unlocking potential

CLOUD SECURITY & COMPLIANCE STANDARDS

for Western Psychological Services

At WPS, your privacy is very important to us.
PLEASE READ THE FOLLOWING CAREFULLY.

625 Alaska Avenue, Torrance, CA 90503
t 800.648.8857 or 424.201.8800
f 424.201.6950

compliance@wpspublish.com
wpspublish.com

JUNE 2021 V 1.0

Security is built in throughout the WPS e-commerce website and the Online Evaluation System.

Maintaining a secure infrastructure and environment that safeguards data and protected health information (PHI) is our highest priority for our customers. This document will focus on the architecture and security that are employed by WPS to safeguard such data.

Before you get started, we recommend you review our Terms of Use and Privacy Policy.

625 Alaska Avenue, Torrance, CA 90503
t 800.648.8857 or 424.201.8800
f 424.201.6950
compliance@wpspublish.com
wpspublish.com

In terms of environment security, WPS is hosted in redundant, state-of-the-art Amazon Web Services (AWS) data centers located within the USA.

What Is AWS?

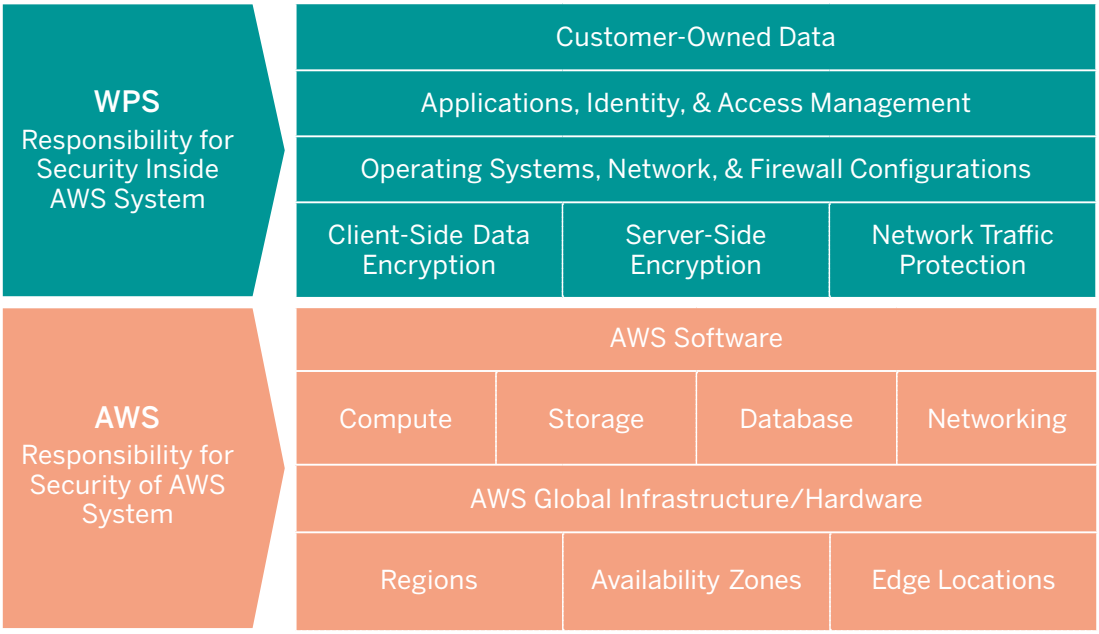
AWS is a secure platform offering computing power, database storage, content delivery, and a variety of other services designed for scalability, resilience, and security. More information about AWS's cloud computing can be found here.

AWS & WPS'S Shared Compliance Responsibility

AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates.

WPS, like any other AWS customer, manages and has responsibility for the guest operating system (including updates and security patches), the WPS sites, and the configuration of the AWS-provided security modules.

In summary, AWS is responsible for the security of the cloud system, and WPS is responsible for the security of the data it stores in the cloud. More details can be found here for the AWS Shared Responsibility Model.



Security & Compliance Standards

From an AWS hosting perspective, the key certifications include:

- SOC 1, 2, & 3
- ISO 270001
- FedRAMP
- FERPA
- CSA
- NIST

AWS allows organizations subject to the U.S. Health Insurance Portability and Accountability Act (HIPAA) to process, maintain, and store protected health information. More information can be found here: AWS HIPAA Information.

WPS is happy to provide security and compliance reports and certifications produced by third-party auditors, which attest to the design and operating effectiveness of the AWS environment. You can read more about AWS Compliance Programs here.

Network Security

Secure Network Architecture

Network devices, including firewalls and other boundary devices, are in place to monitor and control communications at the external boundary of the network and at key internal boundaries within the network. These boundary devices employ rule sets, access control lists (ACLs), and configurations to enforce the flow of information to specific information system services.

Database and application servers are protected by a firewall to ensure that no unauthorized traffic can reach the servers. Access to the servers is also restricted to approved IP addresses and requires a private key authentication.

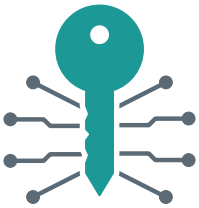
Isolation is achieved through the use of a virtual private cloud (VPC). It becomes a secure network, distinct and separate from the network where our desktop workstations and users on our internal network reside. This makes it much harder for viruses to reach or impact our production network.

Data Encryption

WPS leverages AWS for data encryption in transit (TLS) and at rest (AES-256). WPS currently uses the ELBSecurityPolicy-FS-1-2-Res-2020-10 Security Policy on AWS Application Load Balancers and within AWS CloudFront.

WPS uses the AWS Key Management Service (KMS) to enable data at rest encryption across our products. We use this for encrypting data within databases (RDS), and data stored within S3.

Whether at rest or in transit, we have the capability to provide the highest level of security and encryption to protect the confidential and personal information you entrust to us. This includes strong public/private secret keys and key management systems.



Secure Access Points

AWS has strategically placed a limited number of access points to the cloud to allow for a more comprehensive monitoring of inbound and outbound communications and network traffic. These customer access points are called API endpoints, and they allow secure HTTPS access. In addition, AWS has implemented network devices that are dedicated to managing interfacing communications with Internet service providers (ISPs).

Transmission Protection

You can connect to an AWS access point via HTTPS using Secure Sockets Layer (SSL), a cryptographic protocol that is designed to protect against eavesdropping, tampering, and message forgery.

Network Monitoring & Protection

AWS utilizes a wide variety of automated monitoring systems to provide a high level of service performance and availability. AWS monitoring tools are designed to detect unusual or unauthorized activities and conditions at ingress and egress communication points. These tools monitor server and network usage, port scanning activities, application usage, and unauthorized intrusion attempts. WPS also employs IDS/IPS systems on the corporate network outside of AWS infrastructure.

The AWS network provides significant protection against traditional network security issues such as:

Distributed Denial of Service (DDoS) Attacks

AWS API endpoints are hosted on large, Internet-scale, world-class infrastructure that benefits from the same engineering expertise that has built Amazon into the world's largest online retailer. Proprietary DDoS mitigation techniques are used. Additionally, AWS's networks are multi-homed across several providers to achieve Internet access diversity.

Man-in-the-Middle (MITM) Attacks

All of the AWS APIs are available via SSL-protected endpoints, which provide server authentication.

IP Spoofing

The AWS-controlled, host-based firewall infrastructure will not permit an instance to send traffic with a source IP or MAC address other than its own.

Port Scanning

When unauthorized port scanning is detected by AWS, it is stopped and blocked. Port scans of Amazon EC2 instances are generally ineffective because, by default, all inbound ports on Amazon EC2 instances are closed and are only opened by customers.

Business Continuity & Disaster Recovery

Data Backups & Retention

Data backups are run multiple times throughout the day, as well as replicated to other AWS regions for redundancy and recoverability. WPS maintains seven years of backups. These backups are stored encrypted in accordance with the Data Encryption section listed above.

Restoration tests are performed every two months to ensure recoverability.

Redundant & Resilient Architecture

WPS engineers have designed a highly scalable and resilient product architecture within AWS. Our product withstands sophisticated attacks and is highly adaptable. Our systems' performance within the product architecture is monitored for key metrics, ensuring the load on any one system is within an acceptable range. Should any components become overloaded or experience a fault, automated processes will be executed to bring additional temporary systems online or to cycle out existing systems for new ones.

Automation is built into the WPS architecture, so system monitoring, updates, and corrective actions can take place as needed with no downtime.

Application, Server, & Endpoint Security

Vulnerability Management

Complete annual third-party penetration testing on the live environment is performed by external security experts, whose recommendations are constantly implemented within the product and the environment.

The WPS Infrastructure Team performs web application vulnerability scans every two months. Vulnerabilities are remediated in accordance with the schedule listed below.

Vulnerability Severity	Critical	High	Medium	Low
Remediation Timeline	<2 Weeks	<2 Weeks	Discretionary	Discretionary

All OS or other back-end patches are applied immediately for critical security patches and within 7 to 14 days for non-security patches. Security audits of the server logs are performed on a periodic basis.

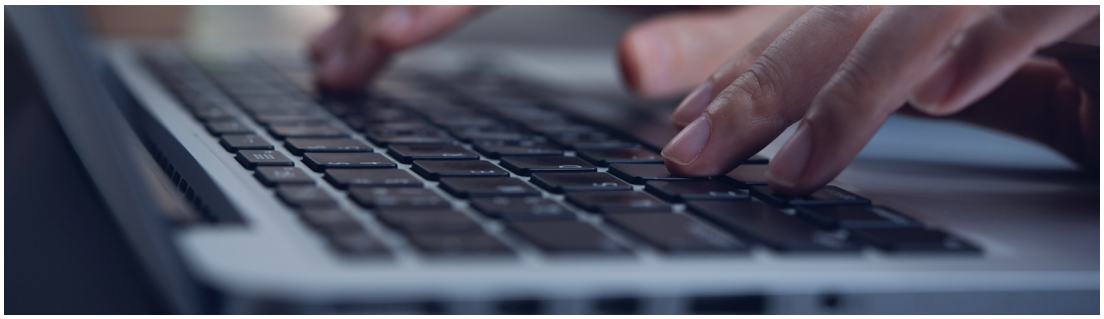
Code Security & Code Updates

The WPS Development Team leverages a continuous integration/continuous delivery (CI/CD) pipeline for managing code deployments. Code changes are peer reviewed, approved by separate QA staff, and tested in a staging environment before they are pushed into production. The staging and production environments are logically separated, and no data is shared between them.

Regular and thorough application security testing is performed at all stages of development to ensure that the application interface cannot be exploited.

Endpoint Security

All endpoints, including servers, are protected using advanced automated threat detection and response against an ever-growing variety of threats, including fileless and ransomware.



Human Factor Security

Access to the servers is restricted to the server administrators, an approved representative of the support team, and an approved representative of the development team (access is revoked if no longer necessary).

Server logins are reviewed periodically. Any changes made to the cloud environment follow a predefined change process, including approvals.

Access & Authentication Controls

WPS restricts access to customer and confidential data on a business need-to-know basis. Access is granted based on one's role within the organization. WPS enforces mandatory multi-factor authentication for all access to confidential data. Where applicable, access to systems is restricted by IP address. SSO is also used wherever applicable.

Password complexity and expirations are based on HIPAA guidelines. No credentials are ever shared between users.

Security Awareness & Training

All WPS employees complete mandatory security awareness and privacy training upon hire and monthly going forward. We conduct simulated phishing and social engineering tests on an ongoing basis at least once a month.