



- **Penelope and Threat Assessment and Assurance**
- **Penelope and HIPAA**
- **Penelope ASP Hosting Facility Features**

Penelope TRA Overview

In terms of the 5 key areas relevant to threat assessment and assurance of information and information processing systems, namely, access control, confidentiality, integrity, availability, and non-repudiation, Penelope Case Management offers a high degree of assurance for organizations processing and storing highly sensitive information both in its design and also in its optional configurations.

Penelope is a secure, highly configurable web application that is used to assist human service organizations in the management of clinical data, human resources and scheduling functions, accounts receivables/ billing, outcomes monitoring and all aspects of service provision. Penelope may be installed on the organization's LAN for use within the network or VPN or alternatively, accessed as an ASP service hosted in a secure facility by Athena Software.

Access Control

For information on access control to the physical server, please see the section on ASP Hosting Facility Overview.

Penelope controls access to confidential data and key functions on a system- configurable "need to know" basis. 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, cases within their department or site, within their site tree, reporting group or other, system-configurable roles. Penelope features broad user groups that correspond to roles at an organization and then above and beyond that, configurable security classes that allow/restrict access to records and functions on a class-by-class basis.

All clinical records can be "locked" (with a user and date/ time stamp) preventing any subsequent modification to the record.

Penelope uses username and password controls to authenticate credentials and restrict access to Penelope to authorized parties. IP-by-IP access rights may be implemented if needed. Terminated employees can have their access rights revoked at any time.

Confidentiality

Penelope may be configured to encrypt all transmissions between the server and the client browsers using any key-length 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. As described in the Access Control section above, access to confidential client records can be restricted on a modular, need to know basis.

Integrity

All transactions and importantly, access/ views of Penelope's pages/ data are logged in an audit trail that records, the IP, user's session credentials and the date/ time. In addition to the locking of records, The audit records the modifications made to any records. Penelope time/ date stamps all clinical records with the user who created or last modified the transaction. Penelope can be configured to automatically lock all notes/ documents upon saving, thus ensuring the integrity of the data and providing maximum assurance that the data was entered at the time/ date displayed and by the authenticated user who performed the function. The database stores – in each table – the name of the user who created the record, when it was created and also last modified, by whom – with the same information stored at the locking point.

Availability

Our ASP network and servers have recorded 99.9824% uptime over the past 24 months. Updates to the system are performed at scheduled intervals and occur early on Sunday mornings and last approximately 20 minutes. For more information relating to the availability of our ASP services, please see the ASP Hosting Facility Overview section below. Our servers can also be configured to have fail-over and load balancing functionality as per the specifications of our clients. Our client's backups are protected via the server's RAID systems, timed backups throughout the day and a nightly off-site secure transfer to another secure facility 10 km away from the hosting facility.

Non-Repudiation

Penelope's audit logs – which as described above record both ACCESS to specific pages and any changes or deletions made to those pages along with the time/ date and user credentials – serve as powerful assurance on the issue of non-repudiation. The logging function has already been called upon many times to support non-repudiation for many of our clients.

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

o 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.

o 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

o 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.

o This log file is only accessible locally on the password-protected server.

Security of Backups / Media

o Penelope can be configured to generate a backup of the data on a ongoing basis – this data may be stored on the password protected server

o It is the responsibility of the organization to ensure that access to any media containing confidential data is restricted as appropriate.

Security of Server

o It is the responsibility of the organization to ensure that physical access to the server is restricted.

o 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.

o 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

o 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.

o After X minutes of inactivity (as defined by the agency), 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

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

Data Encryption / Communications and Networking

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

Data Verification

- o 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).
-

ASP Hosting Facility Overview

Security Perimeters

- o The basic principle of security operations is multiple concentric security perimeters, or a “defense in depth”.
- o Each perimeter of security requires a higher level of authorization than the previous. As the level of security perimeter increases, fewer and fewer employees are allowed access.
- o The concentricity of the security perimeters means that the outer perimeters completely envelope and enclose the inner perimeters.
- o The building has a 24x7x365 alarm system which includes an interior “glass breakage” alarm. The alarm system is remotely monitored with immediate dispatch in the event of an out-of-normal event.

Personnel Access

- o The access to each perimeter is based on RFID's (radio frequency identifier) , each of which has a unique address. Only WDF personnel are issued RFID's. Each use of the RFID is monitored, tracked and if need be, reported. This includes successful uses AND false attempts for each use of the RFID. The RFID's are controlled by a single point of contact within the company.

Customer's Personnel

- o Customers are issued photo ID access cards, which include information about the individual including their photo, about the specific rack destination where their equipment is housed and information about a reference in that Customer's organization (usually the individual who has signed

the contract]. The photo ID is mandatory in order for the Customer to just enter the building. The security ID cards are controlled by a single point of contact.

Escorted Access

- o All access to the building and its security perimeters is 100% escorted 24x7x365. The escorts record the particulars of each access visit, prior to entering the equipment area. The escorts are required to carry out a mandatory inspection of the Customer's access photo ID card. An exact duplicate of the photo ID card is kept in the records for comparison to the Customer's card.
- o Altogether, there are four security perimeters in place. Beyond perimeter 2, all activities are monitored with full time, full motion colour video surveillance. The escorts activate the fourth and final security perimeter that allows the Customer to access their equipment.
- o The escorts are technically knowledgeable IT staff, who monitor and / or assist the Customer in their work. Generally, the escorts have a working knowledge or have a working relationship with the authorized Customer's individuals.

Equipment Protection

- o Protection is provided to the Customer's equipment so that they have uninterrupted operations.

Power Feed

- o The power supply provided includes multiple, redundant UPS's and dual power feeds (A feed and B feed) to each equipment rack.
- o The UPSs are fed by either the local power utility or the on-site diesel generator. The switch over to the generator is controlled by an automatic transfer switch. The diesel startup requires about 8 - 10 seconds to come on-line. Each UPS has a standby capacity of 30 minutes. There is at least 7 days fuel capacity at all times on-site. The fuel quality is routinely checked . The generator is tested weekly for a minimum of 1 hour.
- o The power feed and its components are monitored 24x7x365 and any out-of-normal event is tracked and monitored by the on-site alarm system.
- o The performance to date (over 30 months of operations) is 100% uptime.

HVAC

- o The equipment cooling is provided by telco Central Office standard equipment. It is equipped with dual compressors that ensure continued operation.
- o The on-site diesel generating capacity is designed to support, not only the computing equipment load, but also the HVAC power load.

- o The raised floor (24 inch) environment ensures the even and proper distribution of cooled air to the equipment racks. Routine temperature inspections are made to identify and mitigate any hot-spots within the equipment area.

Fire Suppression

- o Fire suppression is based on an inert dry-gas (Inergen) system. Unlike Halon, the Inergen gas is environmentally benign. The site operates in 4 separate fire suppression zones.

- o In the event of a high temperature event, the system floods the equipment area in alarm mode with the Inergen gas to lower the oxygen level to the point where combustion does not occur. The gas flooding takes about 5 - 6 seconds. This suppresses any fire. The Inergen gas also is designed to continue extracting the heat via the HVAC from the neighbouring equipment to allow uninterrupted operations within the equipment area.

- o The high temperature event simultaneously triggers audible and visual alarms.

Network Feed

- o The network connections are based on a fibre optic cable system, with physical route diversity, connected to 2 physically separate Points of Presence. The traffic is routed to multiple up-stream backbone carriers to ensure continuous operation.

- o It is up to the system administrator at the agency to ensure sound password policies are in effect. Each user has a unique ID that generates an audit trail which can recreate all of their actions in the system during any time period. All changes to the database are recorded in terms of who did them, when and who last modified them and when.