Eleos Data Security FAQ

Does Eleos monitor and test security on a regular basis?

Yes. Eleos contracts with an independent third-party agency that conducts annual penetration testing and automatically monitors our product for security vulnerabilities via external tools and auditors.

Is Eleos HIPAA and FERPA compliant?

Yes. Eleos is fully compliant with both the Health Insurance Portability and Accountability Act (HIPAA) as well as the Family Educational Rights and Privacy Act (FERPA).

What other certifications and compliance approvals does Eleos have?

Eleos is SOC2 and HITRUST compliant and has received Deloitte, ISO 27001, and ISO 27799 certifications.

How does Eleos encrypt data in transit?

All user traffic passes via HTTPS, with at least 256-bit SSL encryption for all Internet-based data. All administrator traffic is encrypted through Eleos Health's secure VPN. Integration traffic also passes through our secure VPN, which encrypts packet data as well as packet headers.

How does Eleos encrypt data at rest?

Sensitive data handled by Eleos Health's cloud applications are encrypted whenever they are stored in persistent memory. When such data are accessed by a user, file-system encryption ensures that access to the physical disk does not expose sensitive data. Database records are further encrypted with 256-bit keys via the industry-standard AES algorithm.

Where is Eleos data housed? Does it ever move locations?

Eleos supports data deployment in specific geographic regions, and we guarantee that these data will not move outside the originally designated region. For example, if a US-based health system desires to keep its data within the US, Eleos will store and process the data only in US-based Amazon Web Services (AWS) data centers.

How does Eleos detect unauthorized access and other threats?

Our system uses a host-based intrusion detection system (HIDS) to continuously monitor for unauthorized access attempts, suspicious activity, and unexpected behavior on each server within the Eleos cloud. Additionally, all company workstations and remote servers deploy endpoint detection and response (EDR) tools to monitor for threats in real time. Our databases also deploy access-control algorithms to identify rare events, items, or observations that differ significantly from standard behaviors or patterns, thus warranting investigation.

What security measures are in place for the AWS data centers Eleos uses?

AWS data centers meet the highest standards for physical security and access control. Access is strictly limited, and anyone granted access is thoroughly vetted and monitored. Additionally, all physical and electronic access to AWS data centers is routinely logged and audited.

What personnel measures are in place at Eleos to protect customer data?

Access to the Eleos cloud is locked down by subnet, port, protocol, server, role, and user. Only the access required for the specific business function is granted. Furthermore, Eleos requires all employees and contractors performing services for Eleos to undergo a thorough background check and participate in security training.

How does Eleos ensure data security when integrating with client systems?

Integrations with client systems are managed via the Eleos cloud VPN. We provision, monitor, and manage the VPN to create an overlay network designed to link a customer's corporate data center and our VPC. This ensures that all communications between the two are encrypted. Finally, a client can leverage Eleos cloud VPN with its existing extranet infrastructure. This VPN supports almost every IPSec data-center extranet solution as well as the standard OpenVPN protocol.

To learn more about data security at Eleos Health, visit eleos.health/security.

Have another data question? Email info@eleos.health.