THERASCAN

Web-based document management for clinical trials

The TheraScan service web-enables clinical trial documentation, management, and monitoring. With a flexible structure and sensitivity to 21 CFR Part 11, ICH E6, and HIPAA; TheraScan puts the last pieces of study-based documentation safely on the Internet.

TheraScan creates certified copies of clinical trial documents. Scans of paper originals, EHR screen captures, existing electronic files, images, or other type of documents needed for clinical trials are certified as an exact copy and stored, along with document-specific data elements, in a HIPAA-compliant repository. This highly flexible infrastructure enables a wide range of possibilities for use in clinical trials.

Coupled with a suite of tools to interface with existing external systems, TheraScan is the solution to complete a tightly integrated, Internet-based, clinical trial.

TheraScan aims to complement rather than replace existing systems; whether EDC, CTMS, accounting, manufacturing, EHR, or otherwise. This allows organizations to leverage existing technologies to solve the “trilemma” of:

- **Speed:** TheraScan trials can offer instantaneous tracking and monitoring of the data flow. Systemic problems are identified earlier in the process to allow for timely resolution. Information, once located in remote locations, is accurately collected in a central repository that is securely available over the Internet in an instant. Properly structured studies can close almost immediately after data collection concludes.

- **Quality:** Monitors, sponsors, and investigators can see, at a glance, where the study stands. Communication is structured, interactions are tracked, and management is solidified. Essential documents and facets of the Trial Master File can be managed centrally.

- **Cost:** Site visits are greatly reduced with online monitoring. Data entry and analysis can be centralized, eliminating duplication of resources in the field. Monitors now concentrate site visits on building relationships and solving problems, rather than working alone in a back room. Sites are also relieved of the responsibility to oversee monitors to ensure patient confidentiality.

TheraScan uses a cloud-based architecture which greatly simplifies the implementation of the system. The client runs in a browser. The only installable feature optionally enables direct communication with a scanner from the browser.

When a record is added to the TheraScan system, a client-specific trigger is activated. Triggers can prompt a purchase order from the accounting system for a newly enrolled patient, alert the medical director of a Severe Adverse Event, or notify clinic staff of a change to the protocol or SOPs.

TheraScan is affordable. With little to no capital expense and a low monthly cost, TheraScan is priced so that it can be used in research that has tight budget constraints. This includes such important areas as orphan drugs, tropical diseases, and epidemiological studies.

TheraScan has many **implementation** options, configured via table-driven logic to allow customization of the application without changing the underlying program. Customers can quickly and easily tailor TheraScan to their needs.

Remote source document verification (rSDV)

Site monitoring brings its own set of challenges to clinical research. Extensive travel is expensive, time consuming, and taxing on staff. Sites must make room for monitors and deal with confidentiality issues relative to their electronic health records. With extended time between visits, issues are slow to be identified and require considerable effort to correct replicated problems.

TheraScan allows monitors to work in near real time from a centralized site. Travel requirement are significantly reduced, Monitoring is accomplished quickly so that issues are identified and correctly before they become endemic. Records with PHI are securely isolated from the local EHR to efficiently maintain confidentiality.

When combined with an EDC system, network-accessible source documents greatly simplify risk-based monitoring by having the source documents available concurrently with EDC data. EDC systems do not require customization in order to incorporate rSDV into the process.

Essential Documents (eBinders and eTMF)

Essential Documents have traditionally been maintained in physical binders for patients, staff and sites in a clinical trial. Checking for accuracy and completeness is a time consuming duty as staff have to go through individual binders in order to view the contents. The TheraScan system has staff upload certified copies of these documents to virtual binders. The resultant organized files may be quickly accessed by both site staff and monitors to confirm the completeness and content of the files at a glance.

Essential documents are not limited to clinical sites. TheraScan can be used by manufacturing sites and laboratory sites to maintain their required documentation, all in a shared repository across the study.

TheraScan can automatically receive and manage documentation for IP shipping and inventory as well as environmental standards using sensors, RFID tags or system interfaces as the data source.

Sponsors and investigators need to ensure that study-wide documentation is collected and up to date. TheraScan supports the collection and organization of documents needed for the Trial Master File. This includes study-wide documents, site-specific documents, site "override" documents, and client-specified documents. Documents are saved for submission and are also sharable across the study so the items like protocols and SOPs can easily be accessed.

Safety (SAEs and Triggers)

Patient safety is critical in clinical research. Often it is difficult to share information after a severe adverse event, especially when it is imperative to move quickly. With a HIPAA-compliant structure, an SAE can be uploaded along with supporting clinical documentation. Alerts via email and SMS messages are immediately sent so study staff is aware of the situation. Additional supporting documents can be added at any time. This allows clinical staff to provide appropriate care and study staff to alert the regulatory agency of the event.

If temperature guidelines are exceeded or if inventory doesn't match with the recorded doses, TheraScan can alert staff according to custom protocols specified by the client.

Safety also encompasses confidentiality. TheraScan allows most users to view metadata related to a document – like the creation date, type of document, or patient study ID – without providing access to the underlying image or file. Only specifically authorized users like monitors or site clinical staff can view documents with PHI, and then the view is logged for audit review.

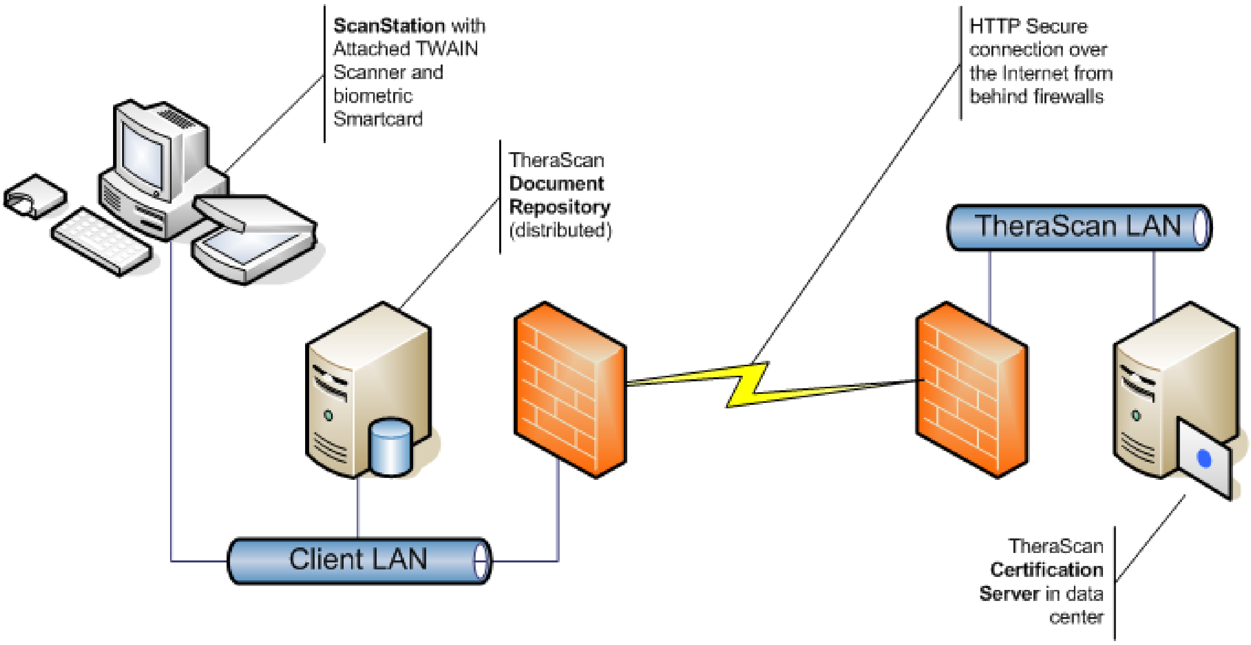
Benefits

When information is processed quickly, and added to the study database in near real time, monitors and auditors are able to identify systemic issues early in the process and rectify them before they become major issues.

With data entry, document storage and retrieval, and record keeping either accomplished or managed centrally, clinical personnel are freed to do the work they are trained for. Medical professionals can provide medical care, while the important but non-clinical work is transferred to staff that are the most efficient for these duties. The result: a more efficient study operation, with high quality data and a greatly reduced cost.

TheraScan Infrastructure

TheraScan generates certified electronic copies of source documents which can stand in for paper originals when auditing and monitoring clinical trials. The system has three components required to copy, certify and upload source documents copies to the system.


ScanStation with Attached TWAIN Scanner and biometric Smartcard
TheraScan Document Repository (distributed)
HTTP Secure connection over the Internet from behind firewalls
TheraScan LAN
Client LAN
TheraScan Certification Server in data center

ScanStation: This is the PC or thin client that will run the web-based application used to scan, load and sign the source-document copies. Therapeias recommends TWAIN scanners from Canon and Fujitsu.

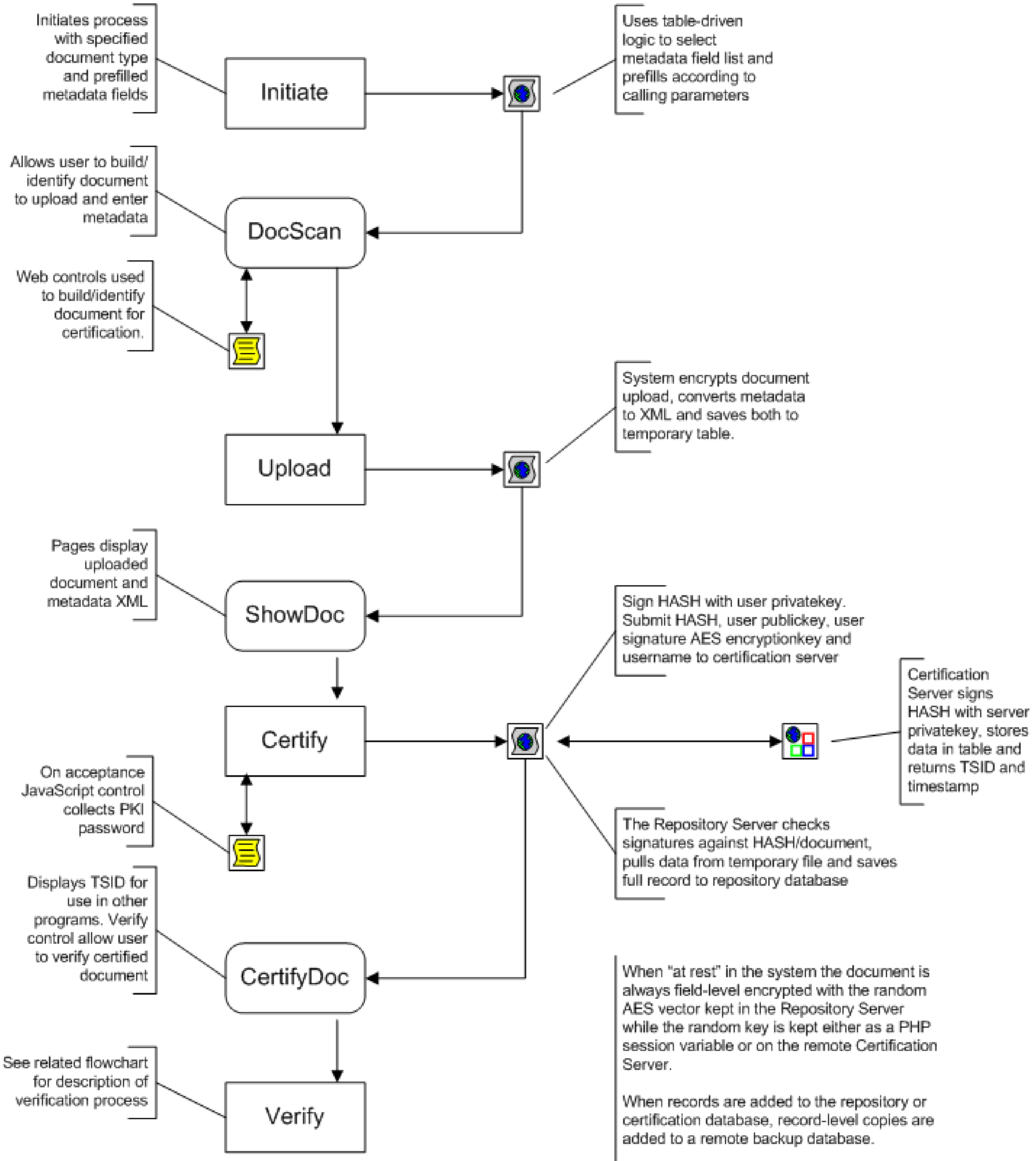
Document Repository: This is a HIPAA-compliant web server and database that processes and holds the encrypted source-document copies generated by the ScanStation. These copies can subsequently be securely viewed over the network. The files are kept within the database as binary objects for excellent scalability, security and ease of backup. Each study has a logical repository so that access can be restricted to specific users and/or locations. Post-certification document handling can be customized per client specification. There are two implementation options for the Document Repository

1. Hosted Option: Therapeias will host the repository on shared equipment in their data center with logical separation of study data. Database backups and system maintenance are be done by Therapeias.

2. Distributed Option (pictured above): The client will provide a VMWare virtualized environment which can be sited behind their institutional firewall (as in the diagram). The standard setup will utilize a PostgreSQL database server with a client option to upgrade to an Oracle database.

Certification Server: This is the centralized system that certifies and confirms the validity of the copies submitted by the ScanStation and later viewed by authorized users. User authentication is managed centrally by this server. Each Document Repository needs to have network access to the Certification Server which will be done via secure connection. The Certification Server is sited at our data center. Only information required for certification is kept on the server, with no individually identifiable health information, eliminating HIPAA Privacy Rule concerns.

TheraScan Certification Flowsheet



Initiates process with specified document type and prefilled metadata fields

Uses table-driven logic to select metadata field list and prefills according to calling parameters

Allows user to build/ identify document to upload and enter metadata

Web controls used to build/identify document for certification.

System encrypts document upload, converts metadata to XML and saves both to temporary table.

Pages display uploaded document and metadata XML

Sign HASH with user privatekey. Submit HASH, user publickey, user signature AES encryptionkey and username to certification server

Certification Server signs HASH with server privatekey, stores data in table and returns TSID and timestamp

On acceptance JavaScript control collects PKI password

The Repository Server checks signatures against HASH/document, pulls data from temporary file and saves full record to repository database

Displays TSID for use in other programs. Verify control allow user to verify certified document

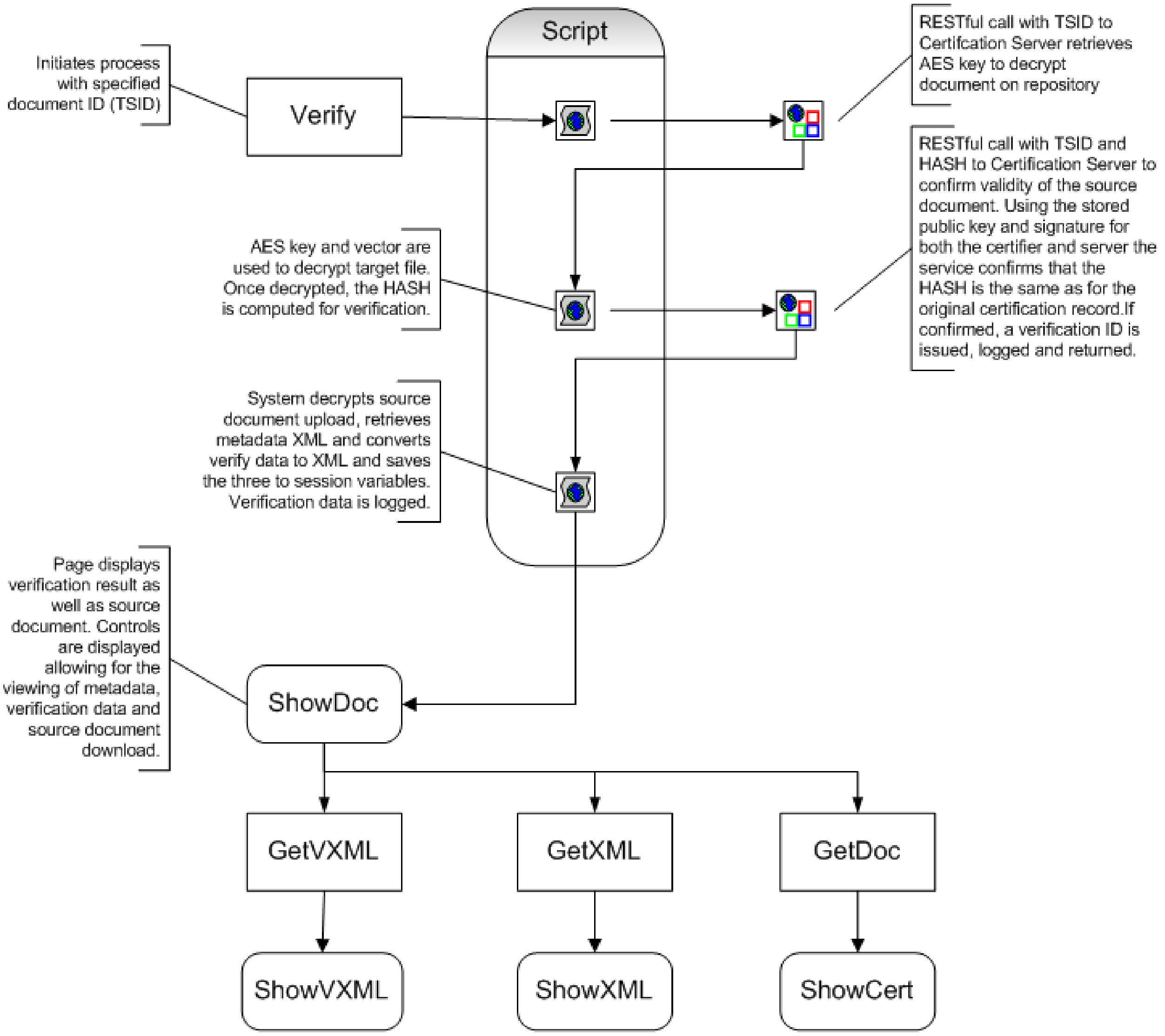
See related flowchart for description of verification process

When “at rest” in the system the document is always field-level encrypted with the random AES vector kept in the Repository Server while the random key is kept either as a PHP session variable or on the remote Certification Server.

When records are added to the repository or certification database, record-level copies are added to a remote backup database.

Encrypted database backups are created nightly and stored in a remote AWS repository

TheraScan Verification Flowsheet



Initiates process with specified document ID (TSID)

RESTful call with TSID to Certifcation Server retrieves AES key to decrypt document on repository

AES key and vector are used to decrypt target file. Once decrypted, the HASH is computed for verification.

RESTful call with TSID and HASH to Certification Server to confirm validity of the source document. Using the stored public key and signature for both the certifier and server the service confirms that the HASH is the same as for the original certification record.If confirmed, a verification ID is issued, logged and returned.

System decrypts source document upload, retrieves metadata XML and converts verify data to XML and saves the three to session variables. Verification data is logged.

Page displays verification result as well as source document. Controls are displayed allowing for the viewing of metadata, verification data and source document download.

When "at rest" in the system the document is always field-level encrypted with the random AES vector kept in the Respository Server while the random key is kept either as a PHP session variable or on the remote certification server.

When records are added to the repository or certification database, record-level copies are added to a remote backup database.

Encrypted database backups are created nightly and stored in a remote AWS repository

TheraScan Design Guidelines

- The TheraScan servers are hosted in an SSAE 16 Type II certified data facility.
- The TheraScan servers are in a secure/locked cabinet behind a dedicated Cisco ASA firewall.
- The systems run in a virtualized environment with the certification and repository functions on separate physical servers. Development and test environments are also on separate physical servers.
- Records with PHI have field-level encryption via SSL with a randomized initialization vector stored on the host server and the randomized key on the remote certification server.
- PHI, which can be included as part of the certified source document copy, is always encrypted when "at rest" in the system.
- The decryption process is individually logged; recording the specific decrypted record id, the authorized requester, as well as a date-time stamp. This log is viewable by the trial investigator.
- Decryption can only be accomplished by the user who loaded the information, other site staff or the investigator-authorized monitor. Exceptions include study-specific documents without PHI such as the protocol or blank CRFs and documents loaded as part of a severe adverse event.
- No direct database access is allowed to users. Access is via the secure web site.
- All communication over the public internet is via the HTTPS, SSL, or SSH protocols.
- Access to the certification server is only via the RESTful web interface from known locations.
- Daily backups are encrypted with a public key and then securely uploaded to a remote repository.
- Incremental (record-level backups) are encrypted with a public key and uploaded to a remote database. Redundant records are regularly purged from the remote database.
- The password-protected private keys needed for decryption are kept on an FIPS 140-2-validated encrypted flash drive in a secure location.
- Monitors are required to use two-factor authentication. TheraScan uses a FIPS 140-2-validated system from Duo Security that utilizes mobile phones as the token.
- Source document certification is made using SSL with a user-specific, password-protected, private key and SHA-256 signature algorithm. This is countersigned by the certification server with a server-specific private key and SHA-256 signature algorithm.
- The user-specific public key, the certification-server public key and the SHA-256 hash "fingerprint" are stored on the certification server for use in verifying the authenticity of the certified source document copy.
- The TheraScan system uses SQL database software from Oracle and PostgreSQL.
- Access-control to the system is processed through the database. A user may only access one study at a time.
- TheraScan utilizes an "insert-only" model such that data records are neither updated nor deleted once in the table.
- Access to specific information in the repository is granted via dynamic, user-specific, views that grant access based on the logged in user. These views do not contain PHI.
- The primary table in the repository contains the encrypted certified object in a BLOB field and the related metadata in an XMLType field. The metadata does not contain PHI.
- Authorization is managed via a two-factor process requiring both email and SMS tokens in order to activate a new user. Passwords require eight characters and must include upper and lowercase letters, numbers, and special characters.
- TheraScan uses HTML5 websockets for communication with the TWAIN device (scanner).
- A study's Informed Consent should include a section to recognize the loading of source documents to the TheraScan system for review by study monitors.