Security & Compliance

How We Store, Process, and Secure Your Data

Data Centers
PharmaServ is hosted at Amazon data centers, running on Amazon Web. This data centers, located both in the US and in the EU, provide physical security 24/7, state of the art fire suppression, redundant utilities, and biometric devices to ensure your data is safe.

Network Security
We take several steps to protect your data and prevent eavesdropping between your systems and ours. All network traffic runs over SSL/HTTPS, the most common and trusted communications protocol on the Internet.

System Security
We're relentlessly updating our systems to protect your data. We regularly replace our virtual systems with new, patched ones. We maintain system consistency using a combination of configuration management, up-to-date images, and continuous deployment.

Security Operations
If we see something, we react quickly. We're always looking for potential system interruptions. If we find something out of place, we address the issue to prevent it in the future.

Restricted Access
Only people who need access, get access. We limit production-system access to key members of the PharmaServ engineering team and expressly forbid passwords.

Penetration Testing
Don't just take our word that our systems are secure. We don't. Even though we've designed secure systems and procedures, we regularly perform security tests to identify and remediate potential vulnerabilities.

Logging
Logging is a critical component to PharmaServ infrastructure, and we're monitoring the platform to identify any misuse or problems. Logging is used extensively for application troubleshooting and investigating issues. Logs are streamed in realtime and over secure channels to a centralized logging service.

Application Level Security

We prevent single points of failure. Even if there is an interruption to one system, the rest of our services stay up and secure. We physically separate the database instances from application servers and heartily believe in the mantra of single function servers.

Data Protection, Continuity, and Retention

We backup and test our systems, just in case. Production data is mirrored to remote systems and automatically backed up daily to an offsite location. Every change to a database is stored in the 'writeaheadlog' and immediately shipped offsite.

Internal IT Security

We protect our own systems to protect your data. PharmaServ offices are protected behind network firewalls from well-known security vendors and secured by keycard access. Our employee workstations and laptops are imaged and managed using JAMF.

Account Cancellation

If we have to part ways, we'll make sure your data isn't at risk. To cancel and delete your account, please contact your PharmaServ account manager. Canceling your account will disable all access to PharmaServ Platform and affects all data associated with your account.

NDPR Compliance

PharmaServ is committed to ensuring ongoing compliance with the Nigeria Data Protection Regulation (NDPR). The NDPR extends the reach of the data protection laws 2019 and establishes many new requirements for organizations that fall under its scope.

Bug Bounty

Our platform is constantly evolving to delight our customers with new features and innovation. In an effort to protect our ever-changing attack surfaces, we have implemented a bug bounty program that challenges our controls and tightens our defenses on a continuous basis.