Non-VA Care Program Integrity Tools

Repository User Guide

Version 2.0



June 2019

Department of Veterans Affairs

Office of Information and Technology (OI&T)

Revision History

NOTE: The revision history cycle begins once changes or enhancements are requested after the document has been baselined.

| Date | Revision | Description | Author |
| --- | --- | --- | --- |
| 6/1/2019 | 1.0 | Program Integrity Tools User Guide | Sowmya Rachaputi (By Light Team) |
| 6/6/2019 | 2.0 | Draft reviewed and finalized | Athar Ahmad - ByLight |

**Artifact Rationale**

Per the Veteran-focused Integrated Process (VIP) Guide, the User’s Guide is required to be completed prior to Critical Decision Point #2 (CD2), with the expectation that it will be updated as needed. A User Guide is a technical communication document intended to give assistance to people using a system, such as VistA end users. It is usually written by a technical writer, although it can also be written by programmers, product or project managers, or other technical staff. Most user guides contain both a written guide and the associated images. In the case of computer applications, it is usual to include screenshots of the human-machine interfaces, and hardware manuals often include clear, simplified diagrams. The language used is matched to the intended audience, with jargon kept to a minimum or explained thoroughly. The User Guide is a mandatory, build-level document, and should be updated to reflect the contents of the most recently deployed build. The sections documented herein are required if applicable to your product.

**Table of Contents**

[1. Introduction 1](#_Toc10669233)

[1.1. Purpose 1](#_Toc10669234)

[1.2. Document Orientation 1](#_Toc10669235)

[1.2.1. Organization of the Manual 1](#_Toc10669236)

[1.2.2. Assumptions 2](#_Toc10669237)

[1.2.3. Coordination 2](#_Toc10669238)

[1.2.4. Disclaimers 2](#_Toc10669239)

[1.2.4.1. Software Disclaimer 2](#_Toc10669240)

[1.2.4.2. Documentation Disclaimer 3](#_Toc10669241)

[1.2.5. Documentation Conventions 3](#_Toc10669242)

[1.2.6. References and Resources 3](#_Toc10669243)

[1.3. National Service Desk and Organizational Contacts 3](#_Toc10669244)

[2. System Summary 4](#_Toc10669245)

[2.1. System Configuration 6](#_Toc10669246)

[2.2. Data Flows 7](#_Toc10669247)

[2.3. User Access Levels 9](#_Toc10669248)

[2.4. Continuity of Operation 11](#_Toc10669249)

[3. PIT Enterprise Data Repository (PITEDR) 11](#_Toc10669250)

[3.1. Key Elements of the Enterprise Data Repository 12](#_Toc10669251)

[3.2. Database Creation in PITEDR 12](#_Toc10669252)

[3.2.1. Create PITEDR Databases 12](#_Toc10669253)

[3.2.1.1. Restoring from a Backup File 12](#_Toc10669254)

[3.2.1.2. Creating the Database from Scratch 16](#_Toc10669255)

[3.2.2. Create PITEDR\_PreStage Database 17](#_Toc10669256)

[3.2.3. Lookup and Reference Data Load 17](#_Toc10669257)

[4. PITEDR Repository Maintenance 17](#_Toc10669258)

[4.1. System Requirements 17](#_Toc10669259)

[4.2. Database Maintenance 18](#_Toc10669260)

[4.2.1. Database Archiving: 18](#_Toc10669261)

[4.2.2. Database Backup: 18](#_Toc10669262)

[4.2.3. Database Recovery 18](#_Toc10669263)

[4.3. Relevant Databases 18](#_Toc10669264)

[4.3.1. Databases Relevant to PIT Application 19](#_Toc10669265)

[4.3.2. Data Repository Update Process: 19](#_Toc10669266)

[4.3.3. Relational Tables and Diagrams 19](#_Toc10669267)

[4.4. External Application Databases 20](#_Toc10669268)

[5. Getting Started 20](#_Toc10669269)

[5.1. Logging On 20](#_Toc10669270)

[5.2. System Menu 20](#_Toc10669271)

[5.3. Changing User ID and Password 20](#_Toc10669272)

[5.4. Exit System 22](#_Toc10669273)

[5.5. Caveats and Exceptions 22](#_Toc10669274)

[6. Using the Software 22](#_Toc10669275)

[7. Developer’s Guide (Data Repository access) 23](#_Toc10669276)

[7.1. Developer Workstation Setup install SQL server management studio 23](#_Toc10669277)

[7.2. Tools and Utilities SQL Server Management Studio 24](#_Toc10669278)

[7.2.1. Connect to PITEDR via SSMS 24](#_Toc10669279)

[7.2.2. Query data 25](#_Toc10669280)

[7.2.3. Save query result as CSV file 26](#_Toc10669281)

[7.2.4. Update Repository data: 26](#_Toc10669282)

[7.2.5. Extend Repository table column 26](#_Toc10669283)

[7.2.6. Create index: 27](#_Toc10669284)

[7.2.7. Gathering statistics 27](#_Toc10669285)

[7.2.8. Using Import Export Data utility to copy data to/from the Repository 27](#_Toc10669286)

[8. SQL Server Command Line Tools and Utilities: 31](#_Toc10669287)

[9. Software Internal Documentation SQL Server Management Studio Documentation; Online Documentation 32](#_Toc10669288)

[10. Troubleshooting 32](#_Toc10669289)

[10.1. Special Instructions for Error Correction 32](#_Toc10669290)

[11. Acronyms and Abbreviations 33](#_Toc10669291)

[12. Appendix A 33](#_Toc10669292)

[1. The Manual Backup Process, Using a GUI 33](#_Toc10669293)

[13. Index 36](#_Toc10669294)

List of Tables

[Table 1: Tier Support Contact Information 3](#_Toc10669186)

[Table 2: AITC Development Environment Configurations 6](#_Toc10669187)

[Table 3: AITC Test Environment Configuration Details 6](#_Toc10669188)

[Table 4: AITC Pre-Production Environment Configurations 6](#_Toc10669189)

[Table 5: AITC Production Environment Configurations 6](#_Toc10669190)

[Table 6: Communication Architecture (Default Ports) 7](#_Toc10669191)

[Table 7: Application Context Description 8](#_Toc10669192)

[Table 8: Microsoft Business Intelligence Reporting Tool User Roles and Privileges 9](#_Toc10669193)

[Table 9: DataStage User Roles and Privileges 9](#_Toc10669194)

[Table 10: JRules User Roles and Privileges 9](#_Toc10669195)

[Table 11: FAMS User Roles and Privileges 10](#_Toc10669196)

[Table 12: PIT Data Repository Key Elements 12](#_Toc10669197)

[Table 13: Physical database names and brief descriptions 19](#_Toc10669198)

List of Figures

[Figure 1: System overview 5](#_Toc10672970)

[Figure 2: SQL Connect to Server Dialog 13](#_Toc10672971)

[Figure 3: Object Explorer Panel 13](#_Toc10672972)

[Figure 4: Restore Database process 14](#_Toc10672973)

[Figure 5: Backup File Selection 14](#_Toc10672974)

[Figure 6: PITEDR.bak backup file 15](#_Toc10672975)

[Figure 7: Restoring the Database 15](#_Toc10672976)

[Figure 8: Restore Completed Successfully 16](#_Toc10672977)

[Figure 9: Selecting the Client Component for SSMS installation 24](#_Toc10672978)

[Figure 10: Connecting to PITEDR database 25](#_Toc10672979)

[Figure 11: Executing a Query and Viewing Query Output 26](#_Toc10672980)

[Figure 12: Using the Import/Export Wizard to Choose a Data Source 28](#_Toc10672981)

[Figure 13: Using the Import/Export Wizard to Choose a Destination 29](#_Toc10672982)

[Figure 14: Using the Import/Export Wizard to Choose a Destination 29](#_Toc10672983)

[Figure 15: Using the Import/Export Wizard to Select Source tables 30](#_Toc10672984)

[Figure 16: Successful Transfer via Import/Export Wizard 31](#_Toc10672985)

[Figure 17: sqlcmd Command Line Utility 32](#_Toc10672986)

[Figure 18: Starting the Backup Process 33](#_Toc10672987)

[Figure 19: General View for Backing Up the Database 35](#_Toc10672988)

[Figure 20: Backing Up the Database (Options) 36](#_Toc10672989)

# Introduction

The Non-VA Care Program Integrity Tools system, or PIT, is a comprehensive set of tools to detect Fraud, Waste, and Abuse (FWA) before reimbursing external providers for healthcare services to eligible Veterans.

The VA Office of Inspector General (OIG) estimates that 12.4% of non-VA Care Fee program’s gross claims payments[[1]](#footnote-1) are improper payments. Noting that ~$6 billion in health care claims payments passes through VA Purchased Care each year, this is a potentially sizable problem. In response, the Veterans Health Administration (VHA) Chief Business Office (CBO), Purchased Care Business Line (PCBL) wants to assess the accuracy of payments, potential fraudulent billing by community providers and other concerns that result in significant improper payments for all non-VA health care claims that are paid by VA across all Purchased Care Programs.

These programs are currently managed in multiple environments, both decentralized at Veterans Affairs Medical Center (VAMC) Veterans Health Information Systems and Technology Architecture (VistA) systems (for Fee Basis Programs - FBCS) as well as a centralized location in Denver at the Health Administration Center (HAC) (for Civilian Health and Medical Program of the VA (CHAMPVA), Spina Bifida and Foreign Medical Programs).  Having multiple environments impacts VA’s ability to assess these programs to prevent improper payments. PIT was conceived to provide a comprehensive assessment of each claim to avoid improper payments to external providers.

## Purpose

The Program Integrity Tools User Guide is intended to provide all the necessary information to use components of Program Integrity Tools including examples of utilization. The manual assumes that the reader has a good knowledge of Program Integrity Tools.

## Document Orientation

The Program Integrity Tools User Guide is used to illustrate the setup and physical configuration of the Program Integrity Tools Enterprise Data Repository (PITEDR) and to provide instructions on managing and maintaining the database. The document is organized into the following main sections:

* Database creation
* Data repository maintenance
* Database access

This document is intended for SQL Server DBAs who understand the architecture and configuration of the Microsoft SQL Server (MSSS) Database (DB).

### Organization of the Manual

Under indicated sections describe how the Program Integrity Tools (PIT) User Guide has been organized.

**Section 2.0: System Summary -** The Program Integrity Tools is comprised of multiple components. The Program Integrity Tools Enterprise Data Repository (PITEDR) is at the core of the PIT System. System Summary describes the overview and purpose of Program Integrity Tools

**Section 3.0: Getting Started –** This section provides a general walkthrough of the Program Integrity Tools from initiation through exit. The logical arrangement of the information shall enable the technical personnel to understand the sequence and flow of the system.

**Section 4.0: Using the Software –** This section describes how components of Program Integrity Tools could be used.

**Section 6.0: Troubleshooting –** This section provides information on handling anticipated errors.

### Assumptions

* The details of the physical architecture and the physical infrastructure are beyond the scope of this document; please contact the Austin Information Technology Center (AITC) team for these details.
* The Drop Zone is a File System-based exchange area for inbound and outbound feeds. It will reside at the Austin Information Technology Center (AITC) and will utilize MS Windows File Share mechanism.
* Windows Server 2008 R2 is the Operating System.
* The configuration of production environment is non-clustered.

### Coordination

* The Program Integrity Tools Servers are maintained and hosted at AITC (Austin Information Technology Center). Any Server or Database incident requests are required to be coordinated with AITC. Austin Information Technology Center (AITC) also assists in monitoring the resource utilization of the Servers.

### Disclaimers

Under indicated sections of disclaimers pertains to the Program Integrity Tools and Documentation disclaimers.

#### Software Disclaimer

*This Program Integrity Tools was developed at the Department of Veterans Affairs (VA) by employees of the Federal Government during their official duties. Pursuant to title 17 Section 105 of the United States Code this software is not subject to copyright protection and is in the public domain. VA assumes no responsibility whatsoever for its use by other parties, and makes no guarantees, expressed or implied, about its quality, reliability, or any other characteristic. We would appreciate acknowledgement if the software is used. The components of Program Integrity Tools can be redistributed and/or modified freely if any derivative works bear some notice that they are derived from it, and any modified versions bear some notice that they have been modified.*

#### Documentation Disclaimer

*The appearance of external hyperlink references in this manual does not constitute endorsement by the Department of Veterans Affairs (VA) of this Web site or the information, products, or services contained therein. The VA does not exercise any editorial control over the information you may find at these locations. Such links are provided and are consistent with the stated purpose of the VA.*

### Documentation Conventions

Not Applicable for Program Integrity Tools (PIT) user guide.

### References and Resources

Below artifacts has been as reference for preparing the Program Integrity Tools (PIT) user guide:

1. Production operations manual (PIT\_POMv2.0)
2. Non-VA Care PIT-Repository User Guide – v1.5

## National Service Desk and Organizational Contacts

The four tiers of support documented here in are intended to restore normal service operation as quickly as possible and minimize the adverse impact on business operations, ensuring that the best possible levels of service quality and availability are maintained.

Table 1: **Tier Support Contact Information**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Role** | **Org** | **Contact Info** |
| Program Integrity Tools Server/Database Requests | Tier 0 | VHA/AITC | Server Incident Requests: Create a help desk ticket requesting to have the ticket assigned to the group: IO.PS.FF. SERVERS.WINDOWS.TRIAGE, also email: [PII](mailto:PII)  Database Incident Requests: Create a help desk ticket requesting to have the ticket assigned to the group:  IO.PS.FF. DATABASE.SQLSERVER, also email: [PII](mailto:PII) |
| Program Integrity Tools – By Light Help Desk Support System | Tier 1 | By Light | Athar Ahmad (Project Manager)  [Athar.Ahmad@Bylgiht.com](mailto:Athar.Ahmad@Bylgiht.com)  [PII](mailto:PII)  Sowmya Rachaputi (Business Analyst)  [Sowmya.rachaputi@bylight.com](mailto:Sowmya.rachaputi@bylight.com)  [PII](mailto:PII) |
|  | Tier 2 | By Light | Bruce Sonnenfeld (Software Engineer)  [Bruce.Sonnenfeld@bylight.com](mailto:Bruce.Sonnenfeld@bylight.com)  [PII](mailto:PII)  Larissa Boudnik (Database Developer)  [Larissa@myarch.com](mailto:Larissa@myarch.com)  PII |
|  | Tier 3 | By Light | Sasha Ananiev (Technical Lead Architect) |

# System Summary

The Program Integrity Tools is comprised of multiple components shown in the figure below. The PIT data repository is at the core of the PIT system, it receives data feeds from other VA claim processing systems including FBCS, CP&E, FSC, eCAMS and CDW; each source system provides data to a central drop zone.

Figure 1: System overview

This figure describes an overview of Program Integrity Tools system. Also about the different drop zones that will feed the claims data into PIT Enterprise Data Repository (PITEDR). Claims Scoring Tool will assign the scores as the ETL will push the claims scores to the drop zone as the reporting tool will accommodate end user browsing.

The Program Integrity Tools is comprised of multiple components:

* The PIT data repository will be fed from FBCS, CP&E, CP&E DW, FSC and eCAMS systems to provide claims and related data through drop zone.
* The claims scoring tools is to assign scores based on the risk of fraud/waste and abuse on a pre-payment basis.
* The ETL will push the claims scores to the drop zone, where, the FBCS systems will retrieve it and, process it accordingly.
* The Dashboard and Reporting tool that will accommodate end user browsing and analysis, standardized reports, ad hoc queries and reports and business intelligence extractions which we anticipate will be used to manipulate dimensional presentation of data.
* The assessment of the predictive modeling application will take in consideration the Fraud/Waste/Abuse (FWA) detection for the post-payment basis.

## System Configuration

Below tables indicate the Hardware, storage, processing and communication architecture (default ports) used for Program Integrity Tools system configuration:

Table 2: AITC Development Environment Configurations

| **Old Server** | **Newly Upgraded Server** | **Purpose** | **IP Address** | **CPU** | **RAM**  **GB** | OS  **GB** | APP  **GB** | DATA  **GB** | LOG  **GB** | TEMP  **GB** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| DNS | DNS | Rules App Server | IP | 2 (3) | 6 | 80 | 200 |  |  |  |
| DNS | DNS | Data Stage Application Server | IP | 2 | 28 | 80 | 39 | 159 | 29 | 19 |
| DNS | DNS | DataStage Application Server | IP | 2 | 8 | 80 | 220 |  |  |  |

Table 3: AITC Test Environment Configuration Details

| **Server** | **Newly Upgraded**  **Server** | **Purpose** | **IP Address** | **CPU** | **RAM**  **GB** | OS  **GB** | APP  **GB** | **DATA**  **GB** | **LOG**  **GB** | **TEMP**  **GB** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| DNS | DNS | SharePoint / BI Application Server | IP | 2 | 8 | 100 | 150 |  |  |  |
| DNS | DNS | Rules App Server | IP | 2 | 6 | 80 | 200 |  |  |  |
| DNS | DNS | FAMS Application Server | IP | 2 | 6 | 70 | 80 |  |  |  |

Table 4: AITC Pre-Production Environment Configurations

| **Server** | **Newly Upgraded**  **Server** | **Purpose** | **IP Address** | **CPU** | **RAM**  **GB** | OS  **GB** | APP  **GB** | DATA  **GB** | **LOG**  **GB** | TEMP  **GB** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| DNS | DNS | Rules App Server | IP | 6 | 12 | 80 | 200 |  |  |  |
| DNS | DNS | Rules App Server | IP | 6 | 12 | 80 | 200 |  |  |  |
| DNS | DNS | DataStage Application Server | IP | 6 | 12 | 80 | 200 |  |  |  |
| DNS | DNS | DataStage Application Server | IP | 6 | 12 | 80 | 200 |  |  |  |
| DNS | DNS | FAMS Application Server | IP | 4 | 12 | 64 | 100 |  |  |  |
| DNS | DNS | Database | IP | 8 | 64 | 100 | 244 | (E)2000  (F)1400  (G)800 | 254 | 530 |
| DNS | DNS | SharePoint / BI Application Server | IP | 6 | 16 | 80 | 260 |  |  |  |

Table 5: AITC Production Environment Configurations

| **Server** | **Newly Upgraded Server** | **Purpose** | **IP Address** | **CPU** | **RAM**  **GB** | OS  **GB** | APP  **GB** | **DATA**  **GB** | **LOG**  **GB** | **TEMP**  **GB** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| DNS | DNS | Rules App Server | IP | 4 | 12 | 80 | 50 |  |  |  |
| DNS | DNS | Rules App Server | IP | 4 | 12 | 80 | 90 |  |  |  |
| DNS | DNS | DataStage Application Server | IP | 8 | 16 | 100 | 700 |  |  |  |
| DNS | DNS | DataStage Application Server | IP | 8 | 16 | 80 | 400 |  |  |  |
| DNS | DNS | FAMS Application Server | IP | 4 | 12 | 60 | 50 |  |  |  |
| DNS | DNS | SharePoint/BI Application Server | IP | 4 | 12 | 60 | 260 |  |  |  |
| DNS |  |  | IP | 8 | 68 | 80 | 544 | (E)2000  (F)2000  (G)773 | 488 | 400 |
| DNS |  |  | IP | 8 | 68 | 80 | 544 | (E)2000  (F)2000  (G)773 | 488 | 400 |
| DNS |  |  | IP | 8 | 68 | 80 | 544 | (E)2000  (F)2000  (G)773 | 488 | 400 |

Table 6: Communication Architecture (Default Ports)

| Component | Default Port Numbers |
| --- | --- |
| IBM Information Server Web-based clients | 9080 |
| IBM Information Server Web-based clients - HTTPS | 9443 |
| WebSphere Application Server Administrative console | 9060 |
| WebSphere Application Server Administrative console (HTTPS) | 9043 |
| IBM Information Server services (RMI/IIOP) | 2809, 9100, 9401–9403 |
| IBM WebSphere Information Services Director services with JMS bindings | 7276, 7286, 5558, 5578 |
| SQL Server database | 1433 |
| IBM Information Server ASB agent | 31531, and a random port number greater than 1024\* |
| IBM Information Server logging agent | 31533 |
| IBM WebSphere DataStage and QualityStage services | 31538 |
| Parallel job monitors | 13400 (port 1) and 13401 (port 2) |
| Parallel engine (APT\_PM\_STARTUP\_PORT) | multiple ports use a port number of 10000 or greater |
| Parallel engine remote process startup (rsh/ssh, multiple nodes only) | 22514 |
| Parallel engine (APT\_PLAYER\_CONNECTION\_PORT, multiple nodes only) | multiple ports use a port number of 11000 or greater |

## Data Flows

Below depicted application context diagram depicts the overall flow of data in the Program Integrity Tools.

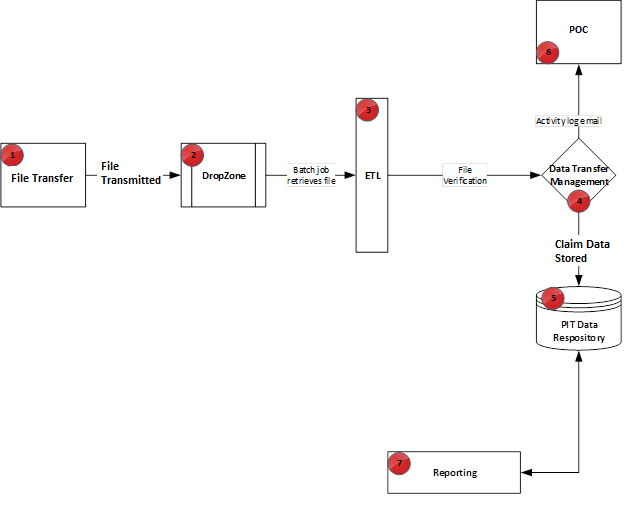


Table 6 describes the entity information shown in the Application Context Diagram.

Table 7: Application Context Description

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Object ID | Name | Description | Interface | Interface System |
| 1 | Data Source | Files (claim data) is transferred to the Drop zone | Drop zone | Drop Zone |
| 2 | Drop Zone | Data exchange | Data file | ETL |
| 3 | ETL | Moves data in batch processes from the Drop Zone and the data repository | ODBC | Drop Zone  Program Integrity Tools Enterprise Data Repository (PITEDR) |
| 4 | Data Transfer Management | Activity log email and Activity log reports | ETL | Program Integrity Tools Enterprise Data Repository (PITEDR) |
| 5 | PIT Enterprise Data Repository (PITEDR) | Enterprise repository to store claim data extracted from VA claim processing systems. | ODBC | ETL |
| 6 | POC | Team (data source from which the claims data had been received) would be notified if there is an issue with the Data Transfer Management System |  | Team (data source from which the claims data had been received) |
| 7 | Reporting | Microsoft BI Reporting Tools | HTTP/GUI | Microsoft Report Builder  Program Integrity Tools (PIT) |

## User Access Levels

The following tables list the identified Program Integrity Tools users based on their roles:

Table 8: Microsoft Business Intelligence Reporting Tool User Roles and Privileges

| Role | Privileges |
| --- | --- |
| Administrator | Sets access to group reports/objects for Power User |
| Report Author | Creates standard/ad-hoc reports for PIT, creates/modifies business rules in partnership with Chief of Program Integrity |
| Information User | Views and utilizes existing reports in Business Intelligence Tool |

Table 9: DataStage User Roles and Privileges

| Role | Privileges |
| --- | --- |
| Administrator | Manages environments and version releases, maintains data integrity, and assists developer with designing ETL processes.  Can create new data structures.  Can execute system reports for capacity, performance, etc. |
| ETL Developer | Formulates data models, creates/maintains tables in data repository, specifies data mapping from source-to-target tables, develops ETL processing capabilities |
| Operator | Can manually run ETL jobs, view ETL processing reports and statistics |

Table 10: JRules User Roles and Privileges

| Role | Privileges |
| --- | --- |
| Administrator | Full administrative rights on Decision Center, including the ability to define users and permissions.  Plus, all Reviewer capabilities. |
| Reviewer | Able to review rules with status “Defined” and either approve them by assigning a status of “Validated”, reject them by assigning a status of “Rejected”, or launch them by assigning a status of “Deployable”.  Plus, all Author capabilities. |
| Author | Able to author and modify business rules and assign a status of “Defined” to rules.  Plus, all Viewer capabilities. |
| Viewer | Able to browse and view defined rules and schemes  (Note: the VA Claims Clerk will continue to use existing VA source systems to see claim line scores) |

Table 11: FAMS User Roles and Privileges

| Role | Privileges |
| --- | --- |
| Administrator | In addition to the functionality of the Power User Role, the Administrator Role grants users’ full administrative rights to the FAMS application. FAMS Administrators can:  Administer security  Load and maintain claim database tables (with the partnership of the individual maintaining the PIT Data Repository, as needed)  Provide database-specific support  Define and create Auto-Extract Processes for Service Level Files  Administer the databases  Update database tables  Perform application data mapping to support the Auto-Extract process and feature selection Post-installation validation  Participate in Defining Peer Group and Models |
| Power User | In addition to the functionality of the Business User Role, the Power User Role allows users to run the Profile Baseline Processes including Service-Level Extract (SLE), Value Set generation and Profiling.  Power Users can:  Assist with documenting/defining business processes for selecting cases using FAMS  Participate in installation  Perform production testing  Assist business users with selecting peer groups for review  Define filters that FAMS administrators should apply to profiles  Generate SLE extraction of claims from the Data Mart  Generate Feature Values (answers to the questions in the scoring model)  Profile data, apply Hypothesis Modules, and provide values and scores for Business Users  Identify entities for review and take notes on rosters |
| Business Analysis User | Create behavior models  Define and document custom report requirements  Perform production testing  Leverage the visualization, data discovery, and reporting capabilities within FAMS to identify outliers  Create case notes and rosters within FAMS, and assign cases for business use  Review case information selected by FAMS Power Users  Leverage FAMS reports to confirm allegations  Print/store all reports required for case creation |

## Continuity of Operation

The Program Integrity Tools system provides an assessment of a claim to prevent improper payments to external providers. It is not critical to patient care and would not cause patient safety issues if down or unavailable. Therefore, disruption of access to or use of information from the PIT would have a limited adverse effect on VA’s organizational operations, assets, or individuals. And because there are no direct dependencies between VA source systems and the PIT system, a temporary disruption of access would not hinder VA’s ability to fulfill claims payments as usual. Likewise, any unauthorized modification or destruction of information would have limited adverse effect on the VHA’s ability to operate.

However, the Program Integrity Tools (PIT) system handles Sensitive Personal Information, which contains personal identifiable information and personal health information. As a result, the unauthorized disclosure of information would have a severe adverse effect on VA’s mission, reputation, and organizational operations.

# PIT Enterprise Data Repository (PITEDR)

The Program Integrity Tools data repository serves as the data store for Purchased Care Claims data for Veterans and their dependents. The intent of the repository is to house healthcare claims data that has been processed and adjudicated across multiple VA systems. The PIT data repository will contain enough data to facilitate multiple goals including the development of a robust FWA program, the reduction of improper payments, the utilization of industry-standard health care claims tools, and the ability to perform analysis on payments across VHA Programs. The database infrastructure will consist of multiple physical databases to handle the persistent layer of the Program Integrity Tools set, including the PITEDR and the PITEDR\_PRESTAGE db’s. PITEDR will store claims data extracted from the VA claims processing systems, while PITEDR\_PRESTAGE will pre-stage data before it is processed by the ETL tool.

The PIT repository will receive and store data the following claims processing systems: FBCS, CP&E, CP&E DW, and CDW. The repository will also serve as the data source for the claims scoring tool, the reporting tool, and a future predictive analytics tool.

The data repository resides on a MS SQL Server DBMS. The physical database design for the production environment meets the following scalability and availability requirements:

* Ability to handle multiple data sources and business areas
* Utilization of failover clustering
* High-volume data storage and data partitioning, where applicable
* Support of different data types
* Indexing to facilitate query workload, ETL bulk-load optimization, and claim score processing

## Key Elements of the Enterprise Data Repository

Table 12: PIT Data Repository Key Elements

|  |  |
| --- | --- |
| Key Element | Tools and Technologies |
| DBMS | Microsoft SQL Server 2012 R2 |
| Data Integration | IBM Infosphere Data Stage 11.5 |
| Data Access | Services: JDBC, ODBC  In/Outbound data feed: flat files |
| Reporting | MS Business Intelligence 2008 |

## Database Creation in PITEDR

This section includes the instructions and the steps required to create the PIT database repository. These steps can be performed by a SQL Server database administrator or a system administrator with Windows command line experience. The individual performing the installation will need to possess server administration rights on the target database server.

The PIT database repository can be created using the steps detailed in the sections below.

### Create PITEDR Databases

There are two methods to create the PITEDR and PITEDR\_PreStage databases:

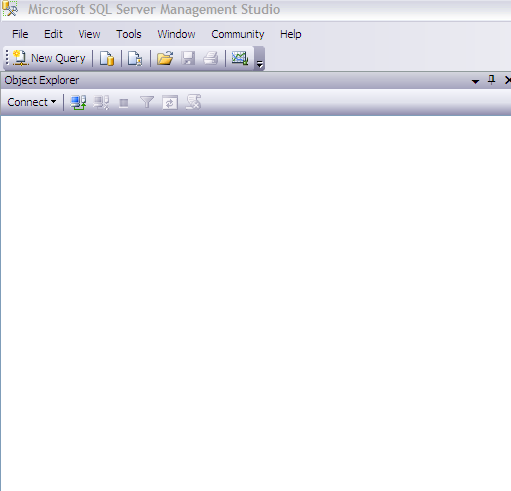
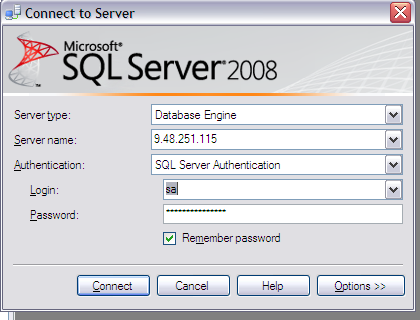
1. To restore from a backup file (which IBM will provide): Use the Microsoft SQL Server Management Studio general user interface, or
2. To create from scratch: Use database creation scripts and the Windows command line interface (this method will be detailed once the scripts are finalized; provided via the *Pre-Production Release Package*)

#### Restoring from a Backup File

The following step-by-step instructions should be used to create a new database from a backup file using Microsoft SQL Server Management Studio (to create the backup file itself, please reference Appendix A).

1. First, connect to the database server from SQL Server Management Studio (see Figure 3).

Figure 2: SQL Connect to Server Dialog



For Server type: Choose **Database Engine** (as shown here)

For Server name: type the host server name or IP address.

For Authentication: depends on environment, and SQL Server or Windows authentication can be used

For Login: (if SQL Server authentication is selected) type in username and the password in Password box.

1. Click **Connect** to login to the database server.
2. On the left side of the screen note the Object Explorer panel in SQL Server Management Studio. Using this panel, right-click **Databases** as shown in the image below. Selectthe **Restore Database** option from the drop-down menu.

Figure 3: Object Explorer Panel

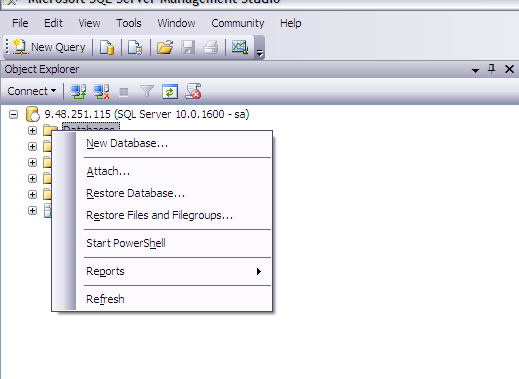
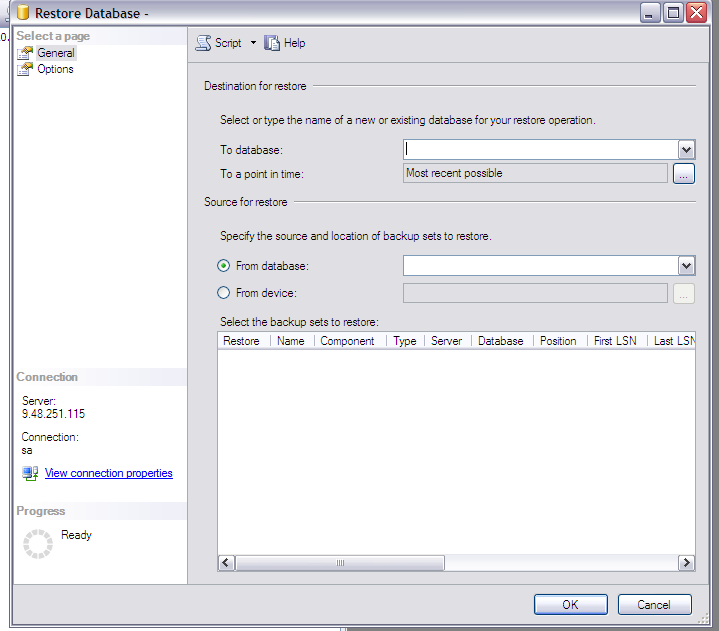
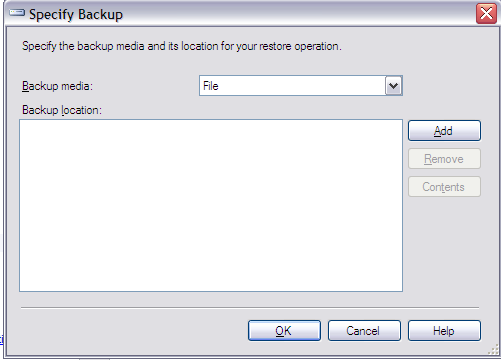


Figure 4: Restore Database process



1. Type “PITEDR” in the ‘To database’ field on top.
2. Select the radio button for ‘From device’ and click on the Ellipse (…) button. It will open another dialog window for Backup file selection as shown in the following picture.

Figure 5: Backup File Selection

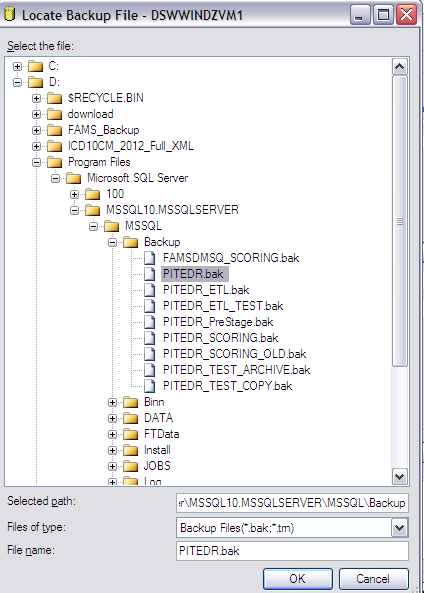


1. Click the **Add** button to open the media in which the backup file is stored.

Example: D:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER \MSSQL\Backup

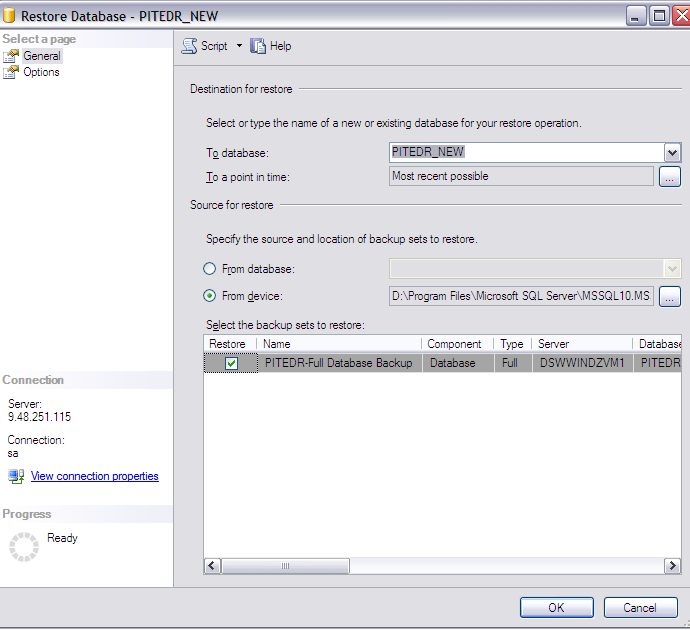
1. Navigate to and select the PITEDR.bak file. Click **OK**.

Figure 6: PITEDR.bak backup file



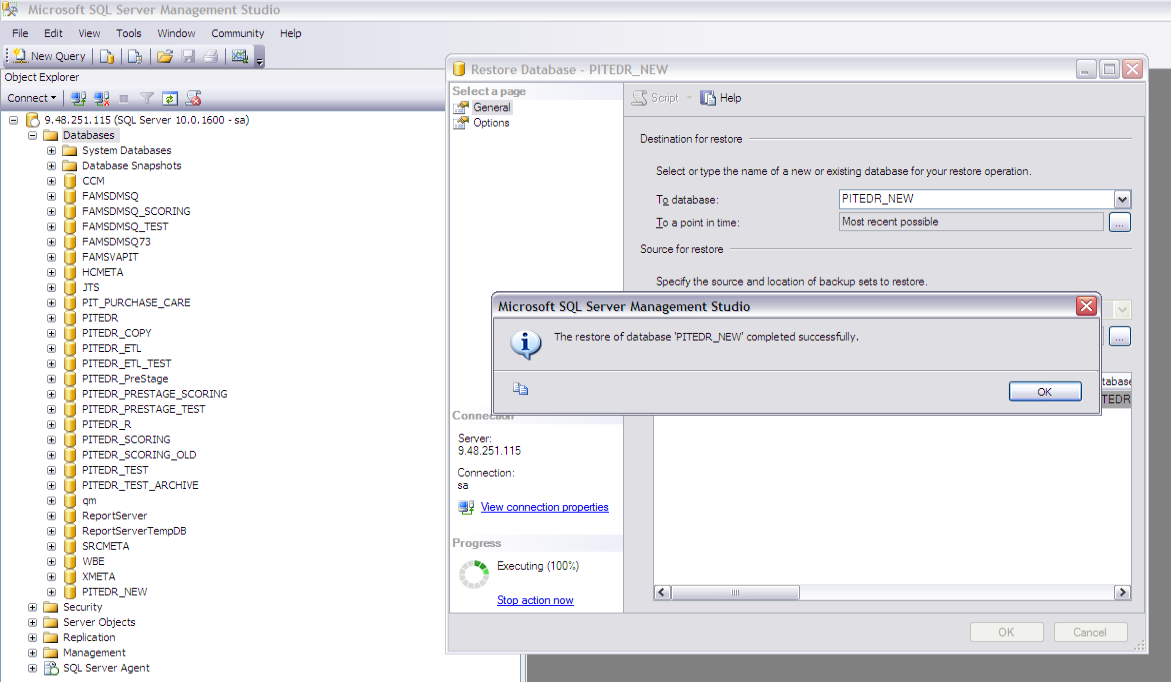
1. Click **OK** on the ‘Specify Backup’ dialog box.
2. Check the Restore box and click **OK** to begin the database restore.

Figure 7: Restoring the Database



The progress of the restore is shown on the left side pane of the Restore Database dialog window. Once the database is completely restored, a confirmation message will pop up in SQL Server Management Studio (as seen in the figure below).

Figure 8: Restore Completed Successfully



Now the database will be successfully created and ready for use.

Note: The User may encounter two typical issues while creating a SQL server database:

1. The user does not have ‘Create Database’ permission in the master database.

Resolution: The user must be provided with this privilege by the DBA.

1. The user does not have read/write permissions to the folder in which data and log files are created.

Resolution: The DBA must provide the user with these permissions.

#### Creating the Database from Scratch

The following step-by-step instructions should be used to create a new database from scratch running SQL scripts with the SQLCMD utility:

1. Retrieve database create scripts to the local database server/client machines
2. Unzip PITEDR\_depl.zip and make PITEDR\_depl the current directory
3. Run cr\_db\_aitc.sql script:
   1. Set SQLCMDSERVER=<server name>
   2. Set SQLCMDDBNAME=master
   3. Set SQLCMDUSER=<sa>
   4. Set SQLCMDPASSWORD=<sa pwd>
4. Sqlcmd -e -i cr\_db\_aitc.sql -o cr\_db\_aitc.log .log
5. Create login/user
6. Restore PITEDR\_PRESTAGE database (utilize Section 2.3, below)
7. Restore the database from backup file PITEDR\_PRESTAGE.bak using SQL Server Management Studio
8. Load reference data and initialize tables with "-1" record in PITEDR (corresponds to section 2.4) by running insrt.sql and insrt-1.sql scripts
9. Create triggers in PITEDR by running sr\_trigg1.sql script

### Create PITEDR\_PreStage Database

A PITEDR pre-staging database (PITEDR\_PreStage) provides an area to load and organize source file data before population into target tables of the PIT data repository. The pre-staging database is also used to store claim-processing reference/external license data (e.g. procedure code, LEIE, NPPES provider table, etc). The pre-staging database can be created using the same general creation process and steps depicted above, with a few key adjustments:

For Step 4, Type “PITEDR\_PreStage” in the ‘To database’ field on top.

For Step 7, the user must Navigate to and select PITEDR\_PreStage.bak file. The user can then click **OK**.

### Lookup and Reference Data Load

Lookup and reference table data used in the PITEDR will be loaded using scripts delivered as part of the initial database software deployment. Once the PITEDR has been created using .BAK, these scripts will need to be separately run to populate the reference data in their respective tables. This data will be staged in PITEDR\_PRESTAGE and the scripts will extract and massage the data for loading into the needed PITEDR reference tables.

Future maintenance of lookup and reference table data will be maintained by the PITEDR DBA and ETL administrator(s) using the information found in the *System Operations and Maintenance Plan*. The PITEDR DBA will also maintain license information within the framework of a VA agreement with the appropriate data provider(s).

# PITEDR Repository Maintenance

This section contains the management guide for PITEDR systems. The intended audience for this documentation is database support personnel, management, and system administration personnel.

## System Requirements

The database’s system requirements apply to PIT database administrators and Infrastructure administrators. Detailed hardware and minimum operating system requirements for the host server and workstation environments (e.g. memory, disk, input/output setup) are described in the *System Architecture Design Document for the AITC.*

## Database Maintenance

### Database Archiving:

The PIT repository will be archived periodically to an offline database as determined by VA AITC requirement and data retention policies. The PITEDR will keep 5 years of data active on the live database, while the repository’s initial data load will include 18 month of historical claim data. After the first 3.5 years, a monthly process will extract transaction data older than 5 years into an offline database. This process can be automated using SQL Server Agent or started manually by the DBA.

Access and maintenance to the offline database (for requests for data which is >5 years old) will be managed by the PITEDR DBA, and data will be able to be extracted from these databases on an on-demand basis.

### Database Backup:

SQL server supports two methods of database backup, full database backup and incremental backup.

The SQL server agent process runs on a schedule to perform a full weekly backup, which means that structures and data are archived as of the backup date and time. In addition, a daily incremental backup process runs using the database transaction log to backup data since the last backup. It is recommended that administrators move backup files to an off-site storage location following the AITC standard system backup process.

The output backup files use the following conventions:

* [System Name]\_[database name]\_full\_yyyymmdd
* [System Name]\_[ [database name]\_incr\_yyyymmdd

Appendix A illustrates the manual backup process using a GUI.

### Database Recovery

In the event of database loss or an irrecoverable database file due to disk corruption, SQL server DBAs can perform database restoration from a backup file using the last full backup and the incremental log.

Database restoration can be performed using the steps described in section 2.2.

## Relevant Databases

### Databases Relevant to PIT Application

The database infrastructure will consist of several physical databases to handle the persistent layer of the Program Integrity Tools set. Table 2 lists the database names and locations as they exist in PITEDR. Table 3 lists the relevant database user IDs.

Table 13: Physical database names and brief descriptions

| Database short name | Database long name | Purpose | Location | DB server | Data Storage Path |
| --- | --- | --- | --- | --- | --- |
| PITEDR | Program Integrity Tools Enterprise Data Repository database | Enterprise repository to store claim data extracted from VA claim processing systems. | AITC | VAAUSPCISQL40 (Pre-Production)  VAAUSPCISQL20 (Production) | E:\ |
| PITEDR\_PRESTAGE | Program Integrity Tools Enterprise Data Repository Pre-Staging database | To load and organize data before being processed by ETL tool | AITC | VAAUSPCISQL40 (Pre-Production)  VAAUSPCISQL20 (Production) | E:\ |

### Data Repository Update Process:

The following step-by-step instructions will be used to update the PIT Enterprise Data Repository database structure.

1. Retrieve database update scripts to the local database server/client machines
2. View the folder deltascripts\release-<releaseID>, which contains all the update scripts for the database
3. Download the scripts to a local folder
4. Run main.sql script with SQLCMD utility from the folder with the following syntax;

sqlcmd -e -r 1 -U sa -P <sa pwd> -S <server> -d PITEDR -i main.sql -o deployment.log

1. Check deployment.log file for any error messages and resolve appropriately

### Relational Tables and Diagrams

Please see the *Enterprise Data Architecture*document for updated details on the PITEDR data dictionary and graphical data models.

## External Application Databases

The FAMS application database reads from and writes to the PITEDR database. Specific steps to create the FAMS application DB are described in the *FAMS User Guide*.

The XMETA database is the InfoSphere Data Stage metadata database. Steps to create the XMETA database are described in the *System Architecture Design Document for the AITC*.

# Getting Started

Under indicated sections describe the operations and Maintenance tasks performed on different components of Program Integrity Tools.

## Logging On

All users coordinate with Austin Information Technology Center (AITC) for an authentication against VA Active Directory. The user base for the Program Integrity Tools is a specialized group of individuals that have access to claims and patient information.

The Program Integrity Tools solution architecture includes four primary components:

* Program Integrity data repository
* Data integration/Extract, Transform Load (ETL) services
* Claims Scoring Tool
* Reporting and analytics capability

Data integration/Extract, Transform Load (ETL) services that will load claim data from source systems into the repository and post claim scoring results for use in payments.

Please refer to Section 2.0: Routine Operations in Production Operation Manual (PIT\_POMv2.0) – for all the information related to operations and maintenance tasks performed on different components of Program Integrity Tools

## System Menu

As indicated above, the Program Integrity Tools is combination of multiple components. System Menu section may not be applicable as there is no interface for Program Integrity Tools.

## Changing User ID and Password

Below listed accounts used would require frequent password resets:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Domain** | **Organizational Unit** | **User ID** | **User Description** | **Password Last Set Date** |
| AAC | DNS.URL | DNS | DNS.URL | 9/5/2018 |
| AAC | DNS.URL | Pciasadmin | SERVICE Account: DNS:DATASTAGE | 3/29/2017 |
| AAC | DNS.URL | DNS | SERVICE ACCOUNT:DNS:SQLCluster | 3/23/2019 |
| AAC | DNS.URL | DNS | SERVICE ACCOUNT:DNS:DATASTAGE Dev | 3/7/2019 |
| AAC | DNS.URL | DNS | SERVICE ACCOUNT: R10853042FY16 | 10/5/2016 |
| AAC | DNS.URL | DNS | SERVICE ACCOUNT:DNSFBCS | 8/7/2018 |
| AAC | DNS.URL | DNS | SERVICE ACCOUNT:DNS:LDAP | 7/30/2018 |
| AAC | DNS.URL | DNS | SERVICE ACCOUNT:DNS:Monitoring:R1384158FY13:Wintel:PCI | 1/25/2019 |
| AAC | DNS.URL | DNS | SERVICE ACCOUNT:R10320342FY16 | 9/1/2016 |
| AAC | DNS.URL | DNS | SERVICE ACCOUNT:DNS:SSRS PreProd:R9360890FY16 :Wintel:PCI | 10/17/2016 |
|  | Program Integrity Tools Enterprise Data Repository Database passwords are reset for these user accounts | Famsdbadmin  Famsadmin  Xmeta  Xmetasr  wodmdbadmin |  |  |
|  | SSH Accounts (on SFTP21) | SFTP\_PCI\_AITC  SFTP\_PCI\_AITC\_CCRS  SFTP\_PCI\_AITC\_CCNNC |  |  |
|  | WAS | Wasadmin  isadmin |  |  |

## Exit System

Please refer to section 2.1.2: System shut-down

## Caveats and Exceptions

The Program Integrity Tools receive claims from different source systems. One of the caveats is when is there is Program Integrity Tools (PIT) integration with a new source system.

* Servers: Servers are required to be accessed for memory space to receive the anticipated claim volume from the source system. If required, memory space might have to be added.
* Servers are required to be monitored and tracked for resource utilization.
* Databases: old claims data need to be archived/purged so that the database storage space is handled efficiently to receive newly integrated claim data.
* Database performance tuning is required (such as creating indexes) for faster reports accessibility.

# Using the Software

The Program Integrity Tools (PIT) Servers operations run 24 hours 7 days a week. When the received claims are processed, different component’s software play a significant role for having the claims processed through completion.

|  |  |  |
| --- | --- | --- |
| **PIT Component** | **Software Name** | **Usage of Software** |
| Program Integrity Tools Enterprise Data Repository |  | Database used |
| Extract, Transformation and Loading Services | IBM Infosphere Data Stage v11.7 | For ETL Services |
| Claim Scoring Tool | Claim Scoring Tool v5.0 | Used for Claims Scoring process |
| Reporting and analytics capability | SQL Server Reporting Services 2012 | Used for Reporting capabilities |

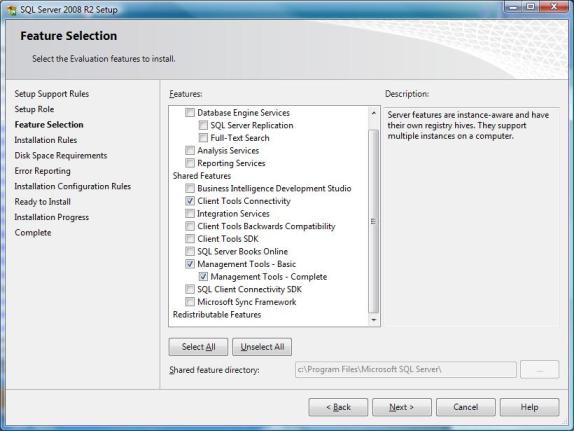
# Developer’s Guide (Data Repository access)

This section describes the developer workstation setup and use of basic SQL Server developer tools to perform common tasks. Please reference the user guide for the Microsoft SQL Server Reporting Services application for tasks related to data repository reporting.

## Developer Workstation Setup install SQL server management studio

SQL Server Management Studio (SSMS) is a main developer tool. SSMS is installed as a client-component option of the SQL Server installation along with Command Prompt tools and connectivity components. The user must select the proper components on the Feature Selection page during SQL Server installation. The figure immediately below indicates which selection to make for SSMS installation.

Figure 9: Selecting the Client Component for SSMS installation



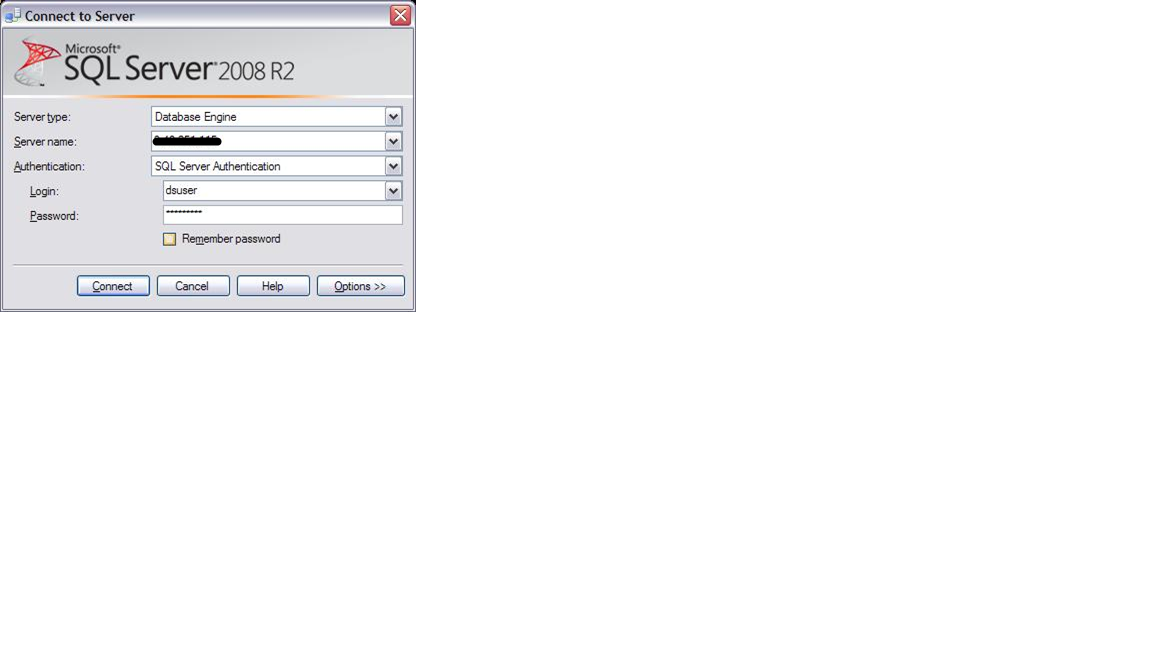
## Tools and Utilities SQL Server Management Studio

SSMS enables developers to explore PITEDR tables, views, stored procedures etc, as well as query, update, and even change data structure. Below are examples of the routine activities conducted by the DBA and DB developers supported by the SSMS interface.

### Connect to PITEDR via SSMS

To connect to the PITEDR, use the connection and database access account provided by the DBA. An example of these credentials is shown below:

Figure 10: Connecting to PITEDR database



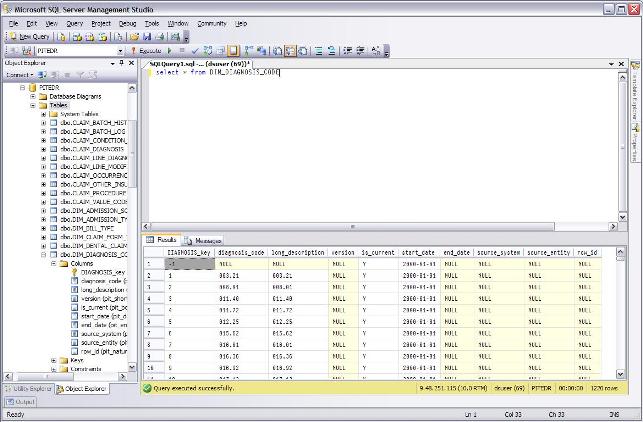
After the database connection is established a user can access all components of the PITEDR.

Note: If the database server is not accessible when attempting to connect, the user should try to ping the database server with the server host name or IP address. After doing so, he/she should contact the system/network administrators to resolve.

### Query data

To query data from the repository, click the **New Query** menu button, select database in the drop-down list, enter a SQL statement in the Editor pane, and click the **Execute** menu button. The query output will display in the Results and Messages tabbed panes, shown below:

Figure 11: Executing a Query and Viewing Query Output



### Save query result as CSV file

Right-click in the Results pane, then select **Save Results as**. Select CSV as the file type and provide a name and location for the file to be saved.

### Update Repository data:

Below is a sample SQL Update statement:

update DIM\_PLACE\_OF\_SERVICE

set start\_date to cast('2/10/2011' as date)

where pos\_key=15

### Extend Repository table column

Below is a sample SQL Alter statement:

ALTER TABLE [BATCH LOG]

ALTER COLUMN batch\_status **varchar**(**40**)

GO

### Create index:

Below is a sample SQL Create statement:

CREATE CLUSTERED INDEX [IX\_3DIGIT]

ON [dbo].[Bill Type]

([3 Digits Code])

GO

### Gathering statistics

Below is a sample SQL statement to update statistics.

UPDATE STATISTICS DIM\_INSTITUTIONAL\_CLAIM

### Using Import Export Data utility to copy data to/from the Repository

The Import/Export Data Utility contains a wizard that specifies source and target mappings for the data to be copied. A walkthrough of this process is shown via the screenshots below:

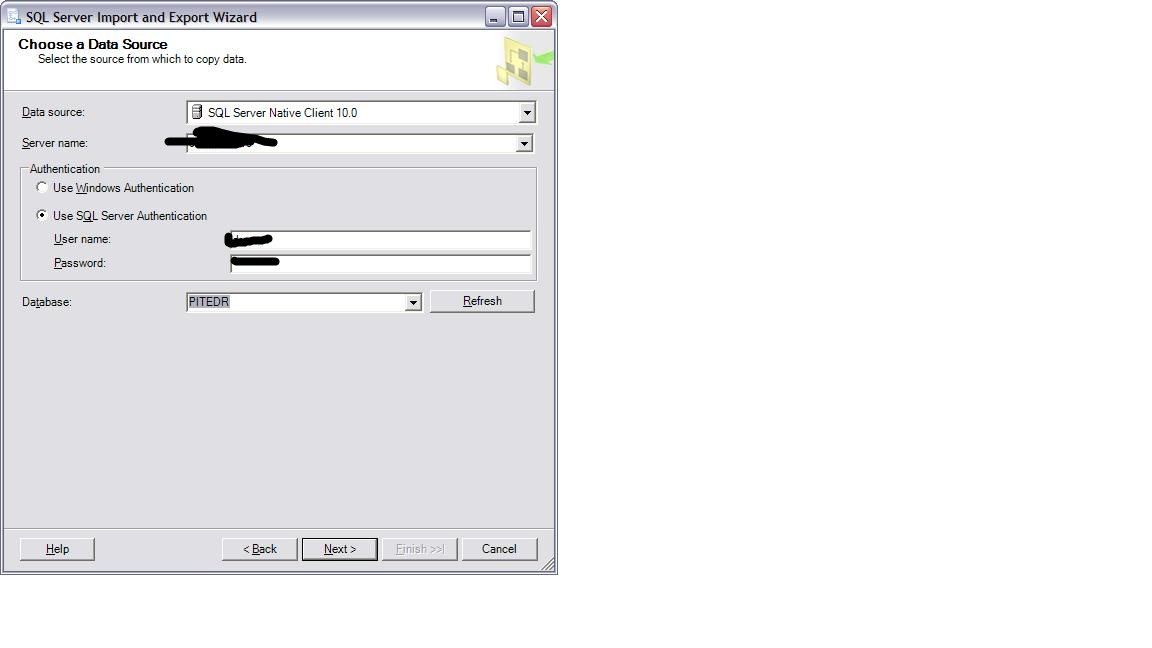
Figure 12: Using the Import/Export Wizard to Choose a Data Source

Figure 13: Using the Import/Export Wizard to Choose a Destination

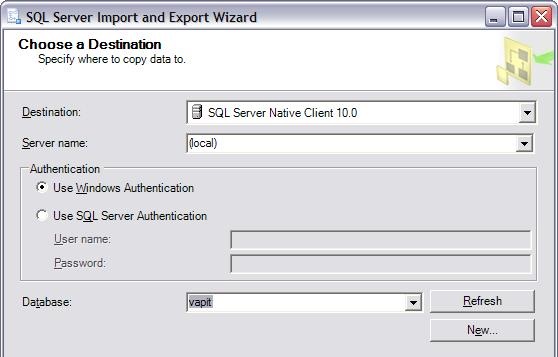


Figure 14: Using the Import/Export Wizard to Choose a Destination

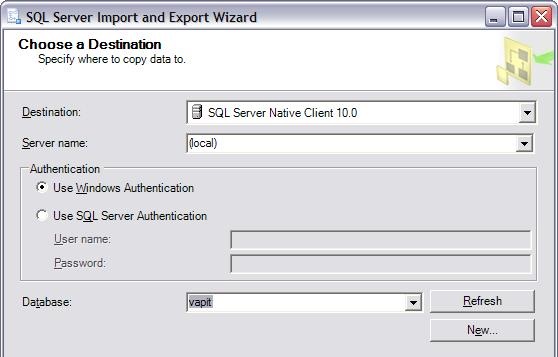


Figure 15: Using the Import/Export Wizard to Select Source tables

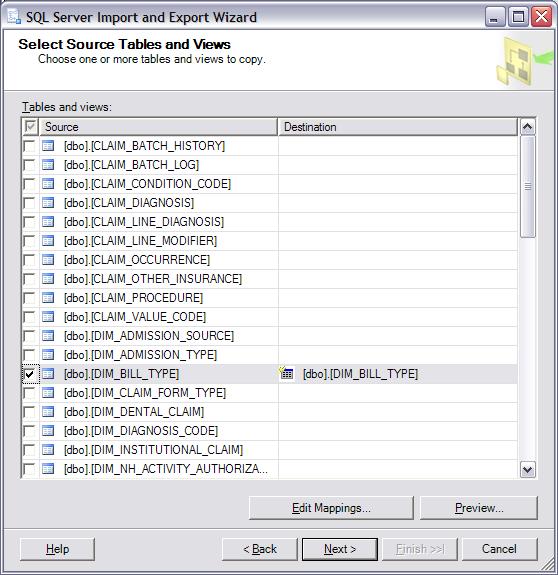
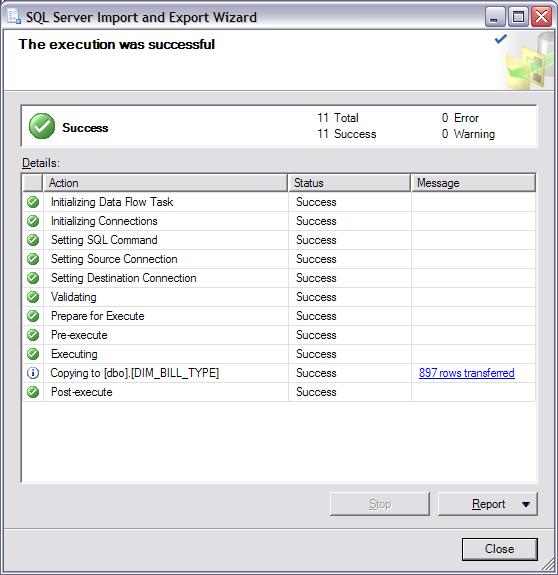


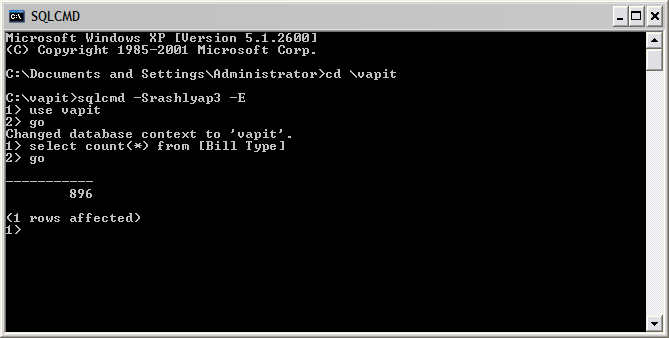
Figure 16: Successful Transfer via Import/Export Wizard



# SQL Server Command Line Tools and Utilities:

Along with developer GUI tools, SQL Server provides command line tools that are useful when running SQL queries and executing bulk data copy. The **sqlcmd** command line utility can run ad-hoc queries as well as prepared script files.

Figure 17: sqlcmd Command Line Utility



# Software Internal Documentation SQL Server Management Studio Documentation; Online Documentation

Documentation related to the tools/utilities included in the database installation can be accessed by running the SQL Server Books Online application. These documents are also available online:

* SSMS Tutorial: <http://msdn.microsoft.com/en-us/library/bb934498.aspx>
* Using the SQL Server Import and Export Wizard to Move Data: http://msdn.microsoft.com/en-us/library/ms141209.aspx
* sqlcmd Utility Tutorial: <http://msdn.microsoft.com/en-us/library/ms170207.aspx>
* bcp Utility Reference <http://msdn.microsoft.com/en-us/library/ms162802.aspx>

# Troubleshooting

Under indicated sections have been described in Production Operations Manual (PIT\_POM\_v2.0). Please refer to Section 3.0: Exception Handling.

## Special Instructions for Error Correction

Please refer to below sections from Production Operations Manual (PIT\_POM\_v2.0):

* Section 3.1: Exception Handling and Data Integrity
* Section 3.2: Dealing with DataStage Failures
* Section 3.3: Dealing with Scoring Failures

# Acronyms and Abbreviations

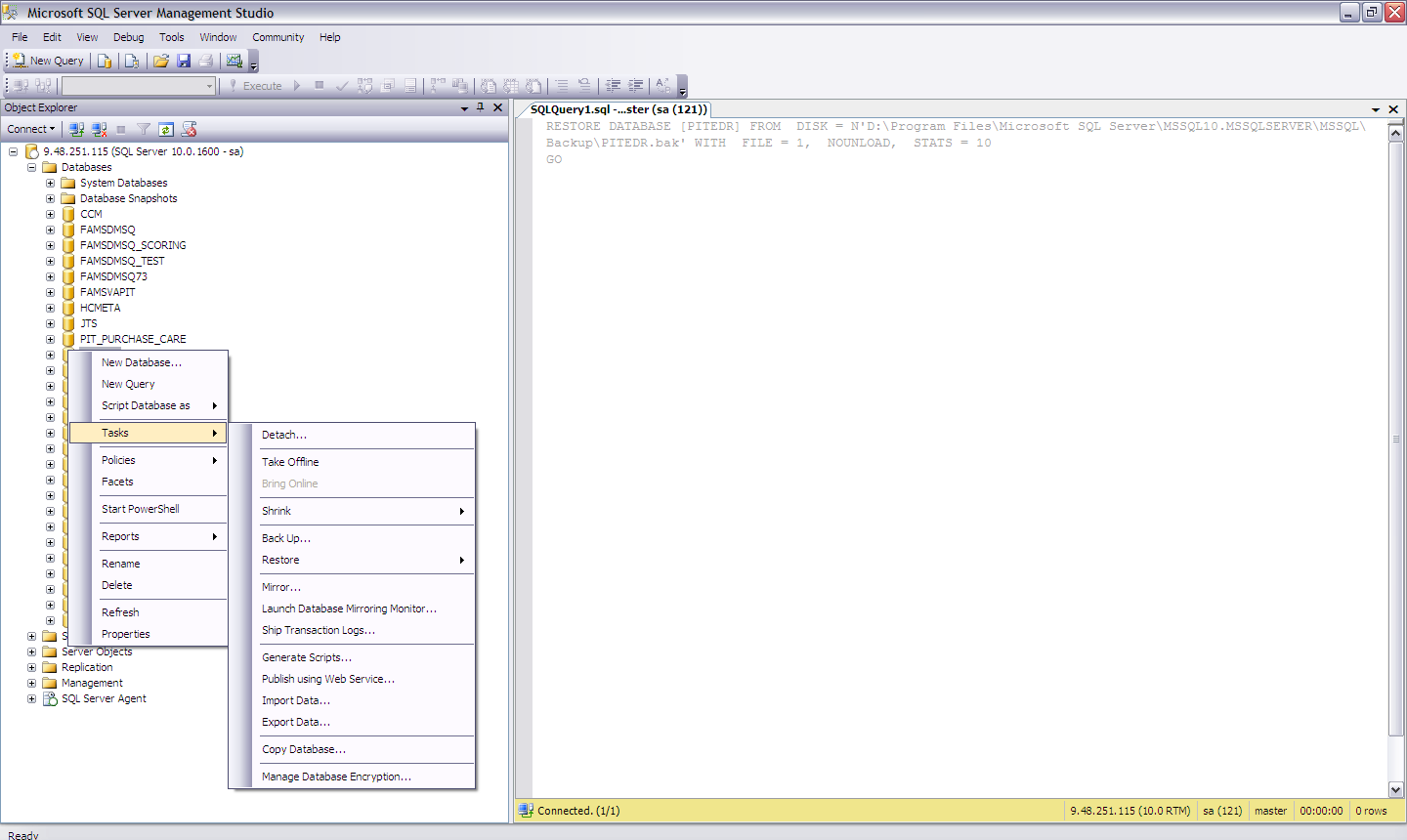
|  |  |
| --- | --- |
| **Acronym** | **Abbreviation** |
| PIT | Program Integrity Tools |
| FWA | Fraud, Waste and Abuse |
| CBO | Chief Business Office |
| PCBL | Purchased Care Business Line |
| VAMC | Veterans Affairs Medical Center |
| VISTA | Veterans Health Information Systems and Technology Architecture (VISTA) |
| FBCS | Fee Basis Claim System |
| HAC | Health Administration Center |
| AITC | Austin Information Technology Center |

# Appendix A

# The Manual Backup Process, Using a GUI

Right-click on the database which needs to be archived. Then click **Tasks** and **Back Up…** to start the backup process.

Figure 18: Starting the Backup Process



The Database box defaults to the database that was selected for backup.

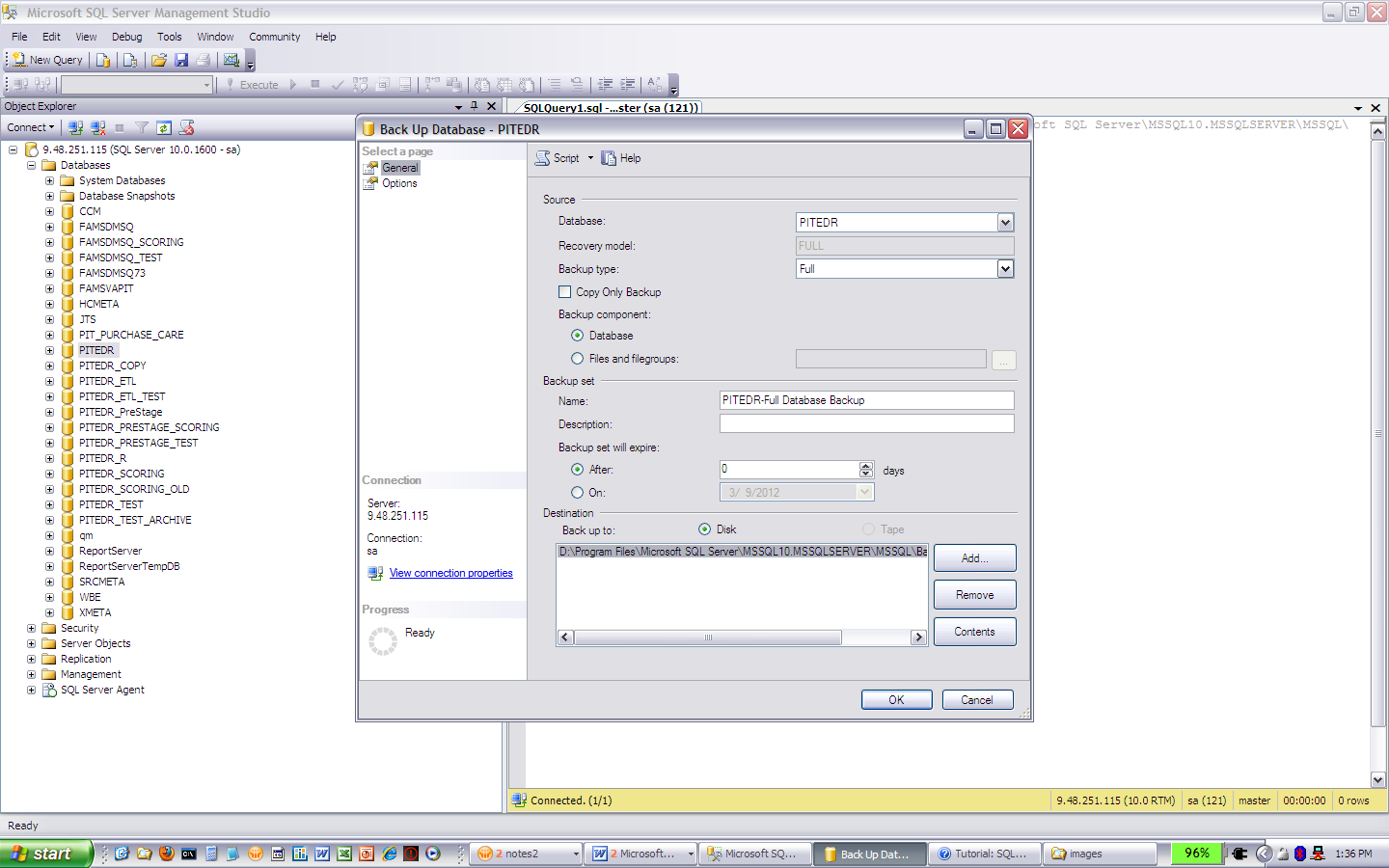
For Backup type, select Full, Differential, or Transaction Log depending on the need. A Full database backup is recommended.

For Destination:

Back up to: Check Disk option and choose one or more backup locations to store the backup file.

Click **OK** to start the backup process.

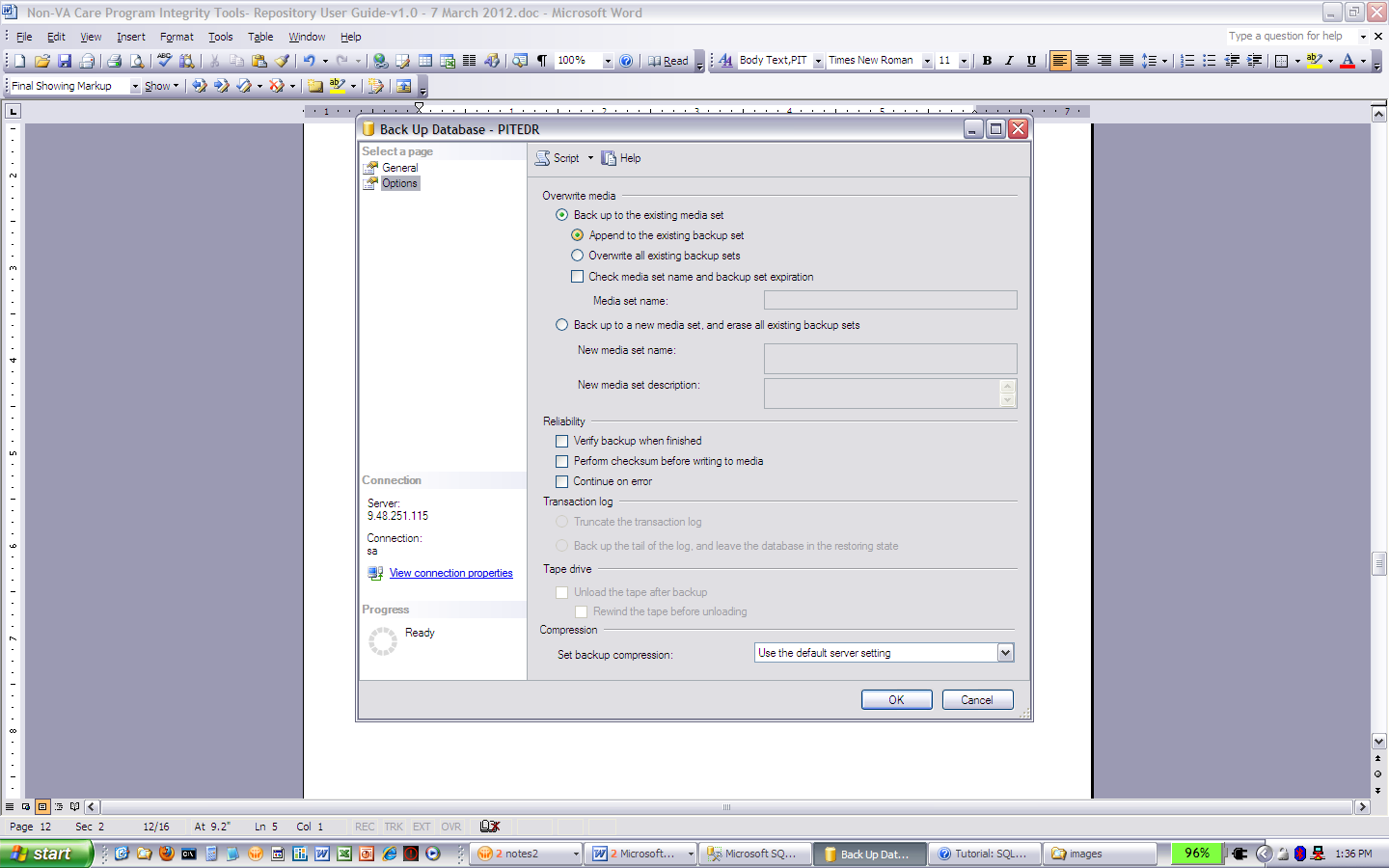
Figure 19: General View for Backing Up the Database



Backup options:

* Full backup usually goes to a new file.
* Differential backup appends to an existing file.

Figure 20: Backing Up the Database (Options)



# Index

The Program Integrity Tools User Guide does not require an index to be included.

Template Revision History

| Date | Version | Description | Author |
| --- | --- | --- | --- |
| March 2016 | 1.7 | Updated to align with new VIP policies and processes | VIP Business Office |
| December 2015 | 1.6 | Updated to align with current OI&T Documentation Standards, edited to conform with latest Section 508 guidelines, and remediated with Common Look Office tool | Process Management |
| June 2015 | 1.5 | Edited to conform with Section 508 guidelines and remediated with Common Look Office tool | Process Management |
| May 2015 | 1.4 | Reviewed and approved by PMAS Process Improvement Lockdown. Updated instructional test | Process Management |
| November 2014 | 1.3 | Updated to conform with latest Section 508 guidelines and remediated with Common Look Office tool | Process Management |
| April 2014 | 1.2 | Changed title page to clarify that version number refers to software version | Process Management |
| April 2011 | 1.1 | Formatted to current ProPath documentation standards and edited to conform with latest Alternative Text (Section 508) guidelines | Process Management |
| June 2009 | 1.0 | Initial Version | PMAS Business Office |

1. Office of Inspector General. (March 2012). *Review of VA’s Compliance with the Improper Payments Elimination and Recovery Act* (Washington, D.C.). [↑](#footnote-ref-1)