

CROWNWeb Security Update: Multi-Factor Authentication Overview

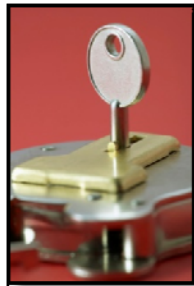
Did you know that federal data systems like CROWNWeb must have a second level of security verification (authentication)? This document will give you a quick overview of what **multi-factor authentication** is and what you need to know.

What is Multi-Factor Authentication?

Multi-factor authentication is associated with the way that data systems validate users who are attempting to sign in.

“Multi-factor authentication (MFA) is a security system in which multiple forms of authentication are [used] to verify [a user’s identification]. In contrast, single-factor authentication involves only a user ID and a password.”

- Definition courtesy of
www.techtarget.com

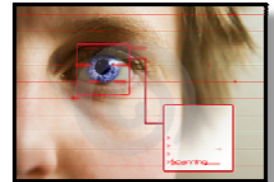


In a system with **multi-factor authentication** built in, users are required to provide their user name, password, and an additional piece of information to prove their identity before being allowed to access the data system.

Where Have I Seen Multi-Factor Authentication Before?

Multi-factor authentication is present in many data systems that you probably already use! You may have seen some form of MFA in the following places:

- Online Banking (choose your custom image AND enter a password)
- ATMs (present your magnetic card AND enter a pin)
- Telephones (receive a callback with a code and use the code AND username/password to log in)
- Biometrics (fingerprints/eye scans AND a pass code)



All of these provide a secondary level of identity verification... a “multiple factor” of authentication when logging in.

Why is Multi-Factor Authentication Important to Me?

CROWNWeb is a federal data system which will include patient-level private health information. It is critical that the information in that system be secure. Because of this need, there is a requirement for **multi-factor authentication**:

QualityNet System Security Policy (Published November, 2009)

Section 5.3.3.2 - User Identification and Authentication

*“Automated identification and authentication (IA) mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to enable unique identification and authentication of individual users (or processes acting in behalf of users) of QualityNet information systems. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of **multi-factor authentication**, some combination therein.”*

In order for CROWNWeb to be released on a national level, the system must be updated to include **multi-factor authentication** so that it will meet the stringent requirements of the QualityNet System Security Policy for federal data systems.

In the near future, more information about **multi-factor authentication** in CROWNWeb will be released, including information on how to configure or reconfigure YOUR CROWNWeb login credentials to meet the Multi-factor requirement.