How Cardinal Health™ OptiFreight® Logistics secures your data

We use this product ourselves, so we understand the importance of strict security and privacy of your data. We utilize different types of security and encryption techniques to help ensure that your data is secure.

Encrypted traffic

OptiFreight® Logistics uses encryption techniques on all access routes. All traffic to and from OptiFreight® Logistics, including sign-on, are encrypted at 256-bit and sent through at least TLS 1.2, adhering to the FIPS 140-2 certification standard.

External security audits and penetration tests

We work closely with third-party leaders in web app and infrastructure security who perform penetration tests, threat modeling and audits of OptiFreight® Logistics. We monitor our product for security vulnerabilities automatically and promptly address all findings.

Where your files are hosted

We utilize multiple Google Cloud data centers across the U.S. to ensure your data is hosted in a secure location. Your data is never stored offshore and is encrypted at rest. For more information about Google security measures, visit cloud.google.com/security

Experienced team of experts

Our engineering teams partner closely with information security and keep their skills current with regular training that covers the latest information security trends, vulnerabilities and threat vectors. We have coded many different online systems and are experienced in all elements of infrastructure, application and system security.

What is TLS?

Transport layer security (TLS) is a cryptographic protocol that provides end-to-end security of data sent between applications over the internet. It is mostly familiar to users through its use in secure web browsing, and in particular the padlock icon that appears in web browsers when a secure session is established. It can and should be used for other applications such as e-mail, file transfers, video or audio-conferencing, instant messaging and voice-over IP, as well as internet services such as domain name system (DNS) and network time protocol (NTP).

TLS is normally implemented in addition to transmission control protocol (TCP) in order to encrypt application layer protocols such as HTTP, FTP, SMTP and IMAP, although it can also be implemented on UDP, DCCP and SCTP (e.g., for VPN and SIP-based application uses). This is known as datagram transport layer security (DTLS) and is specified in RFCs 6347, 5238 and 6083.

CardinalHealth™
OptiFreight® Logistics

Data protection

Critical customer data is backed up regularly while non-critical data is backed up on at least, a daily basis. Our teams track the latest security trends and threats. We promptly upgrade our services to address any vulnerabilities and continuously ensure we are using the latest software available.

Data access

The data you share with OptiFreight® Logistics is private and confidential. We have strict controls over our employees' access to data and we are committed to ensuring that your data remains confidential. Though we follow the least privilege principal, OptiFreight® Logistics operations wouldn't be possible without a few members having access to our databases to optimize performance and storage. This team undergoes significantly more training and all actions are regularly audited.

Protected health information (PHI)

OptiFreight® Logistics does not store, process or transmit PHI.

Pretty Good Privacy (PGP)

We provide an optional layer of security and privacy for our customer's data with convenient PGP encryption. If your organization is interested in using the OptiFreight® Logistics PGP option, contact your OptiFreight consultant to get started.

What is SFTP?

Secure file transfer protocol (SFTP) works over the secure shell (SSH) data stream to establish a secure connection and provide organizations with a higher level of file transfer protection. SFTP uses encryption algorithms to securely move data to your server and keep files readable during the process. Authentication prevents unauthorized file access during the operation.

SFTP gives you the option to perform a wide variety of tasks for sensitive files — from removing files to resuming paused transfers. SFTP only needs a single port number TCP (port 22) to establish a server connection.

CardinalHealth™