South Carolina
Department of Disabilities
and Special Needs

MEMORANDUM

TO: Executive Directors of DSN Boards
CEOs of Contracted Service Providers
Therap Point of Contact

FROM: Jerome Frazier, Chief Information Security Officer Jerome Frazier

DATE: August 2, 2024

RE: Therap Two-Factor Authentication

Background:

Digital security is critical in today's world because both organizations and users store sensitive information online. Everyone interacts with applications, services, and data that are stored on the internet using online accounts. A breach, or misuse, of this online information could have serious real-world consequences, such as financial theft, business disruption, and loss of privacy.

While passwords protect digital assets, they are simply not enough. Expert cybercriminals try to actively find passwords. Multi-factor Authentication (MFA) acts as an additional layer of security to prevent unauthorized users from accessing accounts, even when the password has been stolen. Organizations use multi-factor authentication to validate user identities and provide quick and convenient access to authorized users.

What is Multi-Factor Authentication?

- Multi-Factor Authentication (MFA) is a layered approach to securing data and applications where a system requires you to provide combination of two or more authenticators to verify your identity before the service is granted.

There are three authentication factors:

- Something you know (Password)
- Something you have (Key fob, One Time Password)
- Something you are (Biometrics)

Why Multi-Factor Authentication (MFA) is so important?

- Multi-Factor Authentication (MFA) makes it more difficult for a threat actor to gain access to information systems, such as email, billing systems and/or electronic health records, even if passwords are compromised through phishing attacks or other means.
- Multi-Factor Authentication (MFA) adds a strong protection against account takeover by greatly increasing the level of difficulty for adversaries.

Purpose:

The purpose of this memo is to notify all Therap administrators that the South Carolina Department of Disabilities and Special Needs (DDSN) requires all users logging into the Therap Electronic Health Records system to use MFA.

Violation:

Any Therap administrator that is found in violation of disabling a user’s MFA requirements, whether proactively or during unrelated audits will be subject to loss of administrative access privileges.

Thank you for your prompt attention to this matter as we continue to protect South Carolina Department of Disabilities and Special Needs information assets and consumers privacy from cyber-attacks.

If you have any questions, please call the IT Help Desk at (803) 898-9767.