

Lippincott Solutions Infrastructure Improvements

FAQs

Q: Is the Lippincott Solutions hosted data stored securely?

A: Yes, all communication is via HTTPS and all data is regularly backed up and stored in the cloud (AWS). Additionally, our database encryption is strengthened at rest and in transit.

Q: Is data backed-up securely? Describe the security involved in data archival?

A: The Lippincott Solutions applications run on a load-balanced cluster, with the database having read and write replicas and failovers and data storage using at least AES 256 encryption. Our database, servers, and filesystems are actively replicated across multiple availability zones and regions through our cloud service provider (AWS).

Q: How often are the Lippincott Solutions software platforms updated?

A: Throughout the year, our quarterly content and software releases are proactively put through Quality Assurance testing *prior* to any deployment or release to our customer base.

Q: How well is the Lippincott Solutions application architecture compared to best industry practices and latest technology and trends?

A: Lippincott Solutions uses state-of-the-art technology in a Web-based/Cloud environment to ensure that information is protected. There are redundant back-up servers geographically separated to mitigate risk from natural disasters; typical downtime is less than 1%, with Apple iOS and Google Android mobile application available for customers to access content during hospital power outages.

Q: What is the retention period of the data in the application?

A: Data in the Lippincott Solutions' applications is retained throughout the lifetime of the contract with Lippincott, unless facility administrators choose to delete content manually.

Q: Does Wolters Kluwer encrypt all data at rest and in motion with a minimum standard of 128-bit fixed block cipher?

A: Yes. Lippincott Solutions utilizes a minimum of AES-256 encryption in transit and at rest.

Q: Does Wolters Kluwer have a business continuity plan and a disaster recovery plan for contingency operations in the event of a disaster or other adverse event?

A: Yes.

Q: Will or does Wolters Kluwer store all customer data within the United States, including backup data?

A: Yes.

Q: Does Wolters Kluwer perform third party external information security assessments (e.g., internal and external penetration testing, vulnerability assessment, and/or PCI assessment)?

A: Yes.

Q: Does Wolters Kluwer maintain all applications, servers and network equipment up to date with the latest patches and updates?

A: Yes.

Q: Does Wolters Kluwer follow a full change management process for all changes to the production environment, including enforcing appropriate segregation of duties?

A: Yes.

Q: Is all network traffic over public networks to the production infrastructure sent over cryptographically sound encrypted connections? (e.g., TLS, VPN, IPSEC, etc.)

A: Yes.

Q: Does the application execute an automatic log-off after a period of inactivity? What is the duration of time until the application logs users off?

A: Yes, the application will log-off users due to inactivity after 30 minutes.

Q: What is the accessibility of the solution (within the Client network, outside the network, multiple devices, etc.)?

A: Lippincott Solutions provides numerous access points, including: EMR, Learning Management System, desktop, workstations on wheels, intranet, home, and mobile apps.

Q: What is the maximum number of concurrent users?

A: Individual user credentials may only be accessed by two (2) concurrent users at a time. Institutions may add unlimited users within their authorized/subscribing facilities.

Q: Does your application use Active Directory for authentication?

A: No, Lippincott Solutions uses IP authentication as our primary authentication method. Also, we can enable username and password log-in, Athens authentication, web referral, or trusted entry point as additional/alternative authentication methods.

Q: Does the application have a “thick client” or is it web-based?

A: The Lippincott Solutions’ software platform is a web-based, thin client, and also a native mobile application for Apple iOS and Google Android devices.

Q: Is the application accessible to remote users?

A: Yes. In addition to being granted user credentials, users can access Lippincott Solutions via remote web referral or trusted referral authentication.

Q: Does the audit/activity log show changes made by administrators to the system (e.g., user account added/deleted/modified; application security settings changed)?

A: Yes, when customizations of procedures happen, a procedure customizations audit trail is created to track changes made by administrators.

Q: Can your products be integrated with third-party products?

A: Links to Lippincott Solutions may be placed within the EHR environment. *Lippincott Procedures* and *Lippincott Advisor* have HL7 info button capabilities, as well.

Lippincott Solutions is considered LMS-agnostic; in other words, the industry-standard AICC files available from Lippincott Solutions can integrate with any LMS if the LMS has the capability to receive those files. We have successfully integrated with numerous LMS/EMR providers including (but not limited to): *Cerner, Epic, SumTotal, HealthcareSource-NetLearning, LearnSoft, HealthStream, Cornerstone, Ellucid, PolicyStat, PolicyTech, Compliance 360* (policy management systems), and *PeopleSoft*. Customers may customize/modify existing skills and add hyperlinks to policies on shared drives, websites, or formal policy management systems.

Q: What type of support does your company provide?

A: Lippincott Solutions provides “classroom style” online training, web training, WebEx virtual classroom training, and online technical support. Technical Enterprise Support is available Monday-Thursday 8am – 12am EST; Friday 8am – 7pm EST; Sunday 4pm – 12am EST by phone at 1-844-303-4860 (international 1-301-223-2454) or via email at LNS-Support@wolterskluwer.com. After-hours support is also available by calling 1-877-247-6843.