



HIPAA | Data-Processing & Security

Multiple levels of technology safeguards have been put in place. SiteRx extracts the data from the provider's EHR system through an end-to-end secure channel.

Hardened Security

Processing of the data takes place in two steps, all in transit, in memory - as a first step, a copy of the data gets pushed to an end-to-end encrypted vault, managed by a leading industry provider - TrueVault.

Identity and Access Management

Only SiteRx's Privacy Officer of SiteRx will have direct access to this data, as mandated by HIPAA. As a second step, all identifiable information (18 elements as specified by HIPAA) are removed from this data and then pushed to a secure database, which again is fully access restricted.

Exceeding HIPAA Compliance

SiteRx's machine learning algorithms only run against this de-identified data to come up with accurate trial recommendations.

To make sure that all requirements to satisfy HIPAA compliance are met, SiteRx does the following:

- PHI is fully encrypted, both at rest and in-transit.
- Controlled access to PHI data by only one SiteRx employee
- Only de-identified data is used for analytical purposes
- End-to-end, secure encryption during transmission

Any questions or concerns should be directed to SiteRx's CTO, Manoj Pooleery - email: manoj@siterx.health.



Hardened Security

Sensitive data is encrypted immediately and is protected in transit and at rest, exceeding HIPAA requirements.



Identity & Access Management

Identity & access are controlled and limited to SiteRx's Privacy Officer.



Exceeding HIPAA Compliance

All PHI is stored according to the HIPAA physical and technical safeguards.