



athenasoftware.net

integrated client information / case management solutions

Penelope and HIPAA

HIPAA Security provisions represent best practices for security management and operations and as such pertain primarily to the manner in which confidential data is accessed, stored, transmitted, manipulated recovered, and secured.

Penelope's technology and architecture enables organizations to deploy Penelope in a HIPAA compliant manner.

Information Access Control

- Penelope enables system administrators to determine specific security clearance levels to restrict access to data from within the system; for example, once logged in to the system, users may be designated with a security clearance level that restricts access to information relating to only to assigned cases.
- Penelope uses username and password controls to restrict access to Penelope to authorized parties; terminated employees can have their access rights revoked at any time.

Internal Audits

- Penelope can be configured to generate a daily system log that displays information on all pages viewed, when they were viewed, the user who viewed them, their IP address and any changes that were made to the data. This log file can be reviewed periodically to detect suspicious or anomalous behaviour.
- This log file is only accessible locally on the password-protected server.

Security of Backups / Media

- Penelope can be configured to generate a backup of the data on an ongoing basis – this data may be stored on the password protected server
- It is the responsibility of the organization to ensure that access to any media containing confidential data is restricted as appropriate.

Security of Server

- It is the responsibility of the organization to ensure that physical access to the server is restricted.
- It is the responsibility of the organization to ensure that remote access to the server is restricted through the deployment of VPNs, firewalls and other security practices.
- It is the responsibility of the organization to ensure that physical access to active “logged in” Penelope sessions are restricted as appropriate.

Workstation Security / Entity Authentication

- Penelope does not leave a “cache” on workstations; after logging out, no information relating to the users’ session with Penelope is stored on the workstation used for that session.
- After 70 minutes of inactivity, Penelope automatically terminates the session, forcing users to log back into access the system – this session limit can be modified to suit the organization’s preferences.

Recovery

- Penelope enables users to restore from a data backup in a matter of minutes.

Data Encryption / Communications and Networking

- Penelope may be configured to encrypt all transmissions between the server and the client browsers using SSL technology
- Certificate validation by third parties may be implemented to ensure both the authenticity and source of data
- Penelope can be configured to use an encrypted database

Data Verification

- Penelope automatically tracks who has created data for each entity record (and when) along with the last time the record was modified (and by whom).