



■ Compliant with Privacy & Security Standards

Under the Health Insurance Portability and Accountability Act (HIPAA), Unite Us is a Business Associate to Covered Entities utilizing the software platform. Since 2013, Unite Us has made it a priority to implement controls necessary to maintain the confidentiality and integrity of Protected Health Information (PHI) and Personal Identifiable Information (PII) stored in the system. This includes but is not limited to patient/user rights and technical, physical, and administrative safeguards to mitigate possible incidents or breaches.

Additionally, Unite Us follows the Health and Human Services (HHS) guidelines on Breach Notification and Breach Enforcement procedures established via the Health Information Technology for Economic and Clinical Health Act (HITECH 2009).

Through internal Security Awareness Training and policies and procedures provided to Unite Us team members, it is continually communicated how to maintain HIPAA compliance, investigate and communicate a breach, and perform risk mitigation. Upon completion of the training, team members are required to pass an assessment acknowledging their commitment to compliance at Unite Us.

■ HIPAA, FERPA, & FIPS Compliant

Unite Us has implemented extensive standards that apply cross-functionally to Family Educational Rights and Privacy Act (FERPA 1974) and Federal Information Processing Standards (FIPS) compliance. The technical infrastructure and administrative safeguards are reviewed on a quarterly and as needed basis to ensure consistency and the timeliness of the implementation of additional and preventive improvements.

■ Secured, Encrypted Technical Infrastructure

Unite Us is securely managed on HIPAA compliant servers in a leading high-density data center with SAS-70 Type II certifications via Amazon Web Services (AWS). Safeguards include: 24-7 video surveillance, physical locks, and structured access controls. Through AWS, the best professionals in the industry protect data stored within the platform while the technology team at Unite Us continuously monitors access and activity. Data is encrypted at rest and in transit, while backups are performed throughout the day without interruption to service and are encrypted and stored within the S3 AWS platform. Business Associate Agreements (BAAs) have been signed with all third party technical partners.

■ Access Controls

During the onboarding process into Unite Us, all users must request access to the system; identifying their role and associated permissions prior to entering the system. Once level of access has been approved by the authorizing party, users are provided a unique username and password to enter the system. Their access to information is based on their role and permissions. Internally, Unite Us provides each employee with only the necessary level of access into the system and continuously monitors activity.