Technical security:

We employ all the tools such as vulnerability scanning, WAF and daily log review to ensure that your data is well protected against unauthorized users. But technical safeguards are not one-size-fits-all. We'll work with you to fit the right combination of security technologies to suit your tolerance for risk, compliance obligations, and resource demands. The technical safeguards below are all included in our security packages to comply with PCI DSS standards and are a great addition to lower your risk of data loss if you need to follow HIPPA, SOC 2, or Privacy Shield guidelines.

Daily Log Review

While some providers may offer logging (tracking user activity, transporting and storing log events), we provide the complete, glorious logging experience with daily log review, analysis, and monthly reporting.

File Integrity Monitoring (FIM)

Monitoring your files and systems provides valuable insight into your technical environment and provides an additional layer of data security. File integrity monitoring (FIM) is a service that can monitor any changes made to your files so you can see if anything sneaky is going on.

Web Application Firewall (WAF)

Protect your web servers and databases from malicious online attacks by investing in a web application firewall (WAF). A network firewall's open port allows internet traffic to access your websites, but it can also open up servers to potential application attacks, such as database commands to delete or extract data sent through a web application to the backend database, and other malicious attacks. Sounds bad, right? No worries. WAF is here to save the day.

Two-Factor Authentication

We offer two-factor authentication for VPN (Virtual Private Network) access as an optimal security measure. Considered a best practice for security in general, it’s especially targeted to protect against online fraud and unauthorized access for clients that connect to their networks from a remote location.

Vulnerability Scanning

Vulnerability scanning checks your firewalls, networks, and open ports. It’s a web application that can detect outdated versions of software, web applications that aren’t securely coded, or misconfigured networks. If you need to meet PCI compliance, you’re required to run vulnerability scans and produce a quarterly report.

Patch Management

Why is patch management so important? If your servers aren’t updated and managed properly, your data and applications are left vulnerable to hackers, identity thieves and other malicious attacks against your systems. In fact, many security breaches are caused by thieves exploiting unpatched servers.

Antivirus

Antivirus software can detect and remove malware in order to protect your data from malicious attacks. Reduce your risks of data theft or unauthorized access significantly by investing in a simple and effective solution for optimal server protection. Yeah, it may be the most un-exciting cloud security tool these days, but it should never be underestimated.

SSL Certificate

In order to safely transmit information online, a SSL (Secure Sockets Layer) certificate provides the encryption of sensitive data, including financial and healthcare. An SSL certificate verifies the identity of a website, allowing web browsers to display a secure website.

Encryption

Encryption takes plaintext (your data) and encodes it into unreadable, scrambled text using algorithms that render it unreadable unless a cryptographic key is used to convert it. Encryption ensures data security and integrity even if accessed by an unauthorized user.

Ransomware protection

We offer improved protection from ransomware with data replicas of your environment. With 7 day backup protection, we ensure your data remains intact even if a malicious third party remotely wipes your backup data. Visit our cloud backup page to learn more.

Administrative security:

Outsourcing your IT needs to a third party can be daunting. Otava provides the administrative security you need in the form of contractual requirements and staff training as well as documented policies, procedures, and independent audit reports to lower your organization’s risk.

Audits and Reports

Cloud providers should maintain reports on compliance (ROC) in order to clarify which requirements they cover and which requirements your company needs to fulfill. We provide copies of our audit reports for SOC 1, SOC 2, ISO 27001, HIPAA and PCI compliance.

Policies

Our documented policies and procedures reflect our protocol in the event of a data breach in order to provide your company visibility into our notification timeline. Additionally, documentation can outline other important security standards, from how data is handled after service termination to password policies.

Staff Training

Documented policies and procedures are only effective if employees are regularly made aware of their existence and trained on them. The mishandling and misuse of sensitive data can potentially lead to a data breach. Check the last dates of employee training, and don’t be afraid to ask about hiring policies to ensure your data is in safe hands.

Business Associate Training

As a HIPAA-compliant cloud provider, we are specifically trained on how to handle ePHI. Additionally, we offer to sign and provide a business associate agreement with every healthcare client. Part of your due diligence as a covered entity includes vetting your third-party service providers and ensuring they are trained on how to prevent a data breach.