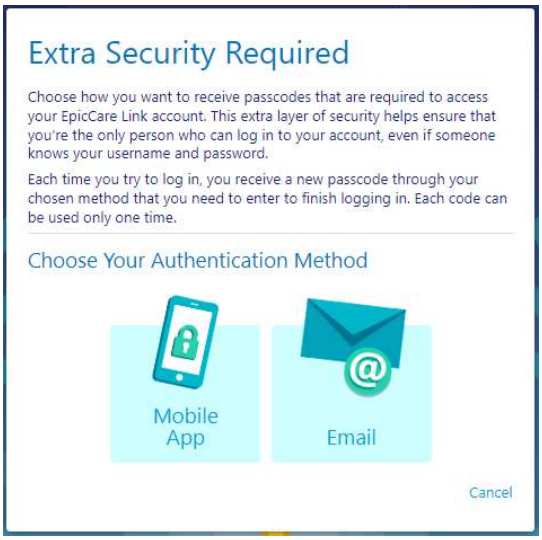
TWO-FACTOR AUTHENTICATION

Two-factor authentication requires community users to enter their standard username and password plus a randomly generated one-time passcode to log in. When two-factor authentication is enabled, even if a malicious user managed to acquire a community user's credentials, user still couldn't log in without also having the community user's one-time passcode.

- When a community user logs in for the first time, user will be prompted to choose a method of receiving the randomly generated passcodes.
- User can choose to use email, text messages, or an authenticator application on their mobile device.
- After user chooses a method, on-screen prompts guide to set it up.
- The next time user attempts to log in, the system sends user a one-time passcode using the method they selected and prompts user to enter that passcode.



- When a community user first sets up two-factor authentication, user also receives a code that can use to reset the two-factor authentication settings. For example, if user replaces her smartphone, user can use this reset code from the login screen to set up two-factor authentication with new phone.

	When a community user is logged in to MLH EpicCare Link, they can change the two-factor authentication settings using the Reset Additional Authentication page on the Settings menu. There is a limited number of times that a user can enter an invalid passcode or reset code before the user is blocked from the web application. If that happens, contact your Site Administrator to open a Help Desk Ticket with MLH EpicCare Link support team.