Service. Technology. Innovation.

Dear STI Cloud Client,

STI has begun the implementation of Two-Factor Authentication in our Cloud environment. Two-factor authentication (or two-step authentication) is an important security measure that adds a second layer of protection in addition to your password. Adding this additional security layer makes it much harder for hackers to break into your accounts as well as complying with The Health Insurance Portability and Accountability Act (HIPAA) regulation. HIPAA requires covered entities to verify that a person seeking access to electronic protected health information (ePHI) has authorization. This is how two-factor authentication (2FA) works and why implementing it will dramatically improve your digital security in the STI Cloud environment.

How does 2FA work?

Two-factor authentication works by adding an extra layer of security to your account — an additional login step — to prevent someone from logging in even if they have access to your password.

When you sign into any of your online accounts, the basic level of authentication requires only your password to log in — that's one step to verify your identity. 2FA adds a second piece of information (or a second layer) that you need to provide before you can get access to your account.

STI will be deploying a product named Duo which is a two-factor authentication (2FA) app that you will install on your smartphone. Another advantage of utilizing 2FA in the STI Cloud environment is that you will no longer need to create a new password every 90 days. You will be able to use a permanent login password.

As we rollout this new security feature, please be on the lookout for more information from us, including instructions for installing the Duo product and using 2FA at your practice.

Sincerely,
STI Computer Services