Auditbase

Office Management System

Version 6.6.0 released for Denmark, Norway, Sweden, Finland, Ireland and the UK

What's New

Changes in version 6.6.0

Auditdata

HL7 interfacing

Merge notification

- Merge notifications from HL7 interfaces can be viewed and processed in the Attention List. No patient data will be sent in the email notification.

Measurement and clinical

Audiogram

- We have updated the audiogram image variables used for Word documents to include axis labels and units.

Audiometer and tymp interfaces

- The upcoming version of Otosuite using the Noah Audiogram 500 and Tymp 500 format has been tested and verified.

Noah

Export

- The Noah export file from Auditbase can now be encrypted and protected by a password.
- The Noah export file from Auditbase can now include Fast Data Views.

Import

- Noah export files containing up to 10 patients can now be imported directly into Auditbase. An additional licence is required to import files with more patients.
- The Noah import will include demographics and Noah actions. Noah audiograms will be used to create Auditbase Audiograms. Text entries from the Noah Journal module will create Auditbase Journal entries, files attached to the Noah Journal will not be imported. FDV files will be accessible as Noah Actions.

- You can choose under which Auditbase user to record the Noah imported records.
- We have made sure that the import matching dialog to merge Noah patient records with existing Auditbase patient records is as user-friendly as possible while reducing as much as possible the likelihood of mismatching patients.
- With the additional licence you will be able to add imported patient records into a Client List.

Other features

Attention list

- The Attention List can now be configured to warn you when changing the selected client.

PAS links

- If the Hosp HL7 system supports updating identifiers and an updated identifier is returned on a query and that identifier is already applied to another patient instance, then the user will receive a notification that a patient merge task is created in the Attention List.

Security

Auditing

- The Security Log has a specific action of 'Admin setup' which covers all the configuration actions performed by users in Auditbase Administration.
- Within that action there is now a drop down of hundreds of individual types of actions that the Security Log can be filtered on.
- You can also use free text in the 'Additional text' field to filter any entries in the Security Log for either Administration or Auditbase itself.
- The Security Log and Security Log Archive Deposit are protected from tampering or deletion by a specific Extended Right.

Security

- The System Administrator SYSADM account will no longer be permitted to log into Auditbase. This increases security by ensuring that all clinical, patient scheduling, and configuration actions are performed by a named user and can be

audited. Configuration tasks that could previously only be done by the System Administrator SYSADM are now covered by Extended Rights that can be assigned to named users.

System Administration

General

- The SYSADM account is now severely restricted and can only create and elevate users, intended for the initial setup of the first elevated users.
- Trusted senior users can now make changes in the separate specific high-level sections in Administration after being granted Extended Rights, so you can allow users to configure the areas in which they specialise and not those in which they do not.
- Specific named Users can now create Users or Roles or modify Roles' rights using a new Elevated Right with an accompanying password. Once a user has logged in with that Elevated Right the session will stay in that mode until they log out. This enables you to have a higher level of security applied to individual members of the Auditbase Administration Role.
- A new template Role has been created, which contains the table rights needed to allow the Extended Rights in Administration to operate. Using this template, you can easily create other Roles to separate the Administration configuration tasks between users with different specialisms.
- Administration pages that the user does not have the Extended Rights to configure will be visible but not editable by them. This allows users to see which options are available when they do not have the rights to configure them.
- All changes made in the Administration tool will be audited under a genuine user name. Now you have the enhanced security control to trace who made configurations changes and when.

User setup, rights and maintenance

- User Views and Setups have been separated from one page to four separate pages for increased affordance and visibility. They are Application options, Client and clinical, Referrals and scheduling, and Locations and departments.
- You can now apply changes or selected settings in the 'Views and setups' pages and 'Alerts' user settings to all or nominated existing members of a Role, rather than just future members.
- The long list of Extended Rights has been organized into a tree structure to make it much easier to find the Extended Right that you need to configure on a Role.