only during enrollment
- MFA enabled after first successful OTP verification

4 Database Evidence

Table: tblUserMfaSettings

Columns:

Column	Purpose
UserId	FK to user
TwoFactorEnabled	MFA status

Column	Purpose
TotpSecret	Unique per-user secret
FailedOtpAttempts	Attempt counter
LockoutUntilUtc	Lockout timestamp
UpdatedUtc	Audit timestamp

```

SELECT UserId, TwoFactorEnabled, FailedOtpAttempts, LockoutUntilUtc
FROM dbo.tb1UserHfaSettings;

```

Results	Messages		
UserId	TwoFactorEnabled	FailedOtpAttempts	LockoutUntilUtc
1	1	0	NULL
62	0	0	NULL

Query executed successfully. | staging-paceplus-2019.c326a... | rootpaceplus1 (72) | SanTanCD | 00:00:00 | 2 rows

5 Brute-Force Protection

Controls Implemented

- Max OTP attempts: 5
- Lockout duration: 15 minutes
- Lockout enforced before validation
- Attempts reset on successful login

6 Audit Logging

Table: tblAuthAuditLog

Logged Events:

- OTP_SUCCESS
- OTP_FAIL
- OTP_LOCKED

Each log includes:

- UserId
- Username
- IP Address
- UserAgent
- Timestamp (UTC)
- Success flag

Proof Query

```
SELECT TOP 20 *
FROM dbo.tblAuthAuditLog
ORDER BY CreatedUtc DESC;
```

Id	UserId	Username	Event Type	Success	IpAddress	UserAgent	CreatedUtc
1	41	admin	OTP_SUCCESS	1	3.216.102.2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW...	2026-03-03 07:23:50.713
2	40	maritzar	OTP_SUCCESS	1	3.216.102.2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW...	2026-03-03 06:37:30.917
3	39	maritzar	OTP_FAIL	0	3.216.102.2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW...	2026-03-03 06:34:59.527
4	38	maritzar	OTP_SUCCESS	1	3.216.102.2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW...	2026-03-03 06:33:57.093
5	37	admin	OTP_SUCCESS	1	3.216.102.2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW...	2026-03-03 06:33:17.353
6	36	admin	OTP_SUCCESS	1	3.216.102.2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW...	2026-03-03 06:18:43.770
7	35	admin	OTP_FAIL	0	3.216.102.2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW...	2026-03-03 06:18:30.560
8	34	admin	OTP_SUCCESS	1	3.216.102.2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW...	2026-03-03 04:52:54.657
9	33	admin	OTP_SUCCESS	1	3.216.102.2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW...	2026-03-03 04:52:03.910
10	32	admin	OTP_SUCCESS	1	3.216.102.2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW...	2026-03-02 04:26:04.553
11	31	admin	OTP_FAIL	0	3.216.102.2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW...	2026-02-27 10:36:28.737
12	30	admin	OTP_SUCCESS	1	3.216.102.2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW...	2026-02-27 06:31:11.370
13	29	admin	OTP_SUCCESS	1	3.216.102.2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW...	2026-02-27 06:29:59.900
14	28	admin	OTP_SUCCESS	1	3.216.102.2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW...	2026-02-27 06:20:08.607
15	27	admin	OTP_SUCCESS	1	3.216.102.2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW...	2026-02-27 06:17:43.613
16	26	admin	OTP_FAIL	0	3.216.102.2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW...	2026-02-27 05:59:03.160
17	25	admin	OTP_SUCCESS	1	3.216.102.2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW...	2026-02-27 05:58:40.620
18	24	admin	OTP_SUCCESS	1	3.216.102.2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW...	2026-02-27 05:58:07.853
19	23	admin	OTP_SUCCESS	1	3.216.102.2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW...	2026-02-27 05:55:16.973

Query executed successfully. staging-paceplus-2019-c326a... rootpaceplus1 (72) SanTanCD 00:00:00 20 rows

7 Security Controls

Manual Key Exposure

- Manual key shown only during initial enrollment

- Hidden for all existing MFA-enabled users

Secret Generation

- Cryptographically secure RNG
- Base32 compliant
- Unique per user

OTP Validation

- RFC 6238 compliant
 - ± 1 time-step drift allowed
 - Constant-time comparison (SlowEquals)
-

8 Compliance Mapping

D13 Requirement	Status
Two-factor authentication supported	✓
MFA enforcement (no bypass)	✓
Enrollment workflow	✓
OTP validation	✓
Attempt limit / lockout	✓
Audit logging	✓
Unique per-user secret	✓
Manual key exposure control	✓

Login Page

The screenshot shows a web browser window with the URL `thairdemo.pace-plus.com/Demo/`. The page features the **PACE+** logo on the left and the **MSHealth** logo on the right. The main content area is a blue rectangle with the text "Sign In" at the top. Below it are two input fields: the first contains the text "admin@" and the second contains a series of asterisks. A "Login to your account" button is positioned below the password field, and a "Reset Password" link is located at the bottom right of the sign-in area. At the bottom of the page, there is a navigation bar with the **PACE+** logo on the left and three links: "HELP", "CONTACT", and "SUPPORT".

When New User Login

The screenshot shows a web browser window with the URL `thairdemo.pace-plus.com/Demo/Verify2FA.aspx`. The page features the **PACE+** logo on the left and the **MSHealth** logo on the right. The main content area is a white rectangle with the text "Multi-Factor Verification" at the top. Below it are two sections: "Scan QR (Authenticator App)" which contains a QR code, and "Enter 8-digit code" which contains an input field and a "Verify" button. At the bottom of the page, there is a navigation bar with the **PACE+** logo on the left and three links: "HELP", "CONTACT", and "SUPPORT".

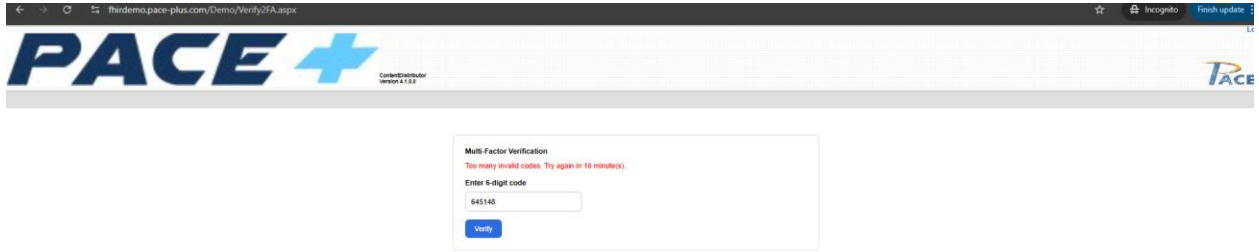
When User Already Scan Google Authentication

The screenshot shows a web browser window with the URL `http://demo.pace-plus.com/Demo/Verify2FA.aspx`. The page header features the **PACE+** logo on the left and a **LogIn** link on the right. The main content area contains a "Multi-Factor Verification" form with the prompt "Enter 6-digit code" and a "Verify" button. The form is empty, indicating a successful scan.

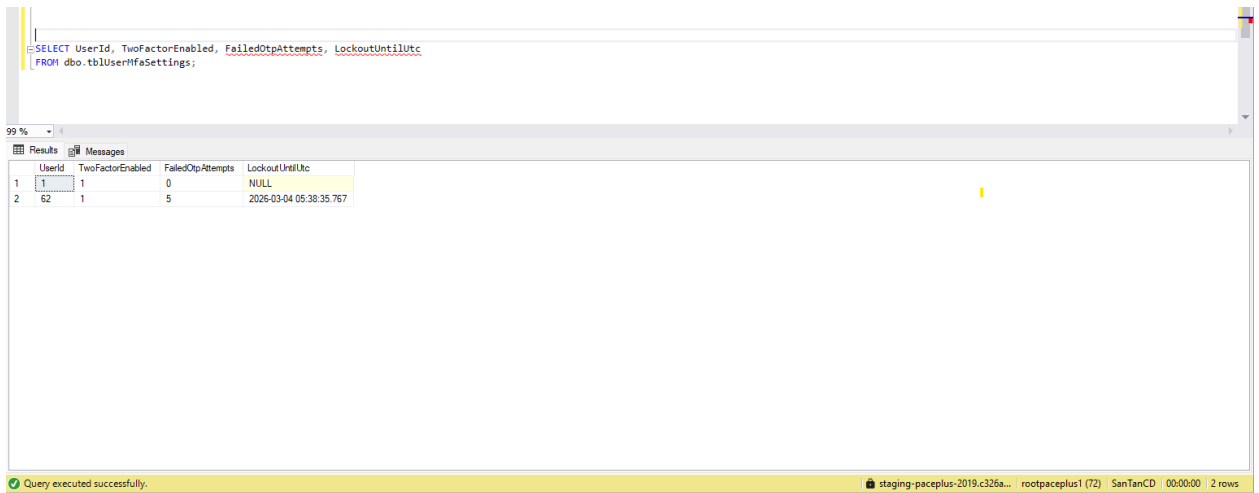
When User Enter Wrong OTP and Enter Expired OTP They showing Invalid Code

The screenshot shows the same PACE+ Multi-Factor Verification page. The form now displays an error message: "Invalid code" in red text. Below the prompt "Enter 6-digit code", the input field contains the code "651433". The "Verify" button is still present.

When User Enter Times Wrong OTP 5 Times Than showing Validation



5 Attempts Proof in Database



DB Proof

```
SELECT TOP 30 *
FROM dbo.tbAuthAuditLog
ORDER BY CreatedUtc DESC;
```

99 %

Results Messages

Id	UserId	Username	Event Type	Success	Ip-Address	UserAgent	CreatedUtc
1	41	admin	OTP_SUCCESS	1	3.216.102.2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW...	2026-03-03 07:23:50.713
2	40	maritzar	OTP_SUCCESS	1	3.216.102.2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW...	2026-03-03 06:37:30.917
3	39	maritzar	OTP_FAIL	0	3.216.102.2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW...	2026-03-03 06:34:59.527
4	38	maritzar	OTP_SUCCESS	1	3.216.102.2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW...	2026-03-03 06:33:57.093
5	37	admin	OTP_SUCCESS	1	3.216.102.2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW...	2026-03-03 06:33:17.353
6	36	admin	OTP_SUCCESS	1	3.216.102.2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW...	2026-03-03 06:18:43.770
7	35	admin	OTP_FAIL	0	3.216.102.2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW...	2026-03-03 06:18:30.560
8	34	admin	OTP_SUCCESS	1	3.216.102.2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW...	2026-03-03 04:52:54.657
9	33	admin	OTP_SUCCESS	1	3.216.102.2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW...	2026-03-03 04:52:03.910
10	32	admin	OTP_SUCCESS	1	3.216.102.2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW...	2026-03-02 04:26:04.553
11	31	admin	OTP_FAIL	0	3.216.102.2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW...	2026-02-27 10:36:28.737
12	30	admin	OTP_SUCCESS	1	3.216.102.2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW...	2026-02-27 06:31:11.370
13	29	admin	OTP_SUCCESS	1	3.216.102.2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW...	2026-02-27 06:29:59.900
14	28	admin	OTP_SUCCESS	1	3.216.102.2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW...	2026-02-27 06:20:08.607
15	27	admin	OTP_SUCCESS	1	3.216.102.2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW...	2026-02-27 06:17:43.613
16	26	admin	OTP_FAIL	0	3.216.102.2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW...	2026-02-27 05:59:03.160
17	25	admin	OTP_SUCCESS	1	3.216.102.2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW...	2026-02-27 05:58:40.620
18	24	admin	OTP_SUCCESS	1	3.216.102.2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW...	2026-02-27 05:58:07.853
19	23	admin	OTP_SUCCESS	1	3.216.102.2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW...	2026-02-27 05:55:16.973

Query executed successfully. staging-paceplus-2019.c326a... rootpaceplus1 (72) SanTanCD 00:00:00 20 rows

```
SELECT * FROM dbo.tbUserIfcSettings;
```

9 %

Results Messages

UserId	TwoFactorEnabled	TotpSecret	RecoveryCodes	UpdatedUtc	FailedOpAttempts	LogoutUntilUtc
1	1	JBSWY3DPEHPK3PX	NULL	2026-03-03 07:23:50.710	0	NULL
2	62	SK63XBFFD3L6DG6RMTYPOG6WBQOV3I76	NULL	2026-03-04 05:23:35.767	5	2026-03-04 05:38:35.767