How does DrChrono keep my information safe?

07/08/2024 7:54 pm EDT

DrChrono Security Measures

DrChrono understands the importance of the security of your information. DrChrono uses nothing but the most secure servers to ensure your information is stored, and protected to the highest of standards. We store all of your information in a HIPAA-compliant SSAE 18 SOC 1 and SOC 2 data center and while you are accessing your information, the data is transported to your device via the secure HTTPS communication protocol. DrChrono uses Amazon Web Services (AWS) for data storage. DrChrono's data is stored in the United States in AWS' Northeast Data Center Region in Virginia.

What does HIPAA stand for and why is it important?

HIPAA - Is the Health Insurance Portability and Accountability Act. It is a requirement of all healthcare providers enacted in 1996 that regulates the interchange of private patient data to help prevent unlawful disclosure or release of their medical information.

There are 7 requirements that make something HIPAA compliant.

1. **Transport Encryption**: Is always encrypted as it is transmitted over the internet.

2. **Backup**: Is never lost, i.e. should be backed up and can be recovered.

3. **Authorization**: Is only accessible by authorized personnel using unique, audited access controls.

4. **Integrity**: Is not tampered with or altered.

5. **Storage Encryption**: Should be encrypted when it is being stored or archived.

6. **Disposal**: Can be permanently disposed of when no longer needed.

7. **Omnibus/HITECH**: Is located on the web servers of a company with whom you have a HIPAA Business Associate Agreement (or it is hosted in-house and those servers are properly secured per the HIPAA security rule requirements).

To learn more about HIPAA compliance click here.

So, what are SSAE 18 SOC 1 and SOC 2?

SSAE 18 (Statement on Standards for Attestation Engagements) is an internationally recognized third-party assurance audit designed for service organizations. Section No. 16 addresses examination engagements undertaken by a service auditor to report on controls at organizations that provide services to user entities when those controls are likely to be relevant to the user entities' internal control over financial reporting.

Service Organization Control (SOC) - These are internal control reports on the services provided by a service organization providing valuable information that users need to assess and address risks associated with an outsourced service.

SOC 1 & 2 - These are auditors reporting methods that have specific control objectives and criteria to report on SSAE 18.

Having these standards in place makes sure that your information is being securely stored, and regulated to the standards set by the AICPA.

Please Note: No information is stored locally on your iPad or computer. It is stored in the cloud and accessed that way. Only the information you export out while signed in to your DrChrono account can be stored locally at the location of your choice. Once you export the information from DrChrono it is your responsibility to store it in a HIPAA-compliant manner.

Your Responsibility: Help Us Keep Your Data Secure

While we employ many security measures, there are security issues outside our control that we ask our users to take the necessary precautions to.

- Keep your login credentials to yourself
- Activate two-factor authentication (2FA) on your DrChrono account
- Keep your devices malware free
- Do not install software, plugins, or add-ons that may compromise your account security
- Use only secure networks
- If you download information from DrChrono, employ all necessary security measures to safeguard that data, including but not limited to password-protecting your computer, encrypting your device, and restricting access to your local account.