Multi-Factor Authentication Use Case Description

American Medical Solutions, Inc. (AMS) has implemented “multi-factor authentication” (MFA) into our practice management / EHR solution Helios.

MFA is used in various parts of our system. All users (patients and internal clinic users) have MFA enabled for logging in. Username, password and a secure email or text message to the user’s phone is sent depending on the users’ preferences. A code is sent and must be entered within the allotted 3 minutes of creation. If the code is not entered or entered incorrectly or not within the timeframe allotted, access will be denied.

MFA is also used when signing / approving encounter notes. Providers are given the ability to sign and once triggered by the signing process, a code is sent to the providers phone or email depending on preferences. A code is sent and must be entered within the allotted 3 minutes of creation. If the code is not entered or entered incorrectly or not within the timeframe allotted, approval will be denied, and the clinic administrator is sent a message of incorrect authentication.

MFA is also used when providers are prescribing controlled substances. AMS has partnered with Exostar, an approved vendor for EPCS authentication. The Exostar application is loaded on the authorized user’s phone. Once the prescription for the controlled substance is triggered, a code will appear on the Exostar application providing a code to be entered. A code is sent and must be entered within the allotted 30 seconds of creation. If the code is not entered or entered incorrectly or not within the timeframe allotted, approval of the prescription will be denied, and the clinic administrator is sent a message of incorrect authentication.