Why does SimpleLTC use Multi-Factor Authentication (MFA)?

At SimpleLTC, we’re often asked what Multi-Factor Authentication (MFA) is, why it’s an option at SimpleLTC, and the pros and cons of enabling it for Simple solutions. This document outlines the reasons for using MFA and how it can help to protect your organization’s critical healthcare data.

## What is MFA?

MFA is a secondary security protocol for accessing a specific website or application, and is often set up using SMS, email, or a smartphone app such as Authy or Google Authenticator. It provides additional security beyond just a username/email address and password. You’ll often encounter MFA when dealing with healthcare, HIPAA, government entities, banks, and other applications that utilize personal information.

## How does Simple use MFA?

SimpleLTC utilizes an SMS service called Twilio for our MFA. A six-digit code is sent to the user once they sign into our application (assuming a valid mobile phone number is in the user’s profile). For now, we offer MFA as an optional feature, as some companies utilize a company SSO (single sign-on) that authenticates their access to our website and is controlled by their company. Other providers don’t allow mobile devices on-premises, so the option to receive a text message is not possible for every organization.

However, we encourage all users with access to a mobile phone to enable MFA, as it adds additional security for those who regularly work with government entities and the PHI of individuals in facilities.

## Pros and cons of MFA

The benefits and drawbacks of MFA often come down to accessibility versus security.

End users sometimes find MFA cumbersome because they must receive and enter a new six-digit code every time a SimpleLTC website session expires. For security purposes, we have a set timeout for application sessions, which means that some users may have to log in and reauthenticate multiple times per day.

Some users may be concerned that their personal mobile phone number could be accessible to other users on our application. To ease this concern, only users who have a defined security role within our application can view users’ personal information, including mobile phone number. This is done intentionally to protect private information.

Another possible concern is downtime with Twilio, our SMS provider. Though outages can happen, Twilio has historically been highly responsive about finding and fixing any service outages. Because Twilio is a third party, SimpleLTC cannot always guarantee that SMS messages are always received in a timely manner. However, we regularly monitor the health of Twilio and will alert our users should an outage occur.

When considered in the context of healthcare data security, however, these concerns are minor. Data security for healthcare providers is extremely important. Should an email/password be leaked or hacked from an end-users account, the results could be catastrophic for a healthcare provider, resulting in leaked PHI, deleted or broken data, or security breaches from end-user accounts. MFA is an important additional layer of security that allows us to increase data security by verifying that the person accessing our website should indeed be granted access.

## Recommendations for MFA

All in all, MFA is highly recommended for all users of Simple solutions to ensure we’re all doing our part to protect PHI and abide by HIPAA regulations. For further questions, please reach out to our SimpleLTC [Support Team](https://www.simpleltc.com/support/). They’ll be happy to address any concerns.