



Epividian uses an adaptive multi-factor framework to support the strongest possible authentication in order to obtain access to our applications. All users are required to use multi-factor by default to access the Epividian CHORUS portal and mobile app.

The screenshot shows the Epividian logo in the top left corner. The main heading is "Select a Two-Factor Authentication Method". Below this, there is a section titled "Two Factor authentication Setup" with a sub-heading "In order to protect patient health information, we have configured your account to utilize two-factor authentication each time you change your CHORUS portal password, including on the first login. This two factor authentication process will link together your CHORUS login with a Personal Authentication Code. This provides superior security because we're combining a shared secret (your login and password) with something you have in your possession (a phone with a unique code). More questions about this? Please e-mail us at [support@epividian.com](mailto:support@epividian.com)." Below this text, there is a prompt: "Please select a Two Factor Authentication method to use with your account". There are two radio button options: "Text Message" (which is selected) and "Time Based One-Time password (TOTP) using an app on your mobile device". The "Text Message" option has a description: "Using this method, you will need to supply us your mobile phone number to store with your user account. Each time you are prompted for your Two Factor Authentication Code, we will send you your code via text message to your mobile phone. You will then need to enter the code from your phone into the provided text box. Note, your mobile phone carrier may charge you a fee for receiving the text message we send you depending on your text messaging plan." The "Time Based One-Time password (TOTP) using an app on your mobile device" option has a description: "Using this method, you will install a free app on your Android or Apple device, and sync the application with the CHORUS portal. Each time you are prompted for your Two Factor Authentication Code, you will need to open the app and enter the code displayed into the provided text box on the CHORUS Portal." At the bottom right of the form, there are "Continue" and "Cancel" buttons.

The screenshot shows the CHORUS mobile app interface. At the top, there is a blue header with the time "9:36", a hamburger menu icon, and the word "CHORUS". Below the header is a "Change Password" button. The main content area has two sections: "Mobile Device PIN: Active" and "Biometrics: Active". The "Mobile Device PIN: Active" section has a description: "To protect your patients' privacy, this app requires you to reauthenticate each time you navigate back to it, even if you left it open. You can use a PIN that you create to speed this process up if you have not closed or signed out of the app." Below this description are "Change PIN" and "Deactivate PIN" buttons. The "Biometrics: Active" section has a description: "To protect your patients' privacy, this app requires you to reauthenticate each time you navigate away and return after a period of 10 minutes or more, even if you left it open. If your organization allows, you can use biometrics to speed up the authentication process." Below this description is a "Deactivate Biometrics" button. At the bottom of the screen, there is a navigation bar with four icons: "Schedule", "Huddle", "Outreach", and "Surveys".

Epividian requires two-factor authentication using a time-based one-time-password algorithm delivered through an authenticator app, such as Google or Microsoft, or delivered to the user via SMS. Two-factor authentication is required for all password changes and is required on login attempts exceeding 31 days or when the system detects access originating from an IP address, computer, and/or browser not previously used to access the CHORUS portal within a 31-day period.