CMS Manual System	**Department of Health & Human Services (DHHS)**
Pub 100-20 One-Time Notification	**Centers for Medicare & Medicaid Services (CMS)**
Transmittal 13736	**Date: April 16, 2026**
	Change Request 14435

SUBJECT: Require Healthcare Integrated General Ledger Accounting System (HIGLAS) Users to Begin Using Phishing-resistant Multi-Factor Authentication (MFA) for Login

I. SUMMARY OF CHANGES: The purpose of this Change Request (CR) is to notify users of Healthcare Integrated General Ledger Accounting System (HIGLAS) that, beginning January 1, 2027, access will require the use of a phishing-resistant Multi-Factor Authentication (MFA) method. This action is required to ensure phishing-resistant MFA is implemented for HIGLAS users and to facilitate the transition to the new authentication front end.

EFFECTIVE DATE: May 18, 2026
**Unless otherwise specified, the effective date is the date of service.*
IMPLEMENTATION DATE: 10 weeks from receipt of security tokens

Disclaimer for manual changes only: The revision date and transmittal number apply only to red italicized material. Any other material was previously published and remains unchanged. However, if this revision contains a table of contents, you will receive the new/revised information only, and not the entire table of contents.

II. CHANGES IN MANUAL INSTRUCTIONS: (N/A if manual is not updated)
R=REVISED, N=NEW, D=DELETED-*Only One Per Row.*

R/N/D	CHAPTER / SECTION / SUBSECTION / TITLE
N/A	N/A

III. FUNDING:

For Medicare Administrative Contractors (MACs):
The Medicare Administrative Contractor is hereby advised that this constitutes technical direction as defined in your contract. CMS does not construe this as a change to the MAC Statement of Work. The contractor is not obligated to incur costs in excess of the amounts allotted in your contract unless and until specifically authorized by the Contracting Officer. If the contractor considers anything provided, as described above, to be outside the current scope of work, the contractor shall withhold performance on the part(s) in question and immediately notify the Contracting Officer, in writing or by e-mail, and request formal directions regarding continued performance requirements.

IV. ATTACHMENTS:
One Time Notification

Attachment - One-Time Notification

Pub. 100-20	Transmittal: 13736	Date: April 16, 2026	Change Request: 14435

SUBJECT: Require Healthcare Integrated General Ledger Accounting System (HIGLAS) Users to Begin Using Phishing-resistant Multi-Factor Authentication (MFA) for Login

EFFECTIVE DATE: May 18, 2026
**Unless otherwise specified, the effective date is the date of service.*
IMPLEMENTATION DATE: 10 weeks from receipt of security tokens

I. SUMMARY OF CHANGES: The purpose of this Change Request (CR) is to notify users of Healthcare Integrated General Ledger Accounting System (HIGLAS) that, beginning January 1, 2027, access will require the use of a phishing-resistant Multi-Factor Authentication (MFA) method. This action is required to ensure phishing-resistant MFA is implemented for HIGLAS users and to facilitate the transition to the new authentication front end.

II. GENERAL INFORMATION

A. Background: Current authentication options for HIGLAS are either a Personal Identity Verification (PIV) Card or a username/password with a second factor such as One Time Password (OTP) from an RSA token, Email-based OTP, or Short Message Service (SMS)-based OTP. The various OTP options have their own weaknesses and, like passwords, are susceptible to phishing. HIGLAS would like to introduce a new option, Fast Identity Online (FIDO)2.

While the PIV card option is phishing-resistant, not all contractors have been issued them for a variety of reasons. For example, it has been a continued challenge to issue the cards to Medicare Administrative Contractor (MAC) staff, and CMS elected to remove issuance stations from the MACs in 2025. Contractors with a PIV card should continue to use it until the card expires. If the certificates expire, they can be renewed remotely.

A FIDO2 hardware security token provides passwordless authentication capabilities using a hardware-based authenticator combined with public key cryptography. FIDO2 and the related WebAuthn protocol are resistant to adversary-in-the-middle attacks. By implementing the hardware security tokens, CMS enables an additional MFA option that complements the existing PIV process for all its employees and contractors.

CMS is also partnering with the U.S. Department of Health and Human Services (HHS) to develop the capability to remotely issue the same certificates used on a PIV card directly to a FIDO2 hardware security token. This will supplement the use of FIDO2 for authentication to HIGLAS. This capability is not expected to be available until fiscal year 2027.

The HIGLAS authentication system is moving from the current Health Integrated Identity Management (HIDM) front end to using Identity Management (IDM) as the front end.

Migration to the new front end will not begin until the contractor firm has the security keys in possession. As users are issued a security token, they will be activated in IDM and start using it to log into HIDM-based systems. Due to differing procurement timelines, contractor firms will begin migrating on different dates. We would like to complete this by January 1, 2027, barring any supply-chain issues.

Once a user has a security token, and they are placed in the IDM group, the user will be asked to set up the security token as a second factor at their first log in. They should also set up a backup factor in case of token loss or theft. CMS will provide a job aid for the second factor set up and will also offer office hours for each contractor firm with IT staff who can assist remotely with setup. We will need someone at each contractor firm to provide us with lists of users who are ready to migrate to IDM.

B. Policy: This CR does not involve any legislative or regulatory policies. This change aligns with IT security policy from both OMB and HHS.

III. BUSINESS REQUIREMENTS TABLE

"Shall" denotes a mandatory requirement, and "should" denotes an optional requirement.

Number	Requirement	Responsibility								
		A/B MAC			DME	Shared-System Maintainers				Other
		A	B	HHH	MAC	FISS	MCS	VMS	CWF	
14435.1	Contractors shall provide each of their staff who use HIDM-back systems such as HIGLAS with a FIPS-validated FIDO2 token, if they do not have an active PIV Card.	X	X	X	X					BCRC, CRC, HIGLAS, MSPIC, MSPSC
14435.2	Contractors should provide other staff who work on CMS systems that use IDM for authentication with a FIPS-validated FIDO2 token.	X	X	X	X					BCRC, CRC, HIGLAS, MSPIC, MSPSC
14435.3	HIGLAS users shall move to use a phishing-resistant MFA option. These include: • PIV Certificates, either on a card or remotely issued (when available) • FIDO2 or WebAuthn	X	X	X	X					BCRS, CRC, HIGLAS, MSPIC, MSPSC
14435.4	HIGLAS users shall no longer be allowed to only use the following MFA options after the contractor firm has provided FIPS-validated FIDO2 tokens to staff (estimated January 1, 2027):	X	X	X	X					BCRC, CRC, HIGLAS, MSPIC, MSPSC

Number	Requirement	Responsibility								
		A/B MAC			DME	Shared-System Maintainers				Other
		A	B	HHH	MAC	FISS	MCS	VMS	CWF	
	• RSA Token One Time Passwords (OTP) • Email or SMS OTPs • Authenticator App OTPs like Google Authenticator									

IV. PROVIDER EDUCATION

None

Impacted Contractors: None

V. SUPPORTING INFORMATION

Section A: Recommendations and supporting information associated with listed requirements: N/A

"Should" denotes a recommendation.

X-Ref Requirement Number	Recommendations or other supporting information:

Section B: All other recommendations and supporting information: N/A

VI. CONTACTS

Post-Implementation Contact(s): Contact your Contracting Officer's Representative (COR).

VII. FUNDING

Section A: For Medicare Administrative Contractors (MACs):
The Medicare Administrative Contractor is hereby advised that this constitutes technical direction as defined in your contract. CMS does not construe this as a change to the MAC Statement of Work. The contractor is not obligated to incur costs in excess of the amounts allotted in your contract unless and until specifically authorized by the Contracting Officer. If the contractor considers anything provided, as described above, to be outside the current scope of work, the contractor shall withhold performance on the part(s) in question and immediately notify the Contracting Officer, in writing or by e-mail, and request formal directions regarding continued performance requirements.

ATTACHMENTS: 0