HIPAA Compliance Data-sheet

HIPAA Compliance

The Health Insurance Portability and Accountability Act and supplemental legislation collectively referred to as the HIPAA rules (HIPAA) lay out privacy and security standards that protect the confidentiality of protected health information (PHI).

The general requirements of HIPAA Security Standards state that covered entities must:

1. Ensure the confidentiality, integrity, and availability of all electronic PHI the covered entity creates, receives, maintains, or transmits.
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the privacy regulations.
4. Ensure compliance by its workforce.

How PsyPack Enables HIPAA Compliance

The following table demonstrates how PsyPack supports HIPAA compliance based on the HIPAA Security Rule published in the Federal Register on February 20, 2003 (45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule).

HIPAA Standard	How PsyPack Supports the Standard
Access Control	
• Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to authorized persons or software programs. • Unique User Identification: Assign a unique name and/or number for identifying and tracking user identity. • Emergency Access Procedure: Establish (and implement as needed) procedures for obtaining necessary electronic health information during an emergency. • Automatic Logoff: Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. • Encryption and Decryption: Implement a mechanism to encrypt and decrypt electronic protected health information.	• Data is encrypted at the application layer using Advanced Encryption Standard (AES). • Multi-layered access control for practitioners and clients. • Web and application access are protected by verified industry-standard authentication. • Unique numbers are assigned to practitioners and clients for identifying and tracking identity. • Access to assessment reports is protected by authentication. • Practitioners control if the client reports are accessible to the clients. • Practitioners and clients are automatically logged off, on account of inactivity.
Audit Controls	
• Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	• Data is stored and processed on secure and compliant infrastructure with annual audits for SSAE16 / ISAE 3402 Type II, ISO 27001, ISO 27017, ISO 27018, FedRAMP ATO, and PCI DSS v3.2.1. (https://cloud.google.com/security/compliance/hipaa) • PsyPack has earned and ISO 9001:2015 and ISO 27001:2011 certifications.

Integrity	
• Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	• Multilayer integration protection is designed to protect both data and service layers. • Access controls are implemented using Identity and Access management, Audit logs, Backups and Alerts. • Controls are in place to protect and encrypt data.
Integrity Mechanism	
• Mechanism to authenticate electronic protected health information. • Implemented methods to corroborate that information has not been destroyed of altered.	• SSL certificate is used authenticate web-app's identity and enable an encrypted connection between web browser and server. • Data connections leverage TLS 1.2 encryption. • Email communication uses PKI Certificates issued by a trusted commercial certificate authority. • Web and application access are protected by industry-standard authentication.
Person or Entity Authentication	
• Verify that the person or entity seeking access is the one claimed.	• Web and application access are protected by industry-standard authentication. • Practitioners are required to submit a self-declaration and proof of legal and jurisdictional competence. • Practitioners can restrict access of assessment reports to the clients.
Transmission Security	
• Protect electronic health information that is stored on the PsyPack platform. • Integrity controls: Ensure that protected health information is not improperly modified without detection. • Encryption: Encrypt protected health information.	• Data encryption protects against passive and active attacks on confidentiality. • Data connections leverage TLS 1.2 encryption and PKI Certificates issued by a trusted commercial certificate authority. • PsyPack employs AES 256-GCM encryption for data to protect health information.