



## HIPAA | Data Processing & Security

SiteRx's HIPAA-Compliant platform is designed to exceed data from the provider's EHR system through a secure channel. Multiple levels of technological safeguards have been put in place to keep all private health information safe.



### Hardened Security

As a first step in data processing a copy gets pushed to an encrypted vault, managed by a leading industry provider TrueVault. In the second step, all data is de-identified before being used to match patients with relevant studies.

### Identity and Access Management

Only SiteRx's Privacy Officer will have direct access to this data, as mandated by HIPAA. All other processing takes place using de-identified data (after removal of 18 elements as specified by HIPAA). Any and all access to this data is through secure, encrypted programmatic interfaces.

### Exceeding HIPAA Compliance

SiteRx's machine learning algorithms only run against this de-identified data to produce accurate trial recommendations. Importantly, SiteRx security protocol is audited by 3rd party HIPAA specialist, Accountable.

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

- PHI is fully encrypted, both at rest and in transit
- Access to PHI data is restricted to SiteRx's Privacy Officer
- Only de-identified data is used for analytical purposes

More detailed questions can be directed to SiteRx CTO:  
Manoj Pooleery | [Manoj@SiteRx.com](mailto:Manoj@SiteRx.com)