

Multi-Factor Authentication Set Up By Coordinator

Multi-Factor Authentication (MFA) is a security technology that requires two or more ways to verify a user's identity before they can log into an application. This extra layer of security protects Personal Identifying Information (PII) and Protected Health Information (PHI). Users of MFA protected Health Commerce System (HCS) applications can choose how they want to verify their identity. To set up MFA, the user can sign up using their NYS driver license or NYS non-driver photo ID. If the HCS user does not have either, then they must see their HCS Coordinator **in person** for the set up.

What is needed to enter my user's MFA information?

1. You will need to validate the user's identity **in person**
2. The user must have a valid photo ID from this list >>>

U.S. Passport, with photograph and name
 US Driver's License with photograph and name
 US Federal, NY State ID card with photograph
 Driver's Lic issued by Canadian Govt.
 Unexpired foreign passport with I-551/I-94
 Alien Registration Card with photograph
 Unexpired Temporary Resident Card(INS I-688)
 Unexpired Employment Card(INS I-688A)
 Unexpired Reentry Permit(INS I-327)
 Unexpired Refugee Travel Document(INS I-571)
 Unexpired Employment Document(INS I-688B)

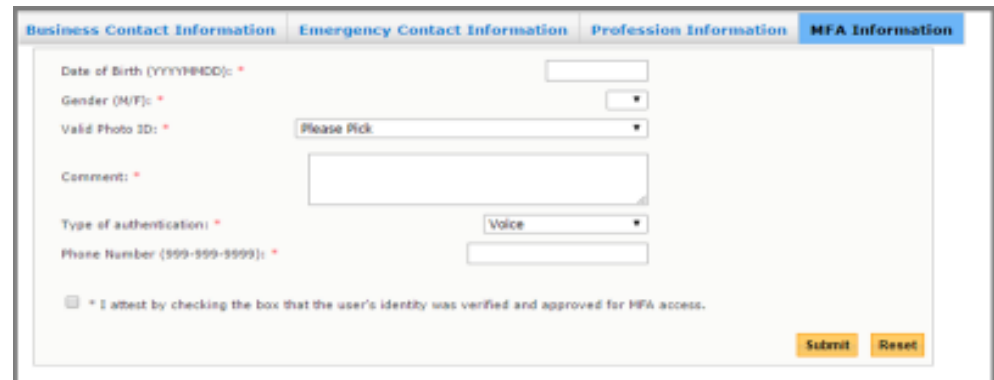
User MFA info can be set up anytime.

Previously submitted MFA info does not display on screen.

HCS Coordinator steps...

Where do I add or update a user's MFA Information?

1. Login to the HCS <https://commerce.health.state.ny.us> with your User ID and Password
2. Click **Coordinator's Update Tool** from My Applications List
3. Select the organization (if not selected)
4. Click **Manage People**
5. Click **user's name** link
6. Click **MFA Information** tab
7. Enter Date of Birth (YYYYMMDD) and Gender (M, F, X)
8. Select valid photo ID from list
9. Enter the following info in Comments:
 - Photo ID Account Number,
 - Photo ID Expiration Date,
 - Database used to validate the photo ID and
 - Method used to validate the Photo ID against the selected database/issuing agency
10. Select how the user wants to receive their authentication code: Voice, SMS or Time Based One Time Password Authenticator
11. Enter phone number, email or have user scan QR Code
12. **Check box to attest** that the user's identity was verified and approved for MFA access
13. Click **Submit**
14. Confirm **MFA information saved successfully**. For security, the user receives email to inform them their MFA has been modified.



Methods of MFA Authentication: SMS (text message), voice call, a Time Based One Time Authenticator or RSA token for internal users. This is why user needs to be in person when their MFA is set up by the Coordinator.