Data Retention Policy

As required by state and federal record retention requirements including HIPAA, the following policy is used to support data retention laws.

This policy, and associated procedures for data retention, has been subcontracted to a third-party, Platform as a Service, HIPAA compliant vendor (PaaS Subcontractor). We have verified that their policies and procedures meet or exceed our standards and those of HIPAA and the HITRUST Common Security Framework. As such, we have assurances that strong intrusion detection tools and policies to proactively track and retroactively investigate unauthorized access are used.

Proof of such due diligence is kept by the Security Officer.

State Medical Record Laws

- Listing of state requirements for medical record retention

Data Retention Policy

- Data is stored on PaaS Subcontractor systems as part of subcontracted service.
- Once we cease to be a Customer, as defined below, the following steps are taken:
    1. Either reinstate the account, if deemed appropriate or necessary.
    2. If we do not wish to reinstate account, we will download all data in a secure and encrypted manner.
    3. Otherwise we can request for the existing PaaS Subcontractor to retain backups of existing data for a negotiated price.
    4. After data has been removed from PaaS Subcontractor's servers, both parts will ensure the *Disposable Media Policy* and all other applicable policies will be followed. As such, no trace of data shall be allowed to remain after leaving PaaS Vendor.