

Release Notes 1.4.0.0

Virtual Private Database (VPD) Security Change

All encounter data is stored in the data mart. The VPD controls access to the data by allowing access to either a specific program or by a specific managed care organization id. The VPD operates at the Oracle database layer and is transparent to the users operating behind-the-scene. A user will simply see appropriate data based upon the VPD restriction enforced.

Some users were experiencing long query execution times and/or query timeout failures when using the LTCare Encounter Datamart Universe. The condition would occur if a user would run a query that included a large number of data elements along with person specific information AND the user had permission to see both Family Care encounter data and Partnership encounter data but was not granted access to the SSI encounter data. Basically, the problem would occur if the user was allowed to see most but not all encounter data.

The original VPD configuration would cause the Oracle database query to generate large temporary datasets that would use up vast amounts of system resources in order to provide the user with the data requested as well as securing the access to only appropriate records. The original VPD configuration would operate efficiently if the user could see all data in the data mart or a smaller subset of data, such as one organization id. But when a user is allowed to see both Family Care and Partnership data, the user is allowed to see approximately 99.5% of the data in the data mart, which is most but not all the data.

This release changed the VPD configuration to optimize query execution in the situation where a user can see most but not all the data. Users that fit the situation above should notice better query execution times and experience less query timeouts.

Secure Data by Detail Table Organization Id

The original encounter data VPD configuration was designed to secure encounter data by a submission. This means that if your organization submitted the encounter data, you are allowed to see all detail records within that submission.

In the near future, encounter data will be collected for children’s long term support waivers. The encounter data will be submitted by a single third party administrator (TPA). The TPA will be submitting encounter data on behalf of hundreds of individual county agencies. The TPA is the submitter but the detail records will be from many county organizations. A future data warehouse requirement dictates that each of the many county organizations must be allowed to see their encounter data in the LTCare Encounter Datamart universe even though they did not submit the records. The original configuration of what-you-submitted is what-you-see will no longer work for this new future requirement.

Revision Date:	6/3/2010	Author:	Mike Guentherman	Approver:	Ron Wollner
Revision Date:		Author:		Approver:	

Wisconsin Healthcare Account Quality Management System

Level 3 – LTCare Data Warehouse

DSS/DW – Release Notes 1.4.0.0

The data warehouse team took the opportunity to prepare for this future requirement when making the VPD security change for the query timeout problem above. The same solution for correcting the query timeout problem also allows the data warehouse security to meet the new future requirement.

This release allows a user to see appropriate encounter detail data in the data mart even though the user is not assigned to the organization that actually submitted the encounter records.

Revision Date:	6/3/2010	Author:	Mike Guentherman	Approver:	Ron Wollner
Revision Date:		Author:		Approver:	