How is my information kept secure?

07/08/2024 7:46 pm EDT

We at DrChrono (the developers of OnPatient) understand the importance of protecting your information. DrChrono uses only the most secure servers to ensure your information is stored and protected to the highest standards. We store all of your information in a HIPAA-compliant SSAE 16 SOC 1 and SOC 2 data center.

What does HIPAA stand for, and why is it important?

HIPAA is the Health Insurance Portability and Accountability Act. It was enacted in 1996 and requires all healthcare providers to comply with it. The act regulates the interchange of private patient data to help prevent the unlawful disclosure or release of medical information.

There are 7 requirements that make something HIPAA compliant.

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

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

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

4. **Integrity**: It is not tampered with or altered.

5. **Storage Encryption**: It 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 16, SOC 1, and SOC 2?

SSAE 16 (Statement on Standards for Attestation Engagements) - This 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 user entities' internal control over financial reporting. To learn more, click here.

The Standard for Attestation Engagements No. 16 effectively replaced SAS 70 on June 15th, 2011.

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 for reporting on SSAE 16. To learn more about this, click here.

Having these standards in place ensures that your information is securely stored and regulated according 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.