HiTrack
EHDI Data Management System

HiTrack 5 Series Security Whitepaper

Overview

The HiTrack EHDI Screening & Tracking Application consists of two primary components – a Database component that stores and processes all of the patient data, and a Client component that presents the processed patient data to users. There are two Client programs that can communicate with the Database – the Web Client and the Merge Companion.

Typically the HiTrack Database is hosted by a state or hospital agency and maintained by their internal IT staff. The HiTrack developers and support staff do not have access to client servers or patient data outside of pre-authorized desktop screen share support sessions. Annual product activation is performed by a unique registration code – the HiTrack application does not "phone home" for activation. No communication of any kind occurs between the HiTrack client software and external or third-party servers.

Database

The HiTrack Database runs exclusively on Microsoft SQL Server 2017 or later (MSSQL). For security and performance reasons, we recommend using a minimum of the Standard Edition of the latest MSSQL release when possible. For optimum performance and security, the MSSQL system should be updated, secured and maintained regularly according to Microsoft Best Practices documented here: https://technet.microsoft.com/en-us/sqlserver/bb671430.aspx

Web Client

The HiTrack Web Client runs on Microsoft Windows Server through the Internet Information Services (IIS) web hosting platform. The IIS Web service connects to the MSSQL HiTrack Database, processes patient data and then serves rendered web pages to the client web browser. All HiTrack communication between the client web browser and the web server is performed through the standard web page ports and protocols and are encrypted using industry standard web page SSL - SHA-256 with RSA Encryption.

The Web Client module authenticates to the Database using either Active Directory credentials or a SQL Server specific username and password. In addition, HiTrack also

utilizes its own internal user authentication via username and password entered at the login screen. The internal authentication determines which specific facility and patient information will be made available to the user. The password is stored encrypted inside the database. Passwords follow Microsoft's default Active Directory complexity rules and can be configured to expire periodically. In versions 5.1.2 and newer single-sign-on (OIDC) and two factor user authentication are available depending on the hosting environment.

The HiTrack Web Client always logs out the user after a preconfigured period of inactivity.

Role-Based Access

All access to patient data and tracking features is controlled with role-based access. System Administrators can choose from more than 250 fine-grained access rights to create site-specific levels of access determined by the authorized needs of users. Access granularity includes view only, add, edit-only-your-own and delete-only-own-your-own entries and others. Various combinations of this granularity provide robust control over every part of patient data.

Patient Level Access

Patient level access is governed by several layers of simultaneous configuration. Age of record is the first layer of control: by default, user access is limited to births within the last year; additional years of access must be granted by an administrator. The next layer of access is controlled by only granting access to births that occurred at individually assigned birth or screening facilities. For users not at birth or screening facilities access is governed on a HIPAA-compliant lookup feature. Record access automatically expires for these types of non-facility users after a specified amount of time has passed.

As mentioned above – role-based access rights control each part of the patient record.

HiTrack maintains a Change Log of all patient record activity inside of the database for auditing purposes. A Database History Log is maintained to document when database backup, restore and upgrade operations take place. A history record of all login attempts is also automatically maintained. Patient level record view-logs are available.

Merge Companion

The HiTrack Merge Companion is a small Microsoft .Net Framework Windows application that can be used when patient data needs to be collected from screening devices. The Merge Companion collects the patient data from the screening device, encrypts the data using industry-standard encryption, and then uploads it to a HiTrack Web Server through SSL encrypted web services (SHA-256 RSA).

The HiTrack Merge Companion requires the user to enter their HiTrack login credentials on each data upload. Use of the Merge Companion equipment data upload is optional but recommended instead of manual data entry for speed and accuracy.