Vitature® Security

Vitature® is the cloud-based solution designed by Healthnotes® with security and privacy in mind.

Healthnotes is committed to achieving and maintaining the trust of our customers by adhering to industry best practices in securing data and ensuring personal and business privacy.

Security Highlights:

Part 11 Compliance
Digital Audit Trails
Electronic Signatures
Secure, Cloud-Based Environment

Vitature Solution:

Centralized, secure repository for all compliance data and documentation.

Cloud-based, centralized workflow for easy, secure collaboration.

Hosting

- Vitature is hosted on Amazon Web Services—the best-in-class for cloud-based solutions.
- Vitature is also mirrored to a failover environment on Microsoft Azure. Frequent updates of customer data are log-shipped to Azure, minimizing data loss in the case of a catastrophic event.

Monitoring

- Vitature is monitored externally for potential failures. Alerts are sent to technical personnel who respond quickly to troubleshoot issues and switch to Azure if necessary.

Separate Subdomains

- All Vitature customers get their own unique subdomain, allowing for greater data control and increased security.

Backup

- Data is backed up frequently each day and stored in a separate physical location, making it easy to restore in the case of a catastrophic event.

Authentication

- Microsoft Web Security is used for form-based logins, providing secure and reliable authentication.
- Passwords are stored as a one-way hash, using the latest cryptographic algorithms—this means even Healthnotes' personnel cannot determine user passwords.

Secure Access

- Vitature access is secured via SSL and TLS. This encrypts all requests to and from customer's browsers to our servers, making it impossible to decipher information "on the wire."
- An HTTP Strict Transport Security (HSTS) header is also used to protect from man-in-the-middle spoofing.

Threats

All the Open Web Application Security Project's top-10 security threats have been addressed, including the following common threats:

- SQL Injection (SQLi): SQLi protection is provided by our proprietary data adapter layer and parameterized queries. All data is accessed though this layer, eliminating the possibility of SQLi hack attempts.
- Cross-Site Scripting (XSS): Script is not allowed in entry fields, and all requests are validated via ASP.NET request validation, eliminating the possibility of an XSS attack.
- Cross-Site Request Forgery (CSRF): All client-server requests use anti-forgery tokens to ensure they are being made from the correct source.

Additional Resources

Supplier Portal Cloud Services Agreement: https://www.healthnotes.com/spcsa/
Cloud Hosting and Delivery: https://www.healthnotes.com/hchp/
Cloud Services Agreement: https://www.healthnotes.com/hcsa-2/
Privacy Policy: https://www.healthnotes.com/hpp/