Together Senior Health’s (TSH’s) data security standards for storage and viewing of class video recordings follow these data protection standards:

Online Storage:

* Class video recordings are stored in the cloud. All data is encrypted at rest
* Data stored in on-line cloud storage which does not provide direct access to the files by users. Users can only stream data directly from cloud storage and cannot easily download videos.
* Streaming access to video is controlled from within our application using RBAC (Role-Based Access Control) to limit access to those user’s whose job function require review of the videos for training, research, compliance, and safety purposes
* Data is encrypted in-motion (during streaming and moving to off-line storage) via HTTPS
* Roles which have access to class video recordings via streaming for training, research, compliance, and safety purposes must use 2FA
* Administrative accounts which have direct access to cloud storage for system administration purposes must use 2FA
* To implement a least privilege access control principal, separate administrative accounts are used to manage private participant data
* Private participant data is segregated from other data to facilitate least privilege access and reduce the possibility of accidental exposure of private data

Offline Storage:

* Data is migrated to off-line storage based on time, usage patterns, and business need
* Data is retained for a period of five years
* All off-line storage is encrypted at rest
* Data in motion between on-line and off-line storage is encrypted via HTTPS
* Administrative accounts which have direct access to retrieve data from off-line cloud storage use 2FA

Direct access or distribution files for other purposes:

* All access to class video files for non-training and research purposes must be approved by the TSH Data Custodian who is responsible for reviewing the use in light of contractual, compliance, and privacy requirements. This review verifies that the proper releases have been obtained, and that recipients have executed the necessary confidentiality and privacy agreements. The Custodian also ensures that secure storage and transmission mechanisms are used for any transfer of data.
* Direct access to files in cloud storage other than for protected streaming is prohibited. For any other access, only that data specifically required to fulfill the needs of the approved purposes will be made available.

While the specific choice of cloud storage and other technologies are subject to change due to evolving technologies and business requirements, the following specific storage and security technologies, as governance policies are currently used:

* Class video recordings are delivered directly to S3 by our CpaaS (Communication Platform as a Service) Video platform
* On-line class video recordings are stored in AWS S3 object storage, Amazon S3-managed keys (SSE-S3) to encrypt the data at rest using the AES-256 algorithm.
* Off-line class video recordings are stored in AWS S3 Glacier object storage where the data is encrypted at rest using the AES-256 algorithm
* Administrative accounts for management of AWS S3 data use AWS RBAC (Role-Based Access Control) with 2FA (Two Factor Authentication) enabled
* Streaming access passwords are managed and validated by our cloud-based IAM (Identity and Access Management) provider Auth0.
* All user accounts which permit streaming access to class video recordings have 2FA (via SMS or push notifications) enabled
* The role of Data Custodian is shared between the CEO and CTO; the CEO must review and approve all data access outside of TSH, and the CTO reviews all data transfers to ensure appropriate security protections are used