Vermont State Agency Application: VHCURES Standard Comprehensive Research Data Set

VERMONT
GREEN MOUNTAIN CARE BOARD
89 Main Street
Montpelier, VT 05620
802-828- 2177
gmcboard.vermont.gov

Application

APPLICATION INSTRUCTIONS

Introduction

The Vermont Health Care Uniform Reporting and Evaluation System (VHCURES)

The Vermont legislature authorized the collection of eligibility and claims data for Vermont residents to enable the Green Mountain Care Board (GMCB) to carry out its statutory duties that include determining the capacity and distribution of existing resources; identifying health care needs and informing health care policy; evaluating the effectiveness of intervention programs on improving patient outcomes; comparing costs between various treatment settings and approaches; providing information to consumers and purchasers of health care; and improving the quality and affordability of patient health care and health care coverage. (18 V.S.A. § 9410)

The GMCB is required to make the VHCURES data set available as a resource for individuals and entities to continuously review health care utilization, expenditures, and performance in Vermont to the extent permitted by the Health Information Portability and Accountability Act (HIPAA) and other pertinent state and federal laws.

The claims and eligibility data available under a data use agreement can be broadly grouped into three lines of business including commercial, Medicaid, and Medicare. The GMCB has independent discretion to make decisions regarding the use and disclosure of commercial insurer data. The Department of Vermont Health Access (DVHA) and the GMCB share discretion with respect to the Medicaid data subset. DVHA must approve the use and disclosure of Medicaid data and must sign the Data Use Agreement (DUA) for authorized users of the Medicaid data subset. Per an agreement with the federal Centers for Medicare and Medicaid Services (CMS), the Medicare data subset is available only to Vermont State Agencies and entities performing research that is directed and partially funded by the State of Vermont. Under a DUA between GMCB and CMS, GMCB has independent discretion to make decisions regarding the use and disclosure of the Medicare data subset by Vermont state agencies.

Vermont state agencies may apply for a standard comprehensive research data set that includes all unrestricted and restricted data elements for broad use internally and by state contractors. Non-state entities may apply for a DUA for a limited use health care claims research data set using a different application form. This type of data set excludes the Medicare data subset and is tailored to specific research purposes as approved by GMCB and DVHA if the Medicaid data subset is requested. Applicants who are non-state entities must justify requests for individual restricted data elements and explain how the requested restricted data elements are applicable to the intended research purpose.

Data Governance Council

The GMCB chartered the Data Governance Council (DGC) to oversee the stewardship of VHCURES including the development and revision of principles and policies to guide decisions on data use and disclosure. The DCG supports the GMCB decision-making process for applications requesting use and disclosure of VHCURES data sets by state agencies as addressed in this application form.

Application Review Process

This application is required of all state agencies requesting a DUA for the VHCURES standard comprehensive research data set with the option of including the commercial, Medicaid, and Medicare subsets included in the data set to support a broad spectrum of uses.

GMCB staff must deem this application complete before initiating the full review process. **This includes submission of all required and applicable optional attachments as listed in the Application Checklist in this application.** Applicants must include a full list of individuals who will have access to the data set upon the effective date of the DUA with this application. Applicants must file Individual User Affidavits (IUA) signed by the Authorized User (AU) or Principal Investigator (PI) for all data users listed on this application. AUs or PIs must ensure that IUAs are filed with GMCB for future data users prior to their access to the data set or risk forfeiture of the DUA and the data set.

After an application is deemed complete, GMCB will start the application review process that may include a public discussion of the application by the DGC. The GMCB has the discretion to approve or disapprove applications for a DUA. All requests for the Medicaid data subset must also be approved by the Department of Vermont Health Access (DVHA). The GMCB will provide DVHA with a copy of the complete application, following a review of the application by the GMCB.

The Agency of Administration (AOA) under "Procurement and Contracting Procedures" of Bulletin 3.5 is required to review and approve the DUA after the GMCB and DVHA, if applicable, have approved the application for a DUA. Applicants may also be required to obtain approval of the AHS Institutional Review Board (IRB) Committee. (See http://humanservices.vermont.gov/boards-committees/irb)

Pertaining to DUAs issued to Vermont state agencies, GMCB must review and approve requests by Vermont state agencies to re-disclose data including custom extracts to state contractors, subcontractors, or other entities external to the state agency for specified research and studies funded under Vermont state contracts and grants. Vermont state agencies must file project review forms (PRF) with the GMCB prior to re-disclosing the data set or any extracts generated from the data set. This ensures continued compliance with provisions of state and federal laws and regulations.

Final Steps in the Application Process

If approved by AOA, the GMCB and the applicant jointly enter into a DUA that is signed by the Authorized User, Principal Investigator, GMCB, and DVHA if the Medicaid data subset is included. Prior to receiving the data set approved under the DUA, all individuals accessing and using the data on behalf of the Authorized User must sign IUAs attesting to understanding the appropriate use and disclosure of the data set and agree to comply with the requirements. If GMCB declines an application, a written statement identifying the specific basis for denial of the application will be provided to the applicant. The applicant may resubmit or supplement the application to address GMCB's concerns including those of DVHA if Medicaid data are being requested. An adverse decision regarding an application may be appealed to the GMCB.

General Instructions

Applicants must complete all required sections of the application and submit an electronic copy of the completed application, including all attachments, to Roger.Tubby@vermont.gov. Incomplete applications will not be reviewed until the applicant has provided all required information. An application checklist is provided to help ensure that your application is complete. For questions about the application process, Roger.Tubby@vermont.gov or (802) 272-5599.

Definitions

Agent: Means any individual or entity (e.g., a contractor, subcontractor, grantee, or subgrantee) acting on behalf of the Authorized User and subject to the Authorized User's control or accessing the Data Set on behalf of the Authorized User.

Authorized User: The Authorized User (AU) is typically an organization or agency. The AU signatory to the Application and the DUA must have the authority to sign legally binding agreements on behalf of the organization or institution.

Custom Extract**:** A custom extract includes the minimum necessary data to support the research purpose. A custom extract is a data subset or table generated from the standard comprehensive research data set with commercial, Medicaid, and Medicare data.

This process ensures continued compliance with the requirements of the DUA and particularly supports the concept of using the minimum necessary data to support the approved research purpose. For example, if a Vermont state agency hires a contractor to analyze VHCURES data for a study of pediatric asthma in the Medicaid population, the GMCB may approve use of a custom extract that includes Medicaid paid claims data for enrollees under the age of 19 only.

Data Custodian: The data custodian is responsible for the establishment and maintenance of physical and technical safeguards to prevent unauthorized access to and use of the data set. Agencies may designate multiple data custodians for different departments and programs. The data custodian(s) typically coordinate the receipt of the approved data set from GMCB's data consolidation vendor. The principal investigator may also be the data custodian. State contractors or other agents approved by the GMCB through a Project Review to receive the data set or custom extracts must identify and file contact information for their data custodian(s) with the GMCB.

Institutional Review Board (IRB): An institutional review board (IRB), also known as an independent ethics committee (IEC), ethical review board (ERB), or research ethics board (REB), is a committee that has been formally designated to approve, monitor, and review biomedical and behavioral research involving humans.

Principal Investigator (PI): The Principal Investigator means the individual designated by the Authorized User to be responsible for ensuring compliance with all the restrictions, limitations, and conditions of use and disclosure specified in the DUA. The Principal Investigator may delegate technical responsibility to other personnel for the establishment and maintenance of security arrangements to prevent unauthorized access to and use of the data.

Project Review: Any Vermont state agency with a DUA intending to re-disclose the VHCURES data set or any custom extracts of the data set to external agents to perform state-directed and funded research must file a Project Review Form (PRF) with the GMCB for review and approval prior to the re-disclosure.

After the GMCB has reviewed a Project Review Form (CPRF) and approved re-disclosure of data to an external agent, the Vermont state agency holding the DUA may generate custom data extracts for the contractor or other approved entities. As needed, the GMCB may request its data consolidation vendor to generate custom data extracts for the contractor or allow the contractor or other approved entities to access the secured data enclave hosted by the vendor. Use of services provided by the GMCB's data consolidation vendor may require payment of a fee to the vendor. This will be determined by GMCB a case-by-case basis after discussions with the state agency holding the DUA.

Research: A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

State Entity: Vermont State agencies, contractors, or external agents performing work for the State of Vermont.

Application Checklist **(For use by the applicant. Applicants must include all required attachments and applicable optional attachments)**

Completed Application

☐ **Section 1:** Research Summary

☐ **Section 2:** Data Management Plan

☐ **Section 3:** Project Team (*Including data users for whom signed IUAs are being filed*)

☐ **Section 4:** Data Procurement and Price *(May apply to agents external to the state agency approved by the GMCB for custom extracts or access to the secure data enclave hosted by the GMCB's data consolidation vendor)*

☐ **Section 5**: Data Transmission and Receipt

☐ **Section 6:** Signatures

Required Attachments

□ **Attachment 1:** Signed Data Use Agreement (*Must be signed by the Authorized User and Principal Investigator*)

□ **Attachment 2:** Agency's Data Governance and Protection Policies and Procedures

Optional Attachments Applicable to Proposed Re-Disclosures of the Data or Extracts

□ **Attachment 3**: Copy of proposed or signed State of Vermont contract(s) or any other agreements with external agents requiring re-disclosure of the data set or custom extracts

□ **Attachment 4:** Project Review Form(s) (PRF) must be filed for every external agent identified under Attachment 3 that will be performing state-directed research requiring use of the data set or extracts of the data set

□ **Attachment 5:** Data Governance Policies and Procedures for every external agent identified under Attachment 3 that will be receiving and managing the data set or extracts of the data set

Miscellaneous Optional Attachments

□ **Attachment 6:** If applicable to this application, IRB review and approval documents including internal to your organization **and** AHS IRB Review Committee approval if you responded "No" to the HIPAA criteria cited under Section 1 item 1-5-2.

□ **Attachment 7:** Other materials requested by the GMCB for the purpose of reviewing the application

APPLICATION

Section 1: Research Summary

Section 1 summarizes the Vermont state agency's research project that may be broad and multi-focused during the term of the DUA. Answer every question in this section. If a question does not apply to your research project, indicate that the item is "Not Applicable." Do not leave a question blank or the application will be deemed incomplete.

Under Attachment 4 above, state agencies must file PRFs for state-directed research projects that may be more narrowly defined and performed by external entities under contracts, grants, or agreements. Narrowly defined research projects are not summarized in the Project Overview below in Section 1-1 but will be described in the PRFs filed under Attachment 4.

1-1. Project Overview

Authorized User Signatory Name & Title: Mark Levine, MD, Commissioner of Health

Vermont State Agency Name: Vermont Department of Health

Principal Investigator Name & Title (if different from Authorized User): Peggy Brozicevic; Research & Statistics Chief

Project Name (Should be broad and multi-use to support multiple studies under the DUA): Public Health Analyses of Medical Claims Database

Brief Project Description (Summary of subsection 1-5-1): The overall use of the health care claims research datasets is for public health surveillance, analysis and evaluation. The dataset will allow us to examine utilization for specific screenings, conditions and procedures, and by demographic groups. It will also allow us to examine utilization patterns and trends.

Project Start Date: 1/1/2018

Project End Date (Term of DUA to be determined by the GMCB):

Funding Source(s)

☒State ☒Federal ☒ If Other, please describe: March of Dimes for one project

Line of Business data subset(s) included in data request:

☒Commercial ☒Medicaid ☒Medicare

If your state agency intends to re-disclose the data to subcontractor(s) or other external parties, identify parties (Must align with documents filed under Attachment 3):

There is one contract in process. A Project Review Form and supporting materials will be submitted at a later date.

1-2. Authorized User Acknowledgements

Please initial each item indicating your acknowledgement

	I agree that I have the authority to sign legally binding agreements on behalf of the organization or institution as applicable to this application and the attached Data Use Agreement (DUA).
	I have read and agree to the terms of the attached DUA including Attachment D to the DUA as applicable to Vermont state agencies. I understand the contents of the attached DUA may only be modified or amended in writing upon mutual agreement of both parties.
	I have read and agree to cooperate with the GMCB to amend the DUA from time to time to the extent necessary for the GMCB to comply with changes to 18 V.S.A. § 9410, HIPAA, or other legal requirements that may apply to the Data Set.
	I understand and agree that I am required to file signed Individual User Affidavits (IUAs) with the GMCB for every individual data user within my organization and those employed by any state contractors, subcontractors or organizations outside my organization approved by the GMCB to access and use the VHCURES data set. I must file the IUAs prior to receipt of the data set and as new users join the project or risk forfeiture of the data set and the DUA.
	I understand and agree that I must obtain the express written approval of the GMCB to release the data set or any derived extracts of the data to any agents or parties outside my organization. I must file a Project Review Form (PRF) with the GMCB for review prior to any re-disclosure of the data set to parties outside of my organization or risk forfeiture of the data and the DUA.

1-3. Project Questions

Answer the following questions about your research project.

Yes ☒ No☐	Is the project directed by the State of Vermont?
Yes ☒ No☐	Is this project partially or wholly funded by the State of Vermont?
Yes ☐ No☒	Will the project products be used to directly generate revenues and income?
Yes ☒ No☐	Is the project useful for determining the capacity and distribution of existing health care resources?
Yes ☒ No☐	Is the project useful for identifying health care needs and informing health care policy?
Yes ☒ No☐	Is the project useful for evaluating the effectiveness of intervention programs on improving patient outcomes?
Yes ☒ No☐	Is the project useful for comparing costs between various treatment settings and approaches?
Yes ☒ No☐	Is this project useful for providing information to consumers and purchasers of health care?
Yes ☒ No☐	Is this project useful for improving the quality and affordability of patient health care and health care coverage?
Yes ☒ No☐	Does this project directly support public health activities?
Yes ☒ No☐	Does this project support educational purposes such as exploring the claims data for quality, potential uses, health services research training, or integration with other data sets?
Yes ☒ No☐	Does this project propose to link VHCURES data with any other individual record-level data sets? *If yes, describe the data sets and proposed methodology for linking in Section 1-5-4.*
Yes ☐ No☒	Does this project anticipate re-disclosure of the data set, custom extracts or analytical files generated from the data set to any identifiable external agents under contracts, grants, and agreements for research purposes that have been specified? *If yes, complete and file Attachment 3 and Attachment 4: Project Review Form. There is one contract pending. The Project Review Form and related attachments will be filed at a later time.*

1-4. Requested Data

Indicate the data files requested in this application.

File Type	Commercial Insurers	Medicaid[1]	Medicare[2]	Data Years or Date Range[3]
Medical Eligibility-VT Residents	☒	☒	☒	2007 - current

Medical Claims-VT Residents	☒	☒	☐	2007 - current
Medical Eligibility- 5% National Sample	Not applicable	Not applicable	☐	
Medical Claims- 5% National Sample	Not applicable	Not applicable	☐	
Pharmacy Eligibility	☒	☒	Not applicable	2007 - current
Pharmacy Claims	☒	☒	Not applicable	2007 - current
Medicare Part D Event- VT Residents	Not applicable	Not applicable	☒	2007 - current
Medicare Part D Event- 5% National Sample	Not applicable	Not applicable	☐	
Medicare MEDPAR	Not applicable	Not applicable	☐	

[1] *The Department of Vermont Health Access (DVHA) must approve uses and disclosure of Medicaid data.*

[2] *Medicare data may only be used for research directed and partially funded by the state of Vermont.*

[3] *VHCURES data are available on a consolidated CY quarterly or annual basis on paid claims date basis starting with CY 2007.*

1-5. Project Overview

1-5-1. Summarize the purpose and objectives of the proposed research. Describe how the research will contribute to generalizable knowledge applicable to the Vermont population, health, and health care and to the State of Vermont as applicable to the development, implementation, and evaluation of programs administered by Vermont state agencies.

Response: The Department of Health's programs and initiatives are designed to help Vermonters live fuller, healthier lives from birth through old age. We empower Vermonters with current, correct and credible information to stay safe and healthy. We work to improve access to health services such as immunizations, mammograms, HIV/AIDS testing and care, and prenatal care. We continually track and report on the health status of Vermonters, health risks and behaviors, and progress toward meeting Healthy Vermonters 2020 goals. We also focus on avoidable health inequalities.

The Vermont Department of Health has long used the hospital discharge datasets for analyses to examine overall hospitalization utilization patterns and trends, utilization for specific conditions such as injuries and asthma, and by specific demographic groups. The Medicaid claims datasets expanded our ability to analyze health care utilization in ambulatory care settings. This has enabled us to conduct analyses such as determining the percent of children receiving the recommended schedule of well child visits and examining the utilization patterns of children with specific health conditions. The VHCURES datasets allowed us to continue these types of analyses for the broader Vermont population. The addition of the Medicare data will give us the broadest representation of the Vermont population. In particular, chronic conditions are more common in the older population and therefore our ability to assess utilization patterns and trends of chronic diseases has been limited without the Medicare claims.

Examples of use include, but are not limited to medication adherence for diabetic and antihypertensive medications, percentage of adult with high blood pressure who had at least one primary care visit in the past year, the setting of care where individuals are seen following a cardiac event, medication use for control of asthma, the number of medical providers applying fluoride varnish to children under six, comparison of developmental screening rates in young children to registry data and survey data, a study of adolescent well visits within the past year with a further analysis of those without a well visit to determine when they last had a well child visit and if they were receiving other visits such as sports physicals, identification of infants with conditions included in the Birth Information Network, analysis of surveillance indicators for substance abuse and mental health, analysis of mental health conditions and concurrent substance abuse diagnosis codes for women of reproductive age, analysis of attention deficit/hyperactivity disorder/attention deficit disorder among children and youth and use of psychotropic medications, and determining the prevalence and burden of youth with serious emotional disturbance.

1-5-2. If your project requires the use of Medicaid data, is the research intended to support public health activities? If yes, explain the application of the project to public health. If no, you may be required to obtain approval to use the Medicaid data from the AHS IRB Review Committee in addition to DVHA. See Optional Attachment 6.

Response: The Medicaid data are an important component of VDH's analyses. Without the Medicaid data we would be unable to examine population health, as Medicaid provides coverage for a significant portion of the state's population.

The Department of Health also routinely compares utilization of the privately insured population to the Medicaid population to determine if there are disparities. In addition, the Medicaid claims are examined to identify changes in utilization because of changes in policy and/or reimbursement.

1-5-3. Summarize the credentials, skills, and experience of the Principal Investigator and key research staff that are evidence that the Data Set will be used to conduct and support systematic investigations guided by expertise in the subject matter and research methods, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

Response: The Principal Investigator has over 30 years of experience at the Health Department. She supervises a staff of 10 public health analysts in the Research & Statistics unit on a wide variety of public health projects. These include managing and analyzing the Vermont Uniform Hospital Discharge Data Set, producing the Vermont Hospital Report Card and conducting ongoing surveys of over 40 health care professions. This unit also provides extensive analysis of maternal and child data such as analysis of vital records data, an ongoing survey of women who recently gave birth, and managing a surveillance system of infants with birth defects or other conditions.

The key research staff are public health analysts who are either managing public health surveillance programs or providing analytical support to Department programs. Public health analysts are required to have training and experience in the analysis of data. These analysts are providing a wide variety of analyzes and evaluations for the Department. Products are crosschecked by other analysts and reviewed by supervisors and the Public Health Statistics Manager.

Most of the staff who signed affidavits are analysts. Additional staff signing affidavits include program staff who will not be accessing the VHCURES data directly, but are working with analysts and may review either row level data or reports prior to the suppression of small cells.

1-5-4. Explain how you will ensure that your organization and external agents performing state-directed research will have access to the minimum necessary data to support specified research purposes and projects.

Response: The VHCURES data is one of multiple data systems used by staff in their research. The Department of Health has many sensitive data sets and staff are trained to use only the minimum necessary data to support their projects. All staff are required to complete HIPAA training prior to accessing any Health Department data, sign a confidentiality agreement and repeat the HIPAA training every two years. A professional environment is maintained throughout the department.

Supervisors are responsible for ensuring all data are handled appropriately. All Division Directors and program managers were sent a copy of the VHCURES DUA with key requirements highlighted in an email.

1-5-5. List and briefly describe any unidentifiable or identifiable record-level data files you are planning to use in conjunction with the requested data. If the files will be linked explain the methodology for linking the data; if applicable which files include direct personal identifiers, and how the identity of individuals and their PHI will be protected from disclosure.

Response: The Birth Information Network (BIN) uses the VHCURES as part of their case finding process and links the potential cases identified through VHCURES to the BIN and to the birth file, both of which include names.

The Birth Information Network (BIN) was established by Vermont legislation in 2003 (18 V.S.A. § 5087) to conduct statewide, population-level surveillance of selected structural birth defects and other congenital conditions in order to improve outreach and referral services for families with children with special health needs, ensure adequate services are available for children and their families, evaluate efforts to prevent health problems and document possible links between environmental and chemical exposure with the special health conditions of Vermont's infants and children.

In 2006, the Vermont Birth Information Network began collecting information about Vermont-resident children diagnosed in the first year of life with one or more of 33 structural and chromosomal birth defects, seven metabolic and endocrine conditions, congenital hearing loss, and very low birth weight (infant born with a birth weight less than 1500 grams).

The BIN uses multiple data sources to identify potential cases and then conducts follow up to confirm or rule out those cases. At the time of the program's start, it relied on predominantly on four data sources: Medicaid claims, reports from Vermont hospitals and physicians, vital records, and records maintained by the Vermont Department of Health's Children with Special Health Needs program (CSHN).

In 2011, additional legislation was passed authorizing the BIN to collect information on additional conditions. The 2011 legislation also specifically authorized the BIN to collect information from the Vermont Healthcare Claims Uniform Reporting and Evaluation System (VHCURES).

VHCURES and the other data sources listed above are used to identify potential cases. The program then requests medical records that are reviewed and compared to the birth defects case definitions, as published by the National Birth Defects Prevention Network. The BIN contracts with a clinical geneticist to review records and make a final determination as to whether the case meets the definition.

VHCURES is a secondary data source for case finding for the BIN. Primary data sources are those with identifiable data, or where the BIN can readily request the names. VHCURES is used after case finding for the calendar year has been completed using the other data sources available. The procedure is as follows:

- The VHCURES data is examined for infants with one or more of the conditions included in the BIN.
- These cases are linked to the BIN based on infant's date of birth and condition to determine if these infants are already included in the BIN.
- For those infants that do not link to a BIN case, the infant is linked to the birth file to identify the infant.
    - Infant's date of birth is not unique enough to link to the birth file, even with gender included. Therefore, the infant is first linked to the mother within VHCURES using the insurance policy number. Then using both mother's and infant's dates of birth the link is made to the birth certificate.

- Once the infant's name is known the BIN can double check to determine if the infant has been previously identified. If not, standard BIN procedures are followed to accept or rule out the case.

VHCURES identifies only a few new cases for the BIN. These are cases where the birth defect is identified after the infant was discharged from the delivery hospital, the treatment for the condition is conducted either on an outpatient basis or in an out of state hospital, and the infant is covered by private insurance.

The legislation establishing the BIN set strict confidentiality requirements. The data are maintained in an Access database in a secure folder that is accessible only to BIN staff. Paper medical records and any case-level reports that contain identifiable, or indirectly identifiable information, are stored in locked file cabinets and securely shredded when no longer needed.

1-5-6. Identify and briefly describe the funding source(s) for the proposed research including both internal and external sources that may be in the form of state and federal funding and grants. Describe the relationship between the funding source(s) and your organization.

Response: Funding for this project will be a combination of state funds and federal grants. The Department of Health's programs and staff are funded substantially by federal grants, primarily from the Centers for Disease Control and Prevention (CDC), the Health Resources and Services Administration (HRSA), and the Substance Abuse and Mental Health Services Administration (SAMHSA). These grants support programs and staff, and require data for program planning and evaluation of program activities. The VHCURES data will provide some of the data required.

The March of Dimes is funding a one-year grant project in Vermont, with funding they received from the CDC. The project is "Using birth defects surveillance methodology to assess the incidence of neonatal abstinence syndrome". The CDC provided funding to the March of Dimes to administer this project, and Vermont was one of three states awarded a grant.

1-5-7. Explain whether any component of the project was review and approved by an Institutional Review Board (IRB). If yes, attach the IRB review and approval under Attachment 7 to this application.

Response: The March of Dimes grant, "Using birth defects surveillance methodology to assess the incidence of neonatal abstinence syndrome" was reviewed and approved by the Agency of Human Services Institutional Review Board. A copy of the approval is attached.

Section 2: Data Management Plan

Section 2 relates to the policies and procedures your organization will use to ensure the proper management of the VHCURES standard comprehensive research data set and custom extracts derived from the data set. The GMCB recognizes the applicability of best practices for information security and privacy used in the CMS Data Privacy Safeguard Program (DPSP)[1] to the review of VHCURES DUA applications. Respond to every question about your organization's and those of approved entities external to your organization policies and procedures to ensure technical and administrative safeguards over the data.

Please answer the questions in each section with references to any attached documents including relevant page and/or section numbers. **Do not simply cite a cross-reference to the policy and procedure documents included under Attachment 2 and 5 of this application in lieu of answering each question. If questions are not answered completely, the application will be deemed incomplete.**

Any Project Review Forms (PRF) filed with this application for external agents under Attachment 4 may cite cross-references to this application for the same items in Section 2 below. Instructions are included on the PRFs.

[1] "Data Privacy Safeguard Program Information Security and Privacy Best Practices" listed under Additional Resources published on https://www.resdac.org/resconnect/articles/158

2-1. Physical Possession and Storage of Data Files

Include specific references to the Data Governance and Protection policies and procedures documents filed with this application under Attachments 2 and 5 in your responses to the items below. ***Do not simply cite a cross-reference to the policy and procedure documents in lieu of answering each question.***

2-1-1. Describe how your organization will maintain an accurate and timely inventory of the VHCURES standard comprehensive research data set including original files received and any derived files used within your organization or released to external agents under state contracts and agreements.

Response: The AHS Data Custodian will manage the VHCURES database using standard Agency of Digital Services procedures. AHS will receive the VHCURES database from the vendor as is. It will never change until AHS receives a subsequent update from the vendor. The Data Custodian maintains the VHCURES database in a secure folder that is accessible only to staff that have approved affidavits.

Staff with approved affidavits have READ access to the VHCURES files and access to a separate secure folder created by the Data Custodian for use by the VHCURES analysts. Analysts typically select the minimum necessary data for their specific project, and save the data in an SPSS or SAS data file. All derived files, programs and draft tables and reports will be kept in this secure folder. The PI will periodically (quarterly or a schedule to be determined with the GMCB) contact all staff with active affidavits to request a description of current or planned projects

The PI will be responsible for cataloging any files released under Health Department contracts.

2-1-2. Describe how your organization will ensure and monitor the compliance of all members of research teams both in-house and those employed by approved external agents with privacy and security policies and procedures as described in the documentation filed under Attachments 2 and 5 to this application and as required by the DUA.

Response: The PI will periodically (quarterly, or a schedule to be determined with the GMCB) contact all staff with active affidavits. Part of this contact will include a reminder about the privacy and security requirements.

Supervisors are responsible for ensuring that staff with access to the VHCURES data comply with all privacy and security policies and procedures. All Division Directors and program managers were sent a copy of the VHCURES DUA with key requirements highlighted in an email.

Most of the staff who will be accessing the VHCURES data directly work in the Public Health Statistics Section of Health Surveillance and are supervised by the PI, the Public Health Statistics Chief, and other statistics supervisors who have signed affidavits.

In addition, any concerns from staff about compliance will be reported to the PI.

2-1-3. Describe the procedures your organization will take to track the status and roles of the research team and notify GMCB of any project staffing changes.

Response: Staff are requested to notify the PI if they no longer need access to the VHCURES database or are leaving the Department of Health. In addition, the PI will periodically (quarterly or a schedule to be determined with the GMCB) contact all staff with active affidavits to request a description of current or planned projects or if they no longer need access to the VHCURES database. The PI will notify the GMCB when a staff member leaves or no longer requires access to the VHCURES data.

2-1-4. Describe your organization's training programs that are used to educate staff on how to protect sensitive data with personally identifiable information, protected health information, and other sensitive financial, socioeconomic, and personal information.

Response: All staff are required to successfully complete HIPAA training before being granted access to Health Department data and to sign a confidentiality agreement. Staff are required to repeat HIPAA training every two years.

Some staff that routinely work with sensitive data have a performance measure regarding maintaining confidentiality of data as part of their annual review.

2-1-5. Describe the protocol that would be followed by your organization or that of approved external agents, if applicable, to report and mitigate a breach in the security of the data set. Who will be responsible for notifying the GMCB (and CMS as applicable to Medicare data) of any suspected incidents of a breach in the security of the VHCURES data?

Response: The Agency of Human Services has policies in place if an employee (or contractor) mishandles a dataset or if there is a HIPAA breach. The Department of Health follows those policies. Any misconduct or breaches will be reported to the PI, who will be responsible for immediately notifying the Green Mountain Care Board, and notifying CMS within 1 hour if the actual or suspected breach includes Medicare data. The PI will also report to her supervisor and Human Resources any misconduct by an employee, which will then be handled by established HR policies. Any HIPAA breaches will be reported to the Department's HIPAA Officer, which will then be handled by established HIPAA policies.

2-1-6. What actions will your organization and approved external entities take to physically secure the data files? This includes files in motion, or on servers, local workstations, and hard media.

Response: All AHS database servers reside in the State's data center at National Life in Montpelier. The physical and environmental controls are managed by the Agency of Digital Services (ADS).

All computers require an authorized login and password. The Health Department complies with all ADS policies and requirements for password management. Staff are prohibited from storing data on portable devices.

Visitors to the Health Department are accompanied by staff members at all times. Visitors are required to sign in at the lobby. When they reach the office they are visiting, they need to call from a phone in the hallway and identify the person they are meeting. They are then met at the door and accompanied while in the office.

2-1-7. Please explain if your organization intends to transmit, store, or transfer the data set or any derived files outside the continental United States.

Response: The Health Department does not intend to transmit, store, or transfer the VHCURES database or any derived files outside the continental United States.

2-2. Data Sharing, Electronic Transmission, Distribution

Include specific references to the Data Governance and Protection policies and procedures documents filed with this application under Attachments 2 and 5 in your responses to the items below. ***Do not simply cite a cross-reference to the policy documents in lieu of answering each question.***

2-2-1. Describe what your organization's policies and procedures will be for sharing, transmitting, and distributing the VHCURES data set and any derived files.

Response: The data will be stored in a SQL database on a secure Agency of Human Services server. The full VHCURES database will be stored in a single location. AHS SQL Server Policies and Procedures will be followed (AHS SQL Server Environment Policies, 7.5). Assessment of user and system access will be continuously scrutinized and audited by Data Base Administrators.

Staff with approved affidavits have READ access to the VHCURES files and access to a separate secure folder created by the Data Custodian for use by the VHCURES analysts. Analysts typically select the minimum necessary data for their specific project, and save the data in an SPSS or SAS data file. All derived files, programs and draft tables and reports will be kept in this secure folder.

2-2-2. The GMCB's preferred method of transmission of the data files is through a secure File Transfer Protocol (SFTP) transmission. If you anticipate requesting encrypted hard media, please explain the reasons that SFTP is not an option.

Response: The Data Custodian will receive the data files through a Secure File Transfer Protocol transmission.

2-2-3. Would your organization and approved external agents be interested in accessing a hosted data enclave or a researchers' workbench environment eliminating the transmission of data files via SFTP or via encrypted hard media outside of the hosted enclave? If yes, would the interest hold if there are fees for this service? If not interested at all or cautious, please explain your concerns.

Response: The Health Department has concerns about accessing the VHCURES data through a hosted data enclave or similar environment.

1. Cost is a consideration. The Health Department has multiple users of the data and the cost could be prohibitive.
2. What resources would be available for working with the data? Approximately half of the Health Department staff use SPSS, while the other half use SAS. Would these be available?
3. How would the results/tabulations/tables be exported from the enclave? Would this be timely? Would there be restrictions? For example, if only tables with data that have already been suppressed can be exported, that could hamper review and verification of analyses.

2-2-4. Describe your organization's methods and those of approved external agents for tracking, monitoring, and auditing access and use of sensitive data such as the VHCURES data set.

Response: The PI sends affidavits for use of the VHCURES data to the GMCB, who in turn notifies the AHS Data Custodian. Staff with approved affidavits are entered in a VHCURES-specific security group by the Data Custodian. AHS Data Services audits all system administrator security groups to all servers daily through an automated process. The VHCURES-specific security groups are manually synchronized with the GMCB based on their list of approved users. This is done by the Data Custodian whenever the GMCB notifies him to add or remove a given user. User access to the data is controlled by the login and password of users.

The use of the data will be tracked and monitored by the PI. The PI will periodically (quarterly or schedule to be determined with the GMCB) contact all staff with active affidavits with a reminder of the requirements of the DUA and to request a description of current or planned projects, or if they no longer need access to the VHCURES database. Additional review of the use of the data will occur during the review process used by the Department of Health for all publications.

External agents will need to provide their procedures for tracking, monitoring and auditing access and use of the VHCURES data. They will not be provided access until their procedures have been reviewed and approved by the Health Department and the GMCB.

2-2-5. Describe the policies and procedures and procedures your organization and approved external agents use to define data access privileges for individual users of the data, including the Principal Investigator, Data Custodian, analysts and researchers, administrative support, and IT support.

Response: Data access privileges are based on job responsibilities at the Health Department. The PI, analysts and researchers all have job responsibilities that include the use of the VHCURES data. Affidavit requests included a requirement to describe how the analyst is currently using the data (for anyone currently using VHCURES data) and any new anticipated uses.

Similarly, the Data Custodian and IT support staff have privileges defined by their job responsibilities. The guidelines for access to VHCURES server and database are outlined in AHS SQL Server Environment Policies, 7.5.7.

2-2-6. Explain the use of technical safeguards for data access (which may include password protocols, log-on/log-off protocols, session time out protocols, and encryption for data in motion and data at rest).

Response: Approved users have access to the data through their login name and password. Passwords are required to be complex, and must be changed regularly. The Health Department complies with all ADS policies and requirements for password management.

Staff are instructed to lock their computer if they will be away from their desk. As a backup, if there is no activity in 10 minutes, the computer screen is automatically locked.

2-2-7. If approved external agents will have access to the data please describe how that organization's analysts will access the data file, e.g., VPN connection, travel to your organization, or house the data at other locations.

Response: Currently there are no approved external agents with access to the VHCURES data.

2-2-8. If additional copies of the data will be housed in separate locations, list the locations and describe how the data will be transferred to these locations.

Response: No additional copies of the data will be housed in another location.

2-3. Data Reporting and Publication

2-3-1. Explain your process for reviewing publications prior to dissemination to ensure accurate and appropriate representation of your data sources, analytic methodology, results, caveats, and disclaimers. Describe how your publications will be reviewed to ensure compliance with requirements in the DUA addressing small n suppression, disclaimer of any GMCB endorsement of findings, and data source citation.

Response: The Health Department has established procedures for reviewing publications prior to dissemination, and these procedures will be used for publications that include VHCURES data.

Analyses are reviewed by a second analyst who verifies the analyses and reviews the publication. The analyst's supervisor then reviews the publication. The final step is the review by the Public Health Statistics Chief.

These reviews include suppression of small numbers, data source citation and the disclaimer of any GMCB endorsement of the findings.

2-4. Completion of Research Tasks and Data Destruction

2-4-1. Describe how you will complete the Certificate of Data Destruction for the data set and derived files stored by your organization or by approved external agents and how the data will be deleted, destroyed or rendered unreadable by all parties with access to the files upon completion of the project.

Response: If the VHCURES data were to be destroyed, ADS would use a disk-wipe algorithm to ensure CMS compliance. This would apply to both the folder/server where the full VHCURES database is stored and the shared folder used by the analysts with access to the VHCURES data. ADS staff would be responsible for the completion of the Certificate of Data Destruction.

2-4-2. Describe your organization's policies and procedures and those of external agents used to protect VHCURES data files when individual staff members of research teams terminate their participation in research projects (which may include staff exit interviews, return of passkeys, and immediate access termination for example).

Response: User access to VHCURES data is determined by login name and password. When a staff person no longer requires VHCURES data, the PI will notify the GMCB who will in turn notify the Data Custodian. The Data Custodian will remove the name from the VHCURES-specific security group. For staff who resign from the Health Department, their logins will automatically be terminated.

External agents will be required to describe their policies and procedures to protect the VHCURES data when a staff member leaves the project before access to the data is approved.

2-4-3. Describe your organization's policies and procedures to ensure original or derived data files, including non-published aggregate reports, are not used following the completion of the project.

Response: If the Health Department project were to end, the Data Custodian would systematically erase the VHCURES database and backups. The shared folder used by analysts of the data would also be erased by the Data Custodian. This folder would include all of the derived files used for specific analyses, as well as non-published reports and analyses.

In addition, the Department of Health's established procedures for reviewing all publication prior to release would flag any unauthorized use of the VHCURES data.

Section 3: Project Team

In Section 3-5, list the anticipated individual users, their respective organizations including state agencies and external agents such as state contractors and subcontractors, and project roles. **Signed IUAs for individual users within your organization and those employed by external entities accessing the data must be filed prior to receipt of the VHCURES data set.**

3-1. Authorized User (State Agency)

Please provide contact information for the Authorized User's signatory.

Name and Title of Signatory for the Authorized User
Mark Levine, MD Commissioner of Health

Organization Name
Department of Health

Street Address
108 Cherry St

City Burlington	State VT	Zip 05401

Telephone 802-652-4155	Email Mark.Levine@vermont.gov

3-2. Principal Investigator (State Agency)

Please provide contact information for the PI if different person than the AU.

☐Same as Authorized User Signatory

Name and Title of Principal Investigator
Peggy Brozicevic, Research & Statistics Chief

Organization Name
Department of Health

Street Address
108 Cherry St

City Burlington	State VT	Zip 05401

Telephone 802-863-7298	Email Peggy.Brozicevic@vermont.gov

3-3. Data Custodian(s)

Provide contact information for the data custodian for your organization and the data custodians for any external agents such as state contractors, subcontractors or other organizations that will storing the VHCURES data set or derived files.

Name and Title of Data Custodian (State Agency) Craig Benson, Director of Data Services		
Organization Agency of Human Services		
Street Address 108 Cherry St		
City Burlington	State VT	Zip 05401
Telephone 802-859-5906	Email Craig.Benson@vermont.gov	

Name and Title of Data Custodian Kevin J. Stapleton, Database Administrator		
Organization Agency of Human Services		
Street Address 108 Cherry St		
City Burlington	State VT	Zip 05401
Telephone 802-859-5949	Email Kevin.J.Stapleton@vermont.gov	

Name and Title of Data Custodian Joshua Harless, Database Administrator		
Organization Agency of Human Services		
Street Address 280 State Dr		
City Waterbury	State VT	Zip 05671
Telephone 802-241-0550	Email Joshua.Harless@vermont.gov	

Name and Title of Data Custodian

Stuart Levasseur, Systems Analyst

Organization

Agency of Human Services

Street Address

280 State Dr

City Waterbury	State VT	Zip 05671

Telephone 802-241-0567	Email Stuart.Levasseur@vermont.gov

3-4. Individual Users

Identify all individuals from state agencies and external agents who will be participating on this project. These individuals may be project managers, analysts, IT professionals, or any other person who may have access to row-level data or aggregate reports prior to the suppression of small n. You must attach a signed individual user affidavit for each of these individual users prior to the receipt of the data after the DUA is approved including any users not identified on this list when this application was submitted.

Name	Organization	Project Role or Title
Brozicevic, Peggy	VDH/HS	PI/Research & Statistics Chief
Braner, Moshe	VDH/HS	Public Health Analyst
Carroll, Barbara	VDH/HS	Public Health Analyst
Davy, John	VDH/HS	Public Health Analyst
Hata, Teri	VDH/HS	Public Health Analyst
Hicks, Jennifer	VDH/HS	Research, Epi & Evaluation Chief
Jones, Amanda	VDH/HS	Public Health Analyst
Kall, Denise	VDH/HS	Public Health Analyst
Kasehagen, Laurin	CDC	MCH Epidemiologist Assignee
Kenny, Michael	VDH/HS	Public Health Analyst
Kinner, Patrick	VDH/HPDP	Chronic Disease Evaluation Director
Maiberger, Matthew	VDH/HPDP	Data & Reporting Coordinator
Martin, Brennan	VDH/HS	Public Health Analyst
McCoy, Richard	VDH/HS	Public Health Statistics Chief
Meddaugh, Paul	VDH/HS	Public Health Analyst
Miller, Robin	VDH/HPDP	Oral Health Director
O'Connor, Bryan	VDH/Business Office	Financial Manager
Orantes, Lucia	VDH/HS	Public Health Analyst
Roemhildt, Maria	VDH/HS	Public Health Analyst
Schroer, Lisa	VDH/HS	GIS Intern
Staskus, Mallory	VDH/HS	Public Health Analyst
Wade, Anita	VDH/HS	CSTE Epidemiology Fellow
Wolforth, Jane	VDH/Planning	Senior Health Policy Analyst

Name	Organization	Project Role or Title
Young, Peter	VDH/HS	GIS Manager

HS – Health Surveillance
HPDP – Health Promotion and Disease Prevention

Section 4: Data Procurement and Price

There will be no fee charged to state agencies that receive the data set via a secure file transfer protocol (SFTP) or encrypted hard media, if approved by the GMCB. The authorized user will receive the data from the GMCB's designated data processing vendor.

In the future, the GMCB may be offering access to the data through a hosted data enclave. This would eliminate or be an additional option for accessing the data via electronic SFTP transmission of the record-level data. GMCB will notify the authorized user for the DUA when this service becomes available as an option and how it will work as to number of user seats and pricing.

There may be fees for custom extracts generated from the standard comprehensive research data set as requested by the state agency. The GMCB strictly prohibits the transmission or shipping of copies or derived extracts of the VHCURES data set to external agents. Custom extracts can be generated to support the data stewardship principle of disclosing the minimum necessary data to support the research purpose. Data users may be authorized to access a secured data enclave hosted by the vendor. Use of services provided by the GMCB's data consolidation vendor may require payment of a fee to the vendor. Onpoint Health Data will manage any invoicing for fees.

The GMCB's designated vendor for the VHCURES Standard Comprehensive Research Data Set and custom extracts is:

Onpoint Health Data

Mailing Address:
75 Washington Avenue, Suite 1E
Portland, ME 04101

Physical Address:
55 Washington Avenue
Portland, ME 04101

Main Phone: (207) 623-2555

www.onpointhealthdata.org

Section 5: Data Transmission and Receipt

Use of an electronic secure File Transfer Protocol is the preferred mode of release for approved data extracts. Onpoint Health Data, the GMCB's data consolidation and warehousing vendor will provide an "Electronic Data Transmission Readiness and Logistics Checklist" to assist you in determining whether you are able to receive the transmission.

Please identify your primary contact below for setting up the logistics for SFTP transmission of the approved data extract. The primary contact must either be the Authorized User or Principal Investigator or Data Custodian identified on the DUA or be designated by the AU or PI.

As noted under Section 4, the GMCB may offer access to the data via a hosted data enclave in the future. Authorized users will be notified when this service becomes available.

Primary Contact for Planning Data Transmission Logistics

Name: Craig Benson
Title/Role in the Project: Director of Data Services/ VHCURES Data Custodian
If not AU, PI or DC, designated by:
Email Address: Craig.Benson@vermont.gov
Phone Number: 802-859-5906
Organization/Agency Affiliation: Agency of Human Services
Street, City, ZIP Address: **108 Cherry St, Burlington, VT 05401**

Section 6: Signatures

All statements made in this application are true, complete, and correct to the best of my knowledge.

Authorized User Name: Mark Levine, MD

Signature:

Date: 12/22/17

Principle Investigator Name (if different from Authorized User): Peggy Brozicevic

Signature: Peggy Brozicevic

Date: 1/4/18

Data Custodian Name: Craig Benson

Signature:

Date: 1/5/18

GMCB Processing Section

For GMCB Use Only

Applicant Organization or Entity Name:

Data Types: Commercial ( ) Medicaid ( ) Medicare ( )

Application Receipt Date/GMCB Initials:

Date Application Deemed Complete:

DVHA Application Approval Date:

GMCB Application Approval Date/GMCB Initials:

Date Applicant Notified of Approval:

Application Disapproval Date:

Date Applicant Notified of Disapproval/GMCB Initials

Summary of reasons for disapproval:

Date Application Deemed Incomplete/GMCB Initials:

Date Applicant Notified Application Deemed Incomplete:

Summary of reasons the application deemed incomplete:

Date Application Deemed Incomplete Resubmitted:

DVHA Application Approval Date:

GMCB Resubmitted Application Approval Date /GMCB Initials:

Date Applicant Notified of Approval of Resubmitted Application:

Resubmitted Application Disapproval Date/GMCB initials:

Summary of reasons for disapproval:

Medical Claims-VT Residents	☒	☒	☒	2007 - current
Medical Eligibility- 5% National Sample	Not applicable	Not applicable	☐	
Medical Claims- 5% National Sample	Not applicable	Not applicable	☐	
Pharmacy Eligibility	☒	☒	Not applicable	2007 - current
Pharmacy Claims	☒	☒	Not applicable	2007 - current
Medicare Part D Event- VT Residents	Not applicable	Not applicable	☒	2007 - current
Medicare Part D Event- 5% National Sample	Not applicable	Not applicable	☐	
Medicare MEDPAR	Not applicable	Not applicable	☐	

[1] *The Department of Vermont Health Access (DVHA) must approve uses and disclosure of Medicaid data.*

[2] *Medicare data may only be used for research directed and partially funded by the state of Vermont.*

[3] *VHCURES data are available on a consolidated CY quarterly or annual basis on paid claims date basis starting with CY 2007.*

Attachment 2

AHS SQL Server Environment

Policies - Version 4.5

Procedures – Version 3.7

Vermont Agency of Human Services

AHS SQL Server Environment

Policies

Version 4.5

Revision History

Date	Version	Description	Author
January 19, 2005	1.0	Created document	Craig Benson
November 17, 2011	1.1	Updated for AHS: updated scope, updated definitions, added references section, added database cataloging policy, updated provisioning policy, updated database backup policy, updated all password-related policies, added vendor / contractor access policy.	Craig Benson
December 19, 2011	1.2	Updated definitions, collapsed backup validation policy into backup policy, removed email configuration section (already referenced in standards document), updated provisioning policy, updated security policy, updated database design policy, added documentation policy	Craig Benson
January 24, 2012	1.3	Updated data access request policy, glossary and references.	Craig Benson
February 29, 2012	1.4	Added Server / Database Access section in Security policy.	Craig Benson
April 10, 2012	1.5	Updated document file versions in Document Policy.	Craig Benson
October 10, 2012	1.6	Updated section 5 and Deployment Policy.	Craig Benson
March 13, 2013	1.7	Updated for Windows7 / Office 2010 compatibility, updated footer address, updated Documentation Policy, updated SQL Server Purpose Policy	Craig A. Benson
May 7, 2013	1.8	Added encryption policy. Updated documentation policy.	Craig A. Benson
July 17, 2013	1.9	Added SQL desktop tools policy. Updated documentation policy. Updated coding policy.	Craig A. Benson
September 17, 2013	2.0	Updated SQL Server provisioning policy. Updated documentation policy. Added database update policy. Added SQL Server patching policy. Replaced all instances of “AHS Computer Operations” with “DII Server Administrators”.	Craig A. Benson
September 24, 2013	2.1	Updated file paths in database backup policy. Updated database cataloging policy.	Craig A. Benson
January 7, 2014	2.2	Updated database cataloging policy	Craig A. Benson
January 16, 2014	2.3	Updated documentation policy. Added migration policy.	Craig A. Benson
February 13, 2014	2.4	Updated documentation policy.	Craig A. Benson
February 19, 2014	2.5	Updated documentation policy. Updated SQL Server patching policy.	Craig A. Benson

Date	Version	Description	Author
March 12, 2014	2.6	Updated documentation policy.	Craig A. Benson
May 20, 2014	2.7	Updated database backup policy. Updated the security policy for the 'SA' account.	Craig A. Benson
June 11, 2014	2.8	Updated database deployment workflow diagram (Figure 3). Updated migration policy. Updated documentation policy.	Craig A. Benson
June 16, 2014	2.9	Updated documentation policy. Updated server access policy.	Craig A. Benson
June 26, 2014	3.0	Updated Definitions, Abbreviations and Acronyms section to reference new Data Services Glossary.	Craig A. Benson
September 29, 2014	3.1	Updated Database Backup Policy.	Craig A. Benson
November 20, 2014	3.2	Updated Policies per annual DBA team review.	Craig A. Benson
January 29, 2015	3.3	Updated Data Retention / Archiving Requirements Policy	Craig A. Benson
March 9, 2015	3.4	Updated documentation policy.	Craig A. Benson
April 27, 2015	3.5	Updated documentation policy—added new database / data warehouse request.	Craig A. Benson
October 9, 2015	3.6	Updated documentation policy.	Craig A. Benson
November 5, 2015	3.7	Updated supported SQL tools policy.	Craig A. Benson
December 14, 2015	3.8	Updated documentation policy.	Craig A. Benson
April 18, 2016	3.9	Updated documentation policy.	Craig A. Benson
September 13, 2016	4.0	Updated documentation policy, updated deployment policy.	Craig A. Benson
November 4, 2016	4.1	Updated policies per annual ADSGC review findings.	Craig A. Benson
December 30, 2016	4.2	Updated documentation policy—added section on Template Usage. Updated SQL templates policy—added section on Template Usage.	Craig A. Benson
January 4, 2017	4.3	Updated documentation and SQL templates policies—refined grandfather clause to include updated documents / database objects.	Craig A. Benson
February 17, 2017	4.4	Added new database audit policy.	Craig A. Benson
September 28, 2017	4.5	Updated database lifecycle diagram. Updated the documentation policy. Added new BI policy.	Craig A. Benson

Table of Contents

Table of Figures

1 Brief Description

This document details the policies for developing, testing, maintaining and supporting AHS SQL Servers and SQL databases. The policies outlined herein were derived from enterprise-scale industry best practices and they form the basis upon which AHS SQL Server standards and procedures were created.

Questions pertaining to AHS SQL Server Environment Policies must be directed to the AHS Director of Data Services.

2 Scope

This document was written for database administrators (DBAs), database and application developers, server administrators (SAs), network administrators (NAs) and IT managers. The policies contained herein are specific to SQL Server; it contains the boundaries in which SQL Servers and SQL databases are to be implemented in the AHS domain. These policies extend beyond that of AHS-developed SQL Server solutions—it is highly recommended that all purchased, contracted or otherwise acquired SQL Server-based applications also conform to these policies as to maintain a consistent, stable SQL Server environment.

3 Policy Enforcement

Policy exceptions will be clearly stated within each applicable section; otherwise all policies will be enforced on a no exception basis. Clearance for any policy exception must be granted in writing by the AHS Data Services Governance Committee (ADSGC).

All designated AHS DBAs are responsible for upholding and enforcing the policies contained herein. Violations of any policy must be documented using the AHS Data Services Policy Exception Form (PEF) and submitted to the AHS Director of Data Services. Execution plans must be written, coordinated and implemented in a timely manner to correct all policy violations that are not approved by the ADSGC as policy exceptions.

4 References

- AHS Data Services Glossary
- AHS Data Services Web Portal
- AHS Data Services Data Dictionary Template
- AHS Data Services Report Specification Template
- AHS Data Services Update Form
- AHS Data Services Policy Exception Form
- AHS Data Services Employee Data Access Request Form
- AHS Data Services Vendor / Contractor Data Access Request Form
- AHS SQL Server Environment Standards
- AHS SQL Server Environment Procedures
- AHS SQL Server Environment Database Deployment Plan Template
- AHS SQL Server Environment Database Architecture Document Template
- AHS SQL Server Environment Database Administrator (DBA) Separation of Duties (SOD) Matrix
- AHS Information Technology and Electronic Communications Policies

5 Definitions, Abbreviations and Acronyms

Please reference the AHS Data Services Glossary.

6 Documentation Techniques

The following conventions are used throughout this document:

This convention	**Indicates**
CAPITAL LETTERS	Keys on the keyboard
KEY + KEY	Key combinations for which you must press and hold down one key and then press another key
[ ]	Information pertaining to a particular instance. Replace the brackets and the text between them with the respective instance of information, e.g. [ServerName] would be replaced with AHSSQLD01P if the applicable server pertained to AHSSQLD01P.
|	The pipe character indicates a logical ‘OR’ whereby the user must select one or another value
Highlighted Text	A button on an interface that requires a mouse click

7 Policies

7.1 *Standards Observence Policy*

In the interest of maintaining SQL Servers and SQL databases in a consistent, best-practices manner, the standards outlined in the AHS SQL Server Environment Standards document are to be observed.

Exceptions to this policy will be granted and documented on a case-by-case basis depending on extenuating circumstances, e.g. vendor databases, legacy systems.

7.2 *Procedures Observance Policy*

In effort to expedite AHS DBA and Data Services' requests, the procedures outlined in the AHS SQL Server Environment Procedures document are to be observed.

Exceptions to this policy will be granted and documented on a case-by-case basis depending on extenuating circumstances, e.g. emergencies, unknown factors.

7.3 *SQL Server Configuration Policy*

All SQL Server instances must be configured using the Global Administration Framework through the procedures outlined in the AHS SQL Server Environment Procedures document. This is necessary as to enable DBAs to maintain all Agency SQL Servers in a predictable, consistant and best-practices manner.

Exceptions to this policy will be granted and documented on a case-by-case basis depending on extenuating circumstances, e.g. legacy servers, end-of-life expectancy.

7.4 *SQL Server Provisioning Policy*

In effort to maximize the purpose, performance and behavior of SQL Servers, the following must be observed:

7.4.1 New SQL Server Requests

Requests for new SQL Servers must be submitted to and approved by the ADSGC.

7.4.2 SQL Server Consolidation

Every attempt will be made by AHS Data Services to consolidate SQL Server resources wherever possible. This entails the relocation of databases and/or routines in effort to minimize the number of SQL Servers on the AHS network.

7.4.3 SQL Server Purpose

7.4.3.1 SQL Engines

Every attempt will be made by AHS Data Services to position instances of SQL Servers to leverage the four SQL engines: Database Services, Integration Services, Analysis Services and Reporting Services. Ideally, each SQL engine type would be installed on a separate Windows server, thereby throttling-up system resources and enhancing scalability. Under no circumstances should all four SQL engines reside on one Windows server.

7.4.3.2 OLTP / OLAP Separation

OLTP databases (transactional databases) must not reside on the same server as OLAP databases (data warehouses, data marts) in effort to not impede daily business operations caused by potential errant queries and long-running ETL routines.

7.4.4 SQL Server Default and Named Instances

SQL Servers must be created using the default instance option, thereby inheriting the name of the Windows server on which it resides. Creating more than one instance (using the named instance option) of SQL Server on a Windows server instance must be avoided.

Exceptions to this policy will be granted and documented on a case-by-case basis depending on extenuating circumstances, e.g. temporary or limited use servers, legacy servers.

7.4.5 SQL Server Upgrades

Every attempt will be made by AHS Data Services to upgrade existing SQL Servers to the latest release of SQL Server providing Mirosoft released, at the very least, its first respective product service pack (SP1).

AHS-developed databases are prime, initial candidates for migration to upgraded SQL Servers because of AHS's in-house knowledge and development lifecycle. In effort to migrate vendor databases, each vendor must be contacted to determine if their database / application is compliant with the new release of SQL Server.

As with all database migrations to new SQL Servers, Database Migration Plans (DBMPs) must be drafted to detail the steps necessary to ensure all applications, reports, import and export routines are re-pointed to the new server.

NOTE: If the re-pointing effort is significant enough to delay a migration and if the old SQL Server would potentially be retired, request that the new SQL Server employ an alias name of the old SQL Server name—no re-pointing would then be required. This is *extremely* rare and would require a policy exception.

7.4.6 Separate Isolated Parallel Environments

For all database applications, a minimum of three separate, isolated, parallel SQL Server environments must exist: Development, Test and Production. Reference the Deployment Policy for the workflow that must transpire between these environments.

Additionally, separate, isolated, parallel application, web, FTP and file servers and/or file structures must be used to completely isolate environments. Routines can then be effectively executed end-to-end in each environment (Development, Test and Production) without environment overlap or issue.

7.4.7 SQL Server and Database Optimization

Every attempt will be made by AHS DBAs to pinpoint bottlenecks in SQL Server and database performance and recommend optimization techniques to respective Agency IT development groups and/or vendors as necessary. Database Deployment Plans must be written and executed in a timely manner to address all performance issues found.

Any SQL Server or database routine not yet placed in production with which a DBA has found performance issues will not be deployed to production until the issues are addressed.

7.4.8 Non-SQL Server Objects / CLR Enablement

No applications, CLR assemblies, executables or file storage structures other than that of SQL Server itself are to be installed on AHS SQL Servers. The CLR must not be enabled on AHS SQL Servers.

Exceptions to this policy will be granted and documented on a case-by-case basis depending on extenuating circumstances. Approvals must be obtained in writing from the ADSGC. Any approved applications, CLR assemblies, executables and/or file sturctures must first be installed by the DBA on a designated AHS development and/or test server as to ascertain its stability and affect on SQL Server. QA / UA testing and ADSGC approval will be necessary before installing anything on an AHS production SQL Server. Any application, CLR assembly, executable and/or file structure that negatively impacts the SQL Server that hosts it will not be placed into production.

7.4.9 “Sand-Box” Activity

All objects on SQL Servers must fulfill an AHS business purpose. The “Northwind”, “Pubs” and “AdventureWorks” Microsoft-shipped sample databases must not be installed on AHS SQL Servers. Personal databases and/or any personal objects that do not fulfill AHS business must not be installed on AHS SQL Servers.

Exceptions to this policy will be granted when the above-mentioned Microsoft-shipped sample databases, and any other “sand-box” database and object, will be installed on any system developer’s local instance of SQL Server.

7.4.10 Supported SQL Tools

Currently, AHS Data Services supports use of the following software tools for SQL Server and database development, maintenance and reporting. See the SQL Desktop Tools Policy that illustrates which employee roles are allowed use of these tools on their desktop.

7.4.10.1 Development Tools

- SSMS
- VS / BIDS / Data Tools
- XML Spy
- Atlassian
- Access
- Excel
- Word

7.4.10.2 Maintenance Tools

- SSMS
- RedGate
- AHS Global Administration
- Atlassian

7.4.10.3 Reporting Tools

- SSRS

7.5 Security Policy

All access to SQL Servers will be granted to individuals and systems on a least-privileged basis. Assessment of user and system access must be continuously scrutinized and audited by DBAs so that overstated, potentially harmful permissions are not granted.

7.5.1 ‘SA’ Account

Passwords for all SQL Server SA accounts are to be maintained by the designated DBAs for the respective servers. Passwords are to be extremely complex in nature (minimum 8 random characters with at least one uppercase letter, at least one lowercase letter, at least one number and at least one special character). Each SA password must be maintained on the AHS Secret Server.

Password changes must be updated on the AHS Secret Server during the same business day of the change.

Under no circumstances are SA accounts to be used as the credential under which databases / applications function. Alternative credentials that employ the ***principle of lowest permission*** must be used to accomplish the given function instead.

SA accounts are to be ***disabled*** on all AHS SQL Servers.

If an SA password is required and the respective DBA is not available, contact the AHS Director of Data Services.

7.5.2 SQL Server Windows Service Accounts

Passwords for all SQL Server service accounts (database service, agent service, integration service, analysis service and reporting service) are to be maintained by the designated DBAs for the respective servers. Passwords are to be extremely complex in nature (minimum 8 random characters with at least one uppercase letter, at least one lowercase letter, at least one number and at least one special character). Each service password must be maintained on the AHS Secret Server.

Password changes must be updated on the AHS Secret Server during the same business day of the change.

If a service account password is required and the respective DBA is not available, contact the respective IT manager or the AHS Director of Data Services.

7.5.3 Login Accounts (Authentication)

7.5.3.1 Windows Logins

Windows authentication is the primary and preferred means of allowing access to SQL Server, as it is the most secure. No individual Windows usernames are to be used as logins; rather Windows security groups must be used.

To create a new Windows security group, send an email to the Help Desk with the recommended name of the group (following AHS naming standards) and a list of initial users who will reside in the group.

7.5.3.2 SQL Logins

SQL authentication is the secondary means of allowing access to SQL Server. SQL login names must specify the name of the database for which it will access, e.g. a database named CAVU could have a SQL login named CAVU_User or CAVU_Admin.

Passwords for all SQL logins are to be maintained by the designated DBAs for the respective servers. Passwords are to be extremely complex in nature (minimum 8 random characters with at least one uppercase letter, at least one lowercase letter, at least one number and at least one special character). Each SQL login password must be maintained on the AHS Secret Server.

Password changes must be updated on the AHS Secret Server during the same business day of the change.

If a SQL login password is required and the respective DBA is not available, contact the respective IT manager or the AHS Director of Data Services.

7.5.4 Server-Level Roles

Only designated DBAs are to be assigned server roles. Only select DBAs are to be assigned the *sysadmin* server role (using security groups).

7.5.5 Database-Level Roles

Allowing access to database resources for AHS-developed software applications must be granted using either application roles or database roles. It is recommended that vendor-developed software applications employ them as well.

The following diagram illustrates the proper means of establishing database access using logins and database-level roles.

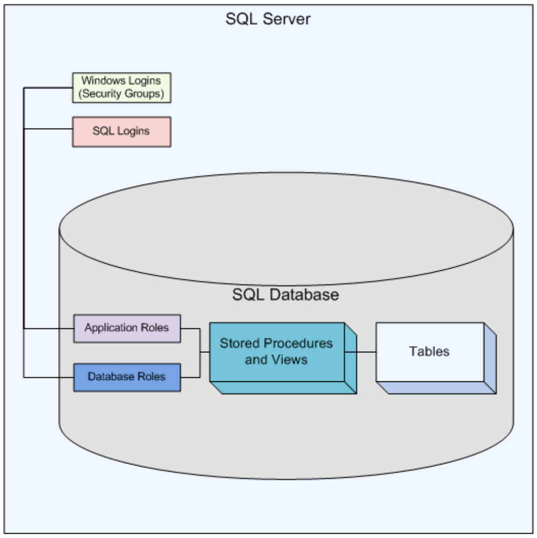


Figure 1 - Login / Database-Level Role Access

7.5.5.1 Application Roles

Application roles are the primary and preferred means to establish user access to database resources, e.g. to execute stored procedures. Application roles are most secure because they employ passwords that can be encrypted. It is highly recommended that AHS-developed software applications employ the use of application roles (at least one application role per software application).

Passwords for all application roles are to be maintained by the designated DBAs for the respective servers. Passwords are to be extremely complex in nature (minimum 8 random characters with at least one uppercase letter, at least one lowercase letter, at least one number and at least one special character). Each application role password must be maintained on the AHS Secret Server.

Password changes must be updated on the AHS Secret Server during the same business day of the change.

If an application role password is required and the respective DBA is not available, contact the respective IT manager or the AHS Director of Data Services.

7.5.5.2 Database Roles

Database roles are the secondary means to establish user access to database resources, e.g. to execute stored procedures. They are less secure than application roles in that passwords are not required. There are 10 Microsoft-shipped database roles that may be assigned, but it is highly recommended that user-defined database roles be implemented instead.

7.5.6 Named Database Schemas

Named database schemas should be used at every opportunity when significant separation of security and / or function is / are necessary. For example, a “diagnostic” schema could be created in which DBA-centric stored procedures could be created for obtaining data or database diagnostics. Named schemas are especially useful in data warehouse solutions.

7.5.7 Server / Database Access

Access to AHS SQL Servers and the databases that reside on them is granted based on the following guidelines:

1. Only designated DBAs will be granted the sysadmin server role.
2. Each SQL Server will have one primary DBA, one secondary (backup) DBA and one tertiary (backup) DBA assigned. The primary DBA is the first line of defence; s/he is the responsible entity for maintaining the respective server(s) per AHS policies, standards and procedures. The secondary and tertiary DBAs are the second line of defence *only in the event the primary and secondary DBAs are unavailable respectively*.
3. Server roles will not be assigned to any non-DBA regardless of the environment.
4. Non-DBA database access (using roles) will be granted based on the following matrix:

Environment	Users	Conditions / Comments
Development	Systems developers and systems analysts (only)	Non-developer / analyst personnel are not allowed access to development servers. AHS developers (through security groups) may be granted the **db_owner** database role or any lesser privileged role. AHS analysts (through security groups) may be granted permissions to execute stored procedures (through database roles) to be able to run given software. Vendor developers (through the VDARF process and security groups) may be granted the **db_owner** database role or any lesser privileged role. Vendor analysts (through the VDARF process and security groups) may be granted permissions to execute stored procedures (through database roles) to be able to run given software.
Test (Q/A, U/A, Staging)	Systems developers, systems analysts, designated Q/A and U/A testers (only)	AHS developers, analysts and testers (through security groups) may be granted permissions to execute stored procedures (through database roles) to be able to run given software thereby emulating production-like behavior. Vendor developers, analysts and testers (through the VDARF process and security groups) may be granted permissions to execute stored procedures (through

Environment	Users	Conditions / Comments
		database roles) to be able to run given software. ***AHS development team leaders are responsible for coordinating deployments to the test environment with the respective DBA using the DDP process.***
Production	Software users (only)	AHS users (through the EDARF process and security groups) may be granted permissions to execute stored procedures (through database roles) to be able to run given software. Vendors are not allowed access to production servers. ***AHS development team leaders are responsible for coordinating deployments to the production environment with the respective DBA using the DDP process.***

7.5.8 Database Table Access

Access must not be granted directly to database tables.

For AHS-developed OLTP applications, only stored procedures are to be used for data access and manipulation; no application is to be developed by embedding DML (or DDL) SQL code within it. Access to stored procedures is enabled by granting EXECUTE permission to applicable database and/or application roles, and then granting applicable logins access to the roles.

For AHS-developed OLAP applications, stored procedures and views may be used for data access. Applications may employ embedded SQL SELECT statements to views, but it is highly recommended that a DBA review the code prior to deploying the application in a production environment. Access to views is enabled by granting SELECT permission to applicable database roles, and then granting applicable logins access to the roles. Nevertheless, the *recommended* data access approach is through stored procedures.

The only exception to this policy is when access to tables is handled through stored procedures that contain dynamic SQL (*very rare*). In this instance, the applicable application and/or database roles are granted the necessary SELECT, INSERT, UPDATE or DELETE permission to the specific table(s) in addition to EXECUTE permission on the calling stored procedure(s).

7.5.9 Password Storage in Database Tables

Passwords must not be stored as plain text within database tables. If passwords are to be stored in tables, they must be stored as encrypted values. Encryption / decryption algorithms may be installed on SQL Servers, but the encryption / decryption algorithm keys must not be stored on SQL Servers.

7.5.10 DTS / SSIS Package Passwords

If DTS or SSIS packages are developed that will be executed outside of SQL Server and they employ password protection, the passwords are to be maintained by the designated DBAs for the respective packages. Passwords are to be extremely complex in nature (minimum 8 random characters with at least one uppercase letter, at least one lowercase letter, at least one number and at least one special character). Each DTS / SSIS package password must be maintained on the AHS Secret Server.

Password changes must be updated on the AHS Secret Server during the same business day of the change.

If a DTS / SSIS package password is required and the respective DBA is not available, contact the respective IT manager or the AHS Director of Data Services.

7.5.11 Personally Identifiable Information (PII) Protection

The following must be observed in effort to protect PII:

1. All PII data must be encrypted, to include data at rest and data in motion, particularly when the State is not in physical control of the data.
2. Additional program data, as determined by the data owner, may also be encrypted.
3. Data encryption methods may encompass cell-level, table-level, database-level, or file-level encryption if objectives 1 and 2 above are met. Additionally, all applications, APIs and services must be able to consume the data successfully using the selected method(s) of encryption.
4. Encryption must use cryptographic key hierarchy conventions or its equivalent.
5. For encryption level, no encryption and simple encryption are unacceptable. 3DES encryption is acceptable if data always resides within the State network. AES encryption with keys of at least 128 bit blocks is preferred.

7.6 Data Access Policy

The Agency's "Information Technology and Electronic Communications Policies" are the basis upon which access to AHS data systems are granted.

7.6.1 Requests for Transmission of Data and/or Database Schema

When data and/or database schema are to be transmitted to entities outside of the AHS and GOVNET firewalls, to include partial table samples up through full database backup files, the following must be observed:

- A current contract, data sharing agreement or MOU must exist between the State and the entity to which data and/or schema will be transmitted
- Permission to transmit relevant data to respective entities must be obtained in writing from the data owners. Permission to transmit relevant schema to respective entities must be obtained in writing from the AHS Director of Data Services.
- Vendor database schema must never be transmitted to competing vendors. This practice is unethical and may perpetuate legal recourse against AHS.
- The data and/or schema must be compressed in a zip file. Encryption and password protection must then be applied.
- The data may then be transmitted using the following methods (in descending order of preference):
    - SFTP
    - PHIN MS
    - Secure Email (file size dependant)
    - FTP
- The zip file password information must be conveyed to the entity using secure email. Reference the secure email procedure within the AHS SQL Server Environment Procedures for details.

7.6.2 Employee Access

All employee access to and/or removal of access from AHS data systems must be documented using the Data Services Employee Data Access Request Form (EDARF).

7.6.3 Vendor / Contractor Access

All vendor / contractor access to and/or removal of access from AHS data systems must be documented using the Data Services Vendor / Contractor Data Access Request Form (VDARF).

Vendor / contractor access will not be considered unless a current and valid contract, data sharing agreement or MOU with the SOV AHS is on file. Any access that may be granted will be limited in duration and in scope (as may be stated in the contract) and be audited by an AHS DBA.

Access may only be granted to vendors / contractors when…

The vendor / contractor will maintain a workstation on site (inside the AHS firewall) and an AHS Windows domain account is issued,

(or)

the vendor / contractor will not maintain a workstation on site, but will access the AHS domain with an AHS Windows domain account through the Citrix gateway using an RSA token,

(or)

the vendor / contractor will neither maintain a workstation on site nor access the AHS domain with an AHS Windows domain account through the Citrix gateway using an RSA token, rather specific AHS database servers will be accessed through an established VPN,

(or)

the vendor / contractor will access specific AHS database servers through online meeting software on an AHS employee's PC, e.g. web-ex, go-to-meeting, etc.

Terms of access:

- A valid, signed vendor contract, data sharing agreement or MOU is on file with the respective business office. A copy of this document must be forwarded to the AHS Director of Data Services.
- A signed, approved Vendor / Contractor Data Access Request Form (VDARF) is on file with the ADSGC
- The expiration date on the applicable vendor / contractor Windows account must be the expiration date on the SOV AHS contract, data sharing agreement or MOU, or 90 days from the account creation (or in 90-day increments), whichever date is earliest.
- All other AHS SQL Server environment policies, standards and procedures apply.

Exceptions to this policy will be granted on a case-by-case basis depending on extenuating circumstances, e.g. contract renewal periods, transition to state employment.

7.7 Database Cataloging Policy

In effort to maintain a working inventory of the SQL databases that are hosted on AHS SQL Servers and the departments, applications, reports, import processes and export processes that utilize them, it is essential that databases be cataloged using the process as outlined in the AHS SQL Server Environment Procedures document.

7.8 Database Backup Policy

Data is the Agency's most valuable asset and it is pertinent to its mission that it is regularly backed up.

The backup process established on each AHS SQL Server is by means of database maintenance plans and/or SQL jobs. Except for test and production data warehouses, all databases are to be backed up at least once per weekday. Test and production data warehouses need not be backed up, rather snapshot backups are to be captured and archived after any schema change. Database size will dictate whether full or differential backups are taken during the week. If differential backups are employed, at least one full backup per week must be captured.

Backup files and maintenance logs are to be placed in their respective subdirectories in the following share. This area is officially known as the "AHS SQL Database Backup Pool."

\\ahs\ahssoft\Backup\SQL

The folders in the backup pool must adhere to the following structure:

1. [SERVERNAME] *(uppercase)*
   a. Backups
      i. [DatabaseName]
         1. [BackupFileName].bak (*full backups*)
         2. [BackupFileName].dif (*differential backups*)
         3. [BackupFileName].trn (*transaction log backups*)
      ii. [DatabaseName]
      iii. [DatabaseName]
      iv. [DatabaseName]
   b. MaintenanceLogs

DII Server Administrators are responsible for backing up the SQL backup files in the above referenced shares to its backup data-mover.

Exceptions to this policy will be granted and documented on a case-by-case basis depending on extenuating circumstances, e.g. poorly designed data warehouses and ETL processes, capacity constraints, etc.

7.8.1 Development and Test Servers

The recovery model is to be 'Simple' for all system and user databases on AHS development and test servers. Transaction logs are not to be backed up, and the log file on each user database must be truncated at least once per day. The development and test backup file retention period within the designated backup shares must not exceed one week.

7.8.2 Production Servers

The recovery model is to be “Simple” for all system databases, data warehouses and static (read-only) databases on AHS production servers and the recovery model is to be “Full” for all transactional-based (ODS) user databases. Transaction logs are to be backed up no more than hourly for all databases with the “Full” recovery model (for at least eight consecutive hours) between the hours of 6:00 AM and 6:00 PM. The log files for all Simple recovery model user databases must be truncated at least once per day. The production backup file retention period within the designated backup shares must not exceed five weeks (with a minimum of eight days).

7.8.3 Database Backup Validation

In an ongoing effort to minimize the impact of data loss, database backup validation excersises must be randomly conducted by DBAs.

DBAs will restore selected production database(s) to development server(s) as to ensure backup files are valid and restore successfully. DII Server Administrators may or may not be involved, depending on the date of the file(s) needed to restore the given database(s). Several queries must then be executed for which known results can be produced. Once the restoration and validation are completed, the respective database(s) can be dropped from the development server(s).

Real-life actual database restorations will be handled by designated DBAs. In the event the respective DBA is not available, contact the AHS Director of Data Services.

7.8.4 Database Backup Archive

Backups are archived whenever a major schema update is made to a development, test or production database; whenever a database snapshot must be retained for legal or historical purposes; or whenever a DBA deems it necessary. Backups that require archiving are to be compressed and stored in the following share. This area is officially known as the “AHS SQL Database Backup Archive.”

\\ahs\ahssoft\Backup\SQL_Archives

The folders in the archive must adhere to the following structure:

1. [SERVERNAME | PRODUCTNAME] *(uppercase)*
    a. [DatabaseName | SERVERNAME *(uppercase)*]
        i. [BackupFileName]_[MetadataAboutBackup].zip

7.9 Database Design Policy

7.9.1 Requirements Analysis

The database design phase must not begin until all requirements (to include data security, capacity, retention and archiving requirements) are gathered, well documented and approved by the applicable stakeholders, DBAs and IT team leads.

In addition to the specific business data requirements, the following requirements must be gathered before a SQL database solution can be appropriately designed.

7.9.1.1 Security Requirements

Database security is best implemented when application functionality is partitioned using role-based methods. Role based functionality most often translates easily to the implementation of database-level roles (see the Database-Level Roles section in the Security policy for details).

The following list details the checkpoints on which security requirements must be gathered.

- ➢ What are the roles involved as they correlate to data elements, e.g. an “Administrator” role can insert, select, update and delete all data in the database; a “Program Manager” role can insert, select, update and delete only data relevant to their program; and a “Case Viewer” role can only select specific data, etc.?
- ➢ What data elements apply to each of the roles?
- ➢ Who are the users that fulfill the roles?

7.9.1.2 Capacity Requirements

Having knowledge of how much data will be inserted, selected, updated and deleted in SQL databases and how many users and systems will interact with the data enables database developers and DBAs to better implement scalable, reliable solutions.

The following list details the checkpoints on which capacity requirements must be gathered.

- ➢ Anticipated number of users and systems who will insert data
- ➢ Anticipated number of users and systems who will select data
- ➢ Anticipated number of users and systems who will update data
- ➢ Anticipated number of users and systems who will delete data
- ➢ Anticipated record size (in kilobytes, based on relevant data elements)

- Anticipated number of records inserted annually
- Anticipated number of records selected annually
- Anticipated number of records updated annually
- Anticipated number of records deleted annually

7.9.1.3 Data Retention / Archiving Requirements

The data in databases and archives must be retained for durations no longer than Federal and/or State statute or program statistical needs require.

There are three categories under which data retention and archiving must be considered: live operational data, live archived data and media archived data.

The following table details the checkpoints on which data retention and archiving requirements must be gathered.

Live Operational Data	**Live Archived Data**	**Media Archived Data**
How long do data need to be kept in the operational database? Data are kept live in operational SQL Server databases per true business needs. It is imperative that accurate retention requirements be discovered during the requirements gathering phase of a project. Statutes and statistical needs concerning applicable data will govern when operational data will be deleted from operational databases and archived to separate, non-operational databases (if necessary). E.g.: Data age < 5 years	How long do data need to be kept in the archive database, if at all? Data are kept live in archive SQL Server databases per the true statistical needs of data owners. Data will be burned to removable media and then deleted from archive databases when it ages beyond statistical needs (if necessary). E.g.: Data age between 5 and 10 years	How long do data need to be kept on removable media, if at all? Data are kept on removable media solely for archival / research purposes. Copies of the media may be distributed to the data owner and statisticians (if necessary). E.g.: Data age > 10 years

Figure 2 - Table of Data Retention / Archive Checkpoints

7.9.2 General Database / Warehouse Design

It is the developer's responsibility that all questions that s/he may have pertaining to the design of database / warehouse objects to fulfill a given use case or task be answered during the design phase. The DAD produced at the end of the design phase is to be a thorough and accurate representation of the physical database / warehouse objects developed. This includes documentation of all parameters, steps, sub-steps and error handling within stored procedures and UDFs; documentation of SSIS packages and jobs; and complete data definitions for all table and view columns including all relevant allowed SRT codes from corresponding SRT codesets.

All database / warehouse design documents are to be created and maintained using the approved AHS DAD template or using RedGate SQL Doc through the procedure outlined in the AHS SQL Server Environment Procedures document. All design documentation must be presented to the respective DBA for review and approval.

Unit testing and DBA code reviews are to be done for each new coding task, enhancement and defect assigned.

7.9.3 Database Normalization

All database tables must meet, at the very least, the third normal form (3NF), as to ensure RDBMS best practices.

Exceptions to this policy will be granted and documented on a case-by-case basis depending on extenuating circumstances, e.g. legacy, staging, intermediary or temporary tables, etc.

7.9.4 Warehouse Denormalization

All warehouse tables must conform to a star (preferable) or snowflake schema design. Data may be intentionally denormalized through a fact / dimension schema paradigm.

Exceptions to this policy will be granted and documented on a case-by-case basis depending on extenuating circumstances, e.g. legacy, staging, intermediary or temporary tables, etc.

7.9.5 Referential Integrity

In OLTP databases, references between tables shold be constrained using physical primary / foreign key relationships.

Exceptions to this policy will be granted and documented on a case-by-case basis depending on extenuating circumstances, e.g. legacy, staging, intermediary or temporary tables, etc.

7.9.6 Primary Keys / Clustered Indexes

All database tables must employ either a primary key or a clustered unique index. Always opt for primary keys intitially.

7.9.7 Index Review

DBAs must regularly analyze database tables for index usage. Duplicate and unused indexes must be dropped; missing indexes must be created; and fragmented indexes must be defraged or rebuilt. Indexing is an on-going database tuning effort. As databases grow and query needs change, so must indexes.

7.9.8 Warehouse ETL Processing

ETL processes may be designed for full loads (complete refreshes) and/or incremental loads (partial refreshes).

If full ETLs are the only means by which a warehouse is refreshed…

1. The ETL must execute in under 1 hour
2. The ETL must be executed no more than once per day

If incremental ETLs are the only means by which a warehouse is refreshed…

1. The ETL must execute in under 1 hour
2. The ETL must be executed no more than once per day

If both full and incremental ETLs are employed…

1. The full ETL must execute in under 1 hour
2. The full ETL must be executed no more than once per week
3. The incremental ETL must execute in under 30 minutes
4. The incremental ETL must be executed no more than once per day

Exceptions to this policy will be granted and documented on a case-by-case basis depending on extenuating circumstances, e.g. legacy ETL processes, VLDB scenarios.

7.9.9 Vendor Database Design

If vendor database functionality is to be extended using AHS-developed objects and routines, under no circumstances are those objects and routines to be deployed in vendor databases (to not invalidate licensing agreements). Instead, database developers must deploy new objects and routines in the **dbVendorExtend** database on the respective target server. If the dbVendorExtend database is not yet deployed to the respective server, contact the AHS Director of Data Services.

Exceptions to this policy will be granted and documented on a case-by-case basis depending on extenuating circumstances, e.g. whether the respective source code is owned by AHS.

7.10 Coding Policy

7.10.1 Hard-Coding

Hard-coding is neither allowed for any AHS-developed application, nor for any vendor application that will be placed on an AHS SQL Server. The VT_SOFTCODE SRT codeset, Windows registry, INI files, CONFIG files, XML files, environment variables, dynamic variables and/or dynamic parameters are some of the methods used to avoid hard-coding. All SQL code is to be written using the SQL coding standards as detailed in the AHS SQL Server Environment Standards document using approved AHS SQL templates.

7.10.2 AHS SQL Templates

All SQL code written for tables, views, stored procedures, UDFs, SSIS package T-SQL steps, jobs T-SQL steps and stand-alone scripts must be created from the applicable approved AHS SQL templates. The templates must reside on each developer's machine in the appropriate SQL templates directory; they can be installed from the AHS Data Services Web Portal. The SQL Templates directory is as follows:

SQL 2012 on Windows7: %AppData%\Microsoft\SQL Server Management Studio\11.0\Templates\Sql\AHS_Templates

7.10.2.1 Template Updates

AHS SQL templates are reviewed annually, at the very least, and they are updated in accordance with changes to our standards, policies and procedures.

When a database object is created or updated, it must employ the latest published template at the time of creation / update. Objects whose creation / update date and template usage precedes a respective template update date will be grandfathered.

7.10.3 AHS SSIS Package Template, Configuration and Deployment

All SSIS packages developed for AHS must be created using the approved AHS SSIS package template. All packages must employ use of a configuration file in accordance with the standards outlined in the AHS SQL Server Environment Standards document. The AHS SSIS package template resides on the AHS Data Services Web Portal and its configuration file must be installed on each developer's machine in the "C:\SSIS-Config" folder.

All developed SSIS packages must be reviewed by the respective DBA and the developer prior to being deployed to any server. For packages that are to be scheduled, developers are not through with their development task until a package is able to run unattended by the SQL job system on the development server.

7.10.4 SQL Source File Versioning

All original source files must be named using the naming standards outlined in the AHS SQL Server Environment Standards document. As deemed necessary by the DBA or the developer, a new file version is to be made using the version naming standards and the code header within the respective source file must reference the new version file name. The new file version must then to be placed under source control in the respective area.

Exceptions to this policy will be granted and documented on a case-by-case basis depending on extenuating circumstances e.g. depending on whether a source control solution is in place for the respective development group. In the event a source control solution does not exist, the following area must be use to maintain SQL source files:

Y:\AHS ALL SHARE\AHS IT DBA\SQL_ScriptLibrary

7.10.5 Unit Testing

All SQL code written to fulfill tasks, defects and enhancements must be thoroughly tested by the developer using AHS-approved test plans and test scripts prior to being made available for code review. Unit testing must include an assessment of the code's stability and error handling capabilities.

7.10.6 Code Review

All SQL code written to fulfill tasks, defects and enhancements is to be reviewed by the respective DBA. The code review is considered the last step for all development activities.

7.10.7 Function Testing

All SQL code written to fulfill tasks, defects and enhancements must be thoroughly tested by the database developer and application developer using AHS-approved test plans.

7.11 Database Update Policy

All updates to AHS databases, most notably those not developed in-house (COTS, GOTS, MOTS databases) must be done via Data Services-approved SQL scripts. Under no circumstances are database updates to be made using compiled executable code (exe's, dll's, vbs', etc).

7.12 Error Handling Policy

All SQL code written for stored procedures, SSIS packages, jobs, triggers, UDFs and stand-alone scripts must employ the error handling standards outlined in the AHS SQL Server Environment Standards document and they are to use the AHS-defined errors as listed in the APPENDIX. The approved AHS SQL templates contain examples of how errors are to be thrown.

7.13 SQL Update Communication Policy

Communication is essential when having to perform any DBA action on a SQL Server or SQL database. No matter how big or how small, all updates made to a SQL Server or SQL database must be communicated to all affected users as far in advance as possible. The approved AHS Data Services Notice Outlook form is the means through which communication must be made. The Outlook form, and its associated Word template, resides on the AHS Data Services Web Portal. It must be installed in your Microsoft templates folder on your hard drive.

7.14 Defect Resolution Policy

All database developers that are assigned defects for any AHS-developed application (that originate because of an error on the respective interface), will be required to work with an application developer to test their code by running the error-generating function within the interface. Refer to the Defect Resolution Procedure in the AHS SQL Server Environment Procedures document.

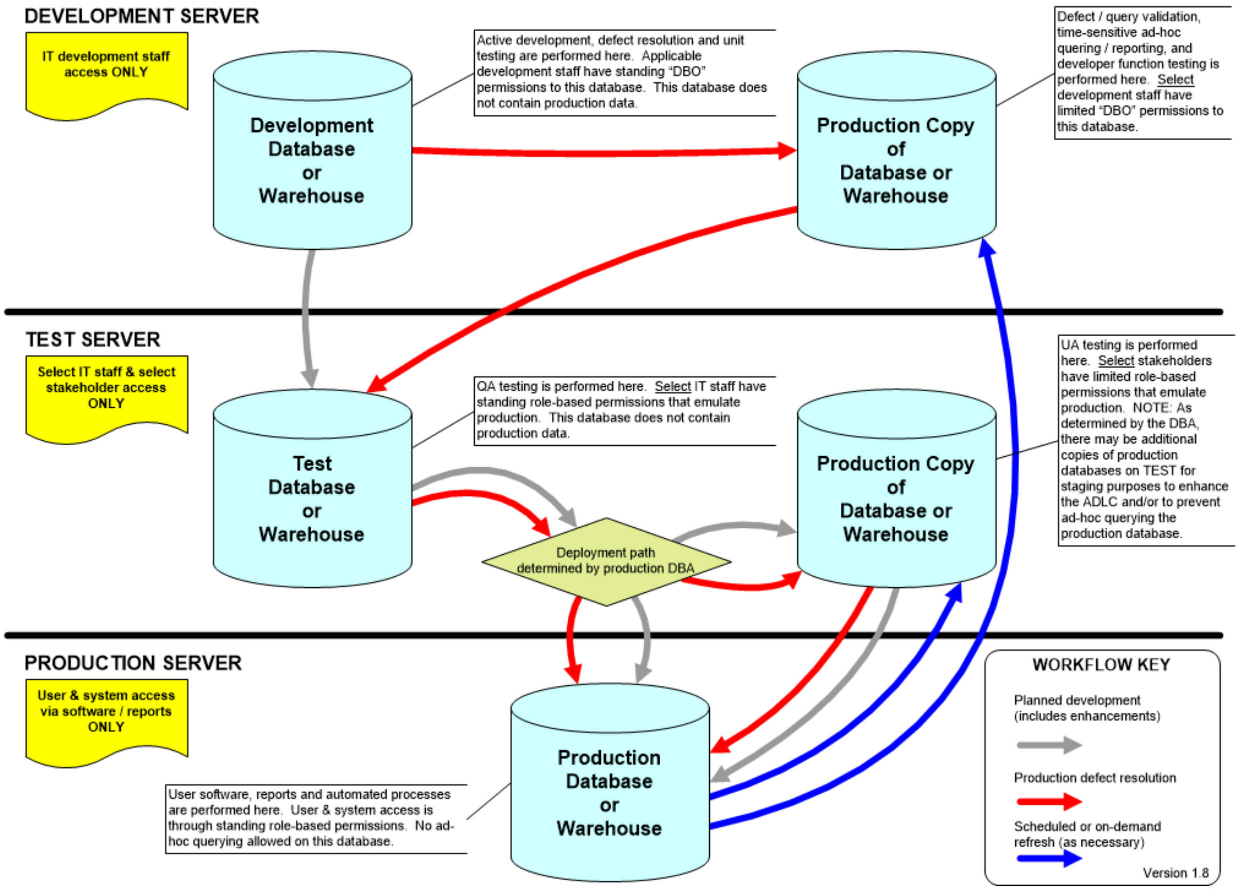
7.14.1 Large-Scale Data-Fix Defects

When having to update a lot of data and external reference data is necessary, developers should employ the dbETL database to create and deploy tables that may be used with ETL operations against a target database. Developers should work with AHS Data Services as necessary to ensure compliance and efficiency for such defects.

7.15 Deployment Policy: The AHS Database Lifecycle (ADLC)

All deployments between databases and/or between server environments (from development to test, from test to production) must be coordinated using the Global Administration Tool or the approved AHS Database Deployment Plan (DDP) template.

The following is the lifecycle AHS databases must undergo.


DEVELOPMENT SERVER
IT development staff access ONLY
Development Database or Warehouse
Production Copy of Database or Warehouse
TEST SERVER
Select IT staff & select stakeholder access ONLY
Test Database or Warehouse
Deployment path determined by production DBA
Production Copy of Database or Warehouse
PRODUCTION SERVER
User & system access via software / reports ONLY
Production Database or Warehouse
WORKFLOW KEY
Planned development (includes enhancements)
Production defect resolution
Scheduled or on-demand refresh (as necessary)
Version 1.8

Active development, defect resolution and unit testing are performed here. Applicable development staff have standing "DBO" permissions to this database. This database does not contain production data.

Defect / query validation, time-sensitive ad-hoc quering / reporting, and developer function testing is performed here. Select development staff have limited "DBO" permissions to this database.

QA testing is performed here. Select IT staff have standing role-based permissions that emulate production. This database does not contain production data.

UA testing is performed here. Select stakeholders have limited role-based permissions that emulate production. NOTE: As determined by the DBA, there may be additional copies of production databases on TEST for staging purposes to enhance the ADLC and/or to prevent ad-hoc querying the production database.

User software, reports and automated processes are performed here. User & system access is through standing role-based permissions. No ad-hoc querying allowed on this database.

Figure 3 – AHS Database Lifecycle (ADLC)

Exceptions to this policy will be granted and documented on a case-by-case basis depending on extenuating circumstances, e.g. environment and capacity constraints. Under no circumstances will compiled executables containing database scripts be accepted to deploy databases and their objects.

7.16 Migration Policy

In effort to employ current technology, and especially to prevent exposure to risk from unsupported, out-of-date technology, AHS Data Services will strive to migrate SQL databases to newer releases of SQL Server whenever possible. All database migrations between servers must be coordinated using the approved AHS Database Migration Plan template. The DBMP template may be used for either a database move or copy operation.

7.17 Ownership of Database Objects Policy

Under no circumstance must the ownership of any database object, to include the database itself, be a user's Windows account. This policy prevents crippled applications and processes must any user leave the AHS organization. Objects are to be owned per the following guidelines:

7.17.1 Databases

Databases are to be owned by a designated SQL login specifically created for the respective application. If one is not created for this purpose, the SA account is to be used.

7.17.2 Tables, Views, Stored Procedures, UDFs, Triggers, Indexes

These database objects are to be owned by 'dbo' unless named schemas are to be used per design/security considerations.

7.17.3 DTS / SSIS Packages

DTS / SSIS packages that are deployed to SQL Servers (as saved in the msdb) must be owned by the server's respective SQL Agent Windows service account (or a proxy account set up for this specific purpose).

7.17.4 SQL Server Jobs

SQL jobs must be owned by the server's respective SQL Agent Windows service account (or a proxy account set up for this specific purpose).

7.18 Documentation Policy

Documentation and the maintenance thereof are vital to the success of Data Services across the enterprise. All documentation pertaining to AHS SQL Servers is to be maintained using only the approved AHS SQL Server Environment templates and forms and it must adhere to AHS naming and versioning standards.

7.18.1 Document Templates

The following is a table of the approved templates and forms and the purpose they fulfill.

Name	File	Type	Description
Data Services Update (DSU)	http://confluence.ahs.state.vt.us/display/AHSDS/Data+Services+Update+Template	Outlook Template	Used to communicate all changes made to any SQL Server and/or SQL database. This Outlook template uses the Word template of the same name.
Data Services Update (DSU)	http://confluence.ahs.state.vt.us/display/AHSDS/Data+Services+Update+Template	Word Template	Used to communicate all changes made to any SQL Server and/or SQL database. This Word template is used by the Outlook template of the same name.
Data Dictionary (DD)	http://confluence.ahs.state.vt.us/display/AHSDS/Data+Dictionary+Template	Word Template	Used to document database elements for requirements analysis. Data dictionaries are supplemental design documents that, along with DADs, enable DBAs to design database and data warehouse solutions. The DD

Name	File	Type	Description
			is a necessary deliverable for any State contracted or acquired system.
Data Mapping Document (DMD)	http://confluence.ahs.state.vt.us/display/AHSDS/Data+Mapping+Document+Template	Excel Template	Used to map table columns from a source data store to a target data store. The DMD is a necessary supporting document to the Data Migration Plan (DMP), but the DMD can potentially exist on its own depending on the project.
Data Migration Plan (DMP)	http://confluence.ahs.state.vt.us/display/AHSDS/Data+Migration+Plan+Template	Word Template	Used to detail the necessary phases (and tasks therein) to successfully migrate data from one data store to another. A completed DMD is also required, as it is to be linked from within the DMP.
Report Specification (RS)	http://confluence.ahs.state.vt.us/display/AHSDS/Report+Specification+Template	Word Template	Used to document report requirements. Report specifications, along with data dictionaries and DADs, enable DBAs to design reports.
Database Architecture Document (DAD)	http://confluence.ahs.state.vt.us/display/AHSDS/SQL+Database+Architecture+Document+Template	Word Template	Used to document new and/or existing database objects, and/or routines necessary to fulfill use cases or tasks.
Database Deployment Plan (DDP)	http://confluence.ahs.state.vt.us/display/AHSDS/SQL+Database+Deployment+Plan+Template	Word Template	Used to document the database objects and routines that are to be placed onto a SQL Server, e.g. when moving objects from a test server to a production server. Not to be used to migrate an entire database.
Database Migration Plan (DBMP)	http://confluence.ahs.state.vt.us/display/AHSDS/SQL+Database+Migration+Plan+Template	Word Template	Used to document the endpoints of a given database that is to be migrated (moved or copied) from one SQL Server to another SQL Server.
Data Services Template (DST)	http://confluence.ahs.state.vt.us/display/AHSDS/Data+Services+Template	Word Template	Used to document all miscellaneous information not contained in approved AHS Data Services templates and forms.
Policy Exception Form (PEF)	http://confluence.ahs.state.vt.us/display/AHSDS/Policy+Exception+Form	Word Form	Used to document exceptions to AHS Data Services Policies.
Employee Data Access Request Form (EDARF)	http://confluence.ahs.state.vt.us/display/AHSDS/Employee+Data+Access+Request+Form	Word Form	Used to request access for employees to Agency data systems.
Vendor / Contractor Data Access Request Form (VDARF)	http://confluence.ahs.state.vt.us/pages/viewpage.action?pageId=13533311	Word Form	Used to request access for vendors / contractors to Agency data systems.
New Database / Data Warehouse Request	http://confluence.ahs.state.vt.us/pages/viewpage.action?pageId=3342	Word Template	Used to request a new database or data warehouse on an AHS SQL Server.

Name	File	Type	Description
	3457		
Server Deployment Request (SDP)	http://confluence.ahs.state.vt.us/display/AHSDS/SQL+Server+Deployment+Plan+Template	Word Template	Used to document the server objects and routines that are to be placed onto a SQL Server, e.g. when moving objects from a test server to a production server.
Power BI Deployment Plan (PBIDP)	http://confluence.ahs.state.vt.us/display/AHSDS/Power+BI+Deployment+Plan+Template	Word Template	Used to document the Power BI objects that are to be published to the test or production Microsoft cloud via the Power BI Service.

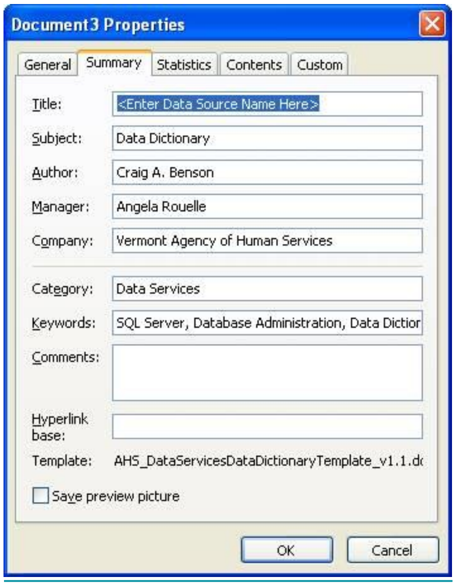
Figure 4 - Table of AHS Data Services Templates and Forms

The referenced templates and forms may be obtained through the AHS Data Services Web Portal.

It is highly recommended that these templates be installed in your Microsoft Templates directory on your C drive:

%AppData%\Microsoft\Templates

NOTE: All AHS Data Services templates contain fields. The fields are to be maintained through the document properties (accessed by clicking the document's "File / Info / Advanced Properties" section). Fields that require updates are on the "Summary" and "Custom" tabs. After saving the properties, highlight the entire document and press the F9 key to update all applicable fields.



Title: <Enter Data Source Name Here>

Subject: Data Dictionary

Author: Craig A. Benson

Manager: Angela Rouelle

Company: Vermont Agency of Human Services

Category: Data Services

Keywords: SQL Server, Database Administration, Data Dictior

Comments:

Hyperlink base:

Template: AHS_DataServicesDataDictionaryTemplate_v1.1.dc

□ Save preview picture

Figure 5 - Document Properties

7.18.1.1 Template Updates

AHS Data Services templates are reviewed annually, at the very least, and they are updated in accordance with changes to our standards, policies and procedures.

When an AHS Data Services document is created or updated, it must employ the latest published template at the time of creation / update. Documents whose creation / update date and template usage precedes a respective template update date will be grandfathered.

7.18.2 Document Repository

All draft (in-process) AHS SQL Server Environment documentation must be maintained as Word documents on the AHS Data Services document library.

Y:\AHS ALL SHARE\AHS IT DBA\DocumentationLibrary

All approved (final) AHS SQL Server Environment documentation must be maintained as PDF’s on the AHS Data Services Web Portal under the applicable documentation areas.

http://confluence.ahs.state.vt.us/display/AHSDS

7.18.3 Documentation Maintenance

As requirements change and evolve, it is crucial to maintain AHS SQL Server Environment documentation such that it reflects the enterprise precisely. It is ultimately the DBA’s responsibility to ensure that all SQL Server documentation is maintained with 100% accuracy. This means that previously approved and published documents require occasional updates to achieve accuracy.

DBAs must ensure that…

- DDs reflect current data elements
- DADs reflect current database objects and routines
- DDPs reflect current objects deployed to SQL Servers
- RSs reflect current reports
- PEFs reflect the current state of policy exceptions
- EDARFs reflect the current state of employee’s access
- VDARFs reflect the current state of vendor/contractor’s access

7.19 SQL Desktop Tools Policy

In effort to control cost and limit risk, the following table illustrates the approved list of SQL tools that may be installed / maintained on AHS user's desktops per the SQL-user role(s) they fulfill.

NOTE: SQL-user roles are determined by the Data Services Director.

Role	SQL Tool	Comments
DBA	1. SQL Server (local Express instance) 2. SQL Server Management Studio (SSMS) 3. SQL Server Integration Services (SSIS) 4. Business Intelligence Development Studio (BIDS) / SQL Data Tools 5. RedGate Toolbelt (with license requirement) 6. AHS SQL Global Administration (GA)	
Database Developer	1. SQL Server (local Express instance) 2. SQL Server Management Studio (SSMS) 3. SQL Server Integration Services (SSIS) 4. Business Intelligence Development Studio (BIDS) / SQL Data Tools 5. RedGate Toolbelt (with license requirement) 6. AHS SQL Global Administration (GA)	
Application Developer	1. SQL Server Management Studio (SSMS Express edition) * 2. AHS SQL Global Administration (GA)	* As deemed necessary
QA Tester (IT)	1. SQL Server Management Studio (SSMS Express edition) * 2. AHS SQL Global Administration (GA)	* As deemed necessary
Analyst / Statistician	1. SQL Server Management Studio (SSMS Express edition)	
User	(Nothing)*	* Pre-approved users may be allowed a local instance of SQL Server Express edition because of software procurement. Every effort must be made to defer this architecture, as it presents a formidable security risk.

7.20 SQL Server Patching Policy

All AHS SQL Servers are to be patched as follows:

Patch Type	Responsible	Comment
All OS patches (hot/CU/KB fixes and service packs)	DII Server Team (via WSUS)	Communicates timing to AHS Data Services
Hot/CU/KB fixes (SQL Server product)	AHS Data Services	Communicates timing to AHS Users
Service Packs (SQL Server product)	AHS Data Services	Communicates timing to AHS Users

All patching performed by AHS Data Services will done through the ADLC procedure (development, then test, then production) to mitigate risk.

7.21 Database Audit Policy

While developer-created audit controls are possible (using stored procedures), it does not prevent data from being viewed and / or edited by other means. Therefore, when database reads and writes are required to be tracked per State and / or Federal statute, a SQL Database Audit must be created by a DBA.

SQL Database Audits must adhere to the guidelines outlined in the Standards and Procedures documents.

SQL Database Audit results must be stored in the following areas under the specified conditions.

Audit results target directory (less-than-or-equal-to 1 year of age):

\\ahs\ahssoft\Backup\SQL_AUDIT

Audit results archive directory (greater than 1 year of age—must be zipped)

\\ahs\ahssoft\Backup\SQL_Archives_AUDIT

Processes must be developed to move and zip audit results from the target directory to the archive directory when the conditions are met.

Audit results must be purged from the archive directory when their statutory retention period has expired.

7.22 Business Intelligence (BI) Policy

7.22.1 Approved BI Tools

In effort to maintain standardization and curtail cost, only the following BI tools are endorsed by AHS:

- Excel
- Power BI Desktop
- Tableau
- Oracle BI

NOTE: Business Objects (BO) is being phased out. No new instances of BO are to be installed. Exceptions to BO installations may be granted based on extenuating circumstances.

7.22.2 BI Database Connectivity

Connectivity to live production databases is not allowed within BI tools. Instead, users must connect to production copy databases that reside in the AHS test environment for the purposes of developing BI reports and / or dashboards.

Only Data Services-vetted and published reports and dashboards may connect to live production databases.

Vermont Agency of Human Services

AHS SQL Server Environment

Procedures

Version 3.7

Revision History

Date	Version	Description	Author
January 19, 2005	1.0	Created document	Craig Benson
October 10, 2012	1.1	Updated for AHS	Craig Benson
March 14, 2013	1.2	Updated for Windows7 / Office 2010 compatibility, updated footer address, added Database Development Procedure, added Database Deployment Procedure	Craig A. Benson
July 17, 2013	1.3	Updated the GA SQL Server configuration procedure. Updated the database development procedure. Updated the database deployment procedure.	Craig A. Benson
September 24, 2013	1.4	Added database cataloging procedure.	Craig A. Benson
January 7, 2014	1.5	Updated database cataloging procedure.	Craig A. Benson
January 16, 2014	1.6	Updated database cataloging procedure. Added database migration procedure.	Craig A. Benson
February 18, 2014	1.7	Updated the GA SQL Server configuration procedure.	Craig A. Benson
March 12, 2014	1.8	Updated the GA SQL Server configuration procedure.	Craig A. Benson
April 10, 2014	1.9	Updated the GA SQL Server configuration procedure. Added new Secret Server SQL Password Management Procedure.	Craig A. Benson
May 29, 2014	2.0	Updated the GA SQL Server configuration procedure.	Craig A. Benson
June 23, 2014	2.1	Updated the GA SQL Server configuration procedure.	Craig A. Benson
June 26, 2014	2.2	Updated Definitions, Abbreviations and Acronyms section to reference new Data Services Glossary. Updated Database Development Procedure (added workflow diagrams).	Craig A. Benson
September 23, 2014	2.3	Updated GA SQL Server configuration procedure.	Craig A. Benson
September 29, 2014	2.4	Updated database cataloging procedure.	Craig A. Benson
November 6, 2014	2.5	Updated database cataloging procedure.	Craig A. Benson
November 24, 2014	2.6	Updated procedures per annual DBA team review.	Craig A. Benson
January 29, 2015	2.7	Updated GA SQL Server configuration procedure.	Craig A. Benson
July 17, 2015	2.8	Updated GA SQL Server configuration procedure.	Craig A. Benson
November 16, 2015	2.9	Updated GA SQL Server configuration procedure.	Craig A. Benson
March 4, 2016	3.0	Updated GA SQL Server configuration procedure.	Craig A. Benson
April 19, 2016	3.1	Added new add data disk procedure. Updated the database cataloging procedure. Updated the database deployment procedure.	Craig A. Benson

Date	Version	Description	Author
May 24, 2016	3.2	Updated add data disk procedure.	Craig A. Benson
July 18, 2016	3.3	Updated GA SQL Server configuration procedure.	Craig A. Benson
August 4, 2016	3.4	Updated GA SQL Server configuration procedure.	Craig A. Benson
November 4, 2016	3.5	Added new SSAS cube development procedure. Updated “state.vt.us” email addresses to use “vermont.gov”. Updated address in footer.	Craig A. Benson
January 13, 2017	3.6	Updated GA SQL Server configuration procedure.	Craig A. Benson
November 14, 2017	3.7	Updated GA SQL Server configuration procedure to accommodate SQL 2016.	Craig A. Benson

Table of Contents

Table of Figures

1 Brief Description

This document details the procedures for developing, testing, maintaining and supporting AHS SQL Servers and SQL databases. The procedures outlined herein were derived from enterprise-scale industry best practices and they form the basis upon which AHS SQL Server policies and standards were created.

Questions pertaining to AHS SQL Server environment procedures must be directed to the AHS Director of Data Services.

2 Scope

This document was written for database administrators (DBAs), database and application developers, server administrators (SAs), network administrators (NAs) and IT managers. The procedures contained herein are specific to SQL Server; it contains the boundaries in which SQL Servers and SQL databases are to be implemented in the AHS domain. These procedures extend beyond that of AHS-developed SQL Server solutions; it is highly recommended that all purchased, contracted or otherwise acquired SQL Server-based applications also conform to these procedures as to maintain a consistent, stable SQL Server environment.

3 Procedures Enforcement

All designated AHS DBAs are responsible for upholding and enforcing the procedures contained herein. Violations of any procedure must be documented using the AHS SQL Server Environment Policy Exception Form and submitted to the AHS Director of Data Services. Execution plans must be written, coordinated and implemented in a timely manner to correct all procedure violations.

Procedure exceptions will be clearly stated within each applicable section; otherwise all procedures will be enforced on a no exception basis. Clearance for any procedure exception must be granted in writing by the AHS Data Services Governance Committee (ADSGC).

4 References

- AHS Data Services Glossary
- AHS Data Services Web Portal
- AHS Data Services Data Dictionary Template
- AHS Data Services Report Specification Template
- AHS Data Services Update Form
- AHS Data Services Policy Exception Form
- AHS Data Services Employee Data Access Request Form
- AHS Data Services Vendor / Contractor Data Access Request Form
- AHS SQL Server Environment Standards
- AHS SQL Server Environment Procedures
- AHS SQL Server Environment Database Deployment Plan Template
- AHS SQL Server Environment Database Architecture Document Template
- AHS SQL Server Environment Database Administrator (DBA) Separation of Duties (SOD) Matrix
- AHS Information Technology and Electronic Communications Policies

5 Definitions, Abbreviations and Acronyms

Please reference the AHS Data Services Glossary.

6 Documentation Techniques

The following conventions are used throughout this document:

This convention	**Indicates**
CAPITAL LETTERS	Keys on the keyboard
KEY + KEY	Key combinations for which you must press and hold down one key and then press another key
[ ]	Information pertaining to a particular instance. Replace the brackets and the text between them with the respective instance of information, e.g. [ServerName] would be replaced with AHSSQLD01P if the applicable server pertained to AHSSQLD01P.
|	The pipe character indicates a logical 'OR' whereby the user must select one or another value
Highlighted Text	A button on an interface that requires a mouse click

7 Procedures

7.1 SQL Server GA OLTP/OLAP Database Server Configuration Procedure

Assumption: It is assumed that the person executing this procedure is an experienced AHS DBA.

All SQL Server 2012+ instances must be configured using the AHS Global Administration (GA) framework as follows. Unless otherwise noted, all steps in this procedure are to be accomplished via SSMS. The scripts identified in BLUE TEXT below are maintained by the Director of Data Services.

1. Create new non-expiring service accounts for the server using the AHS naming standard. Save the passwords in Secret Server. Each SQL service that is to be used should have its own account, e.g. Data Services service, SQL Agent service, Reporting Services service, Analysis Services service and/or Integration Services service.
2. Add the SQL Server and SQL Agent service accounts to the “SQL_BackupAccess” security group.
3. Create new “SQL_Admins_[SERVERNAME]”, “SQL_Managers_[SERVERNAME]” **(2012+ DEV & TEST only)** and “SQL_Stewards_[SERVERNAME]” **(2012+ DEV & TEST only)** Windows security groups for the server using the AHS naming standard (ensure the appropriate DBA’s user names and service accounts are in the respective groups). Allow Data Services Director to manage the group.
4. Add the 2 SQL Service accounts necessary for GA deployment automation to the “SQL_Admins_[SERVERNAME]” Windows security group
5. Add the new “SQL_Admins_[SERVERNAME]” Windows security group to the Local Administrators and Remote Desktop Users groups on the server
6. **(2012 only)** Using **gpedit.msc**, add the SQL Server service account to the “Windows Settings \ Security Settings \ Local Policies \ User Rights Assignment” **Lock pages in memory** and **Perform volume maintenance tasks** policies
7. Ideally, the server should contain five physical drives labled as C, D, F, L and T. Ensure all drives are at least RAID 1. If five physical drives are not available, e.g. when implementing a SAN, create five logical drives labeled as C, D, F, L and T. Depending on the anticipated capacity and transaction volume, designated LUN space may be required. Work with the SAN administrator accordingly.
8. Create the following directories on the server drives:

C:\ Deadlocks (for deadlock event XML files)

C:\SSIS-Config (for SSIS configuration files) **NOTE: Add the department subfolders, too!**

D:\SQL_Data (for SQL mdf and ndf data files)

D:\SQL_Data\dbGlobalAdmin (for GA mdf and ndf data files)

F:\SQL_Text (OPTIONAL for SQL full-text and BLOB files)

L:\SQL_Logs (for SQL ldf log files)

T:\SQL_Temp (for the SQL TempDB mdf data and ldf log files)

9. Move the installation media to the C:\Temp folder
10. Install SQL Server 2012+. **NOTE: Run as Administrator!**
    a. Ensure SQL Server and Windows Authentication are enabled during installation
    b. Ensure the SQL services are set to run using the corresponding Windows service account. **NOTE: Disable SQL Browser (default instances only)!**
    c. Set database / log / tempDB settings to default to those created in step 6 above.
11. Reboot the server
12. Install any necessary Service Packs. **NOTE: Turn off all SQL Services first!**
13. Delete the installation media from the C:\Temp folder
14. Create two scheduled tasks to start SQL Server and SQL Agent when they're not running.
    a. Create a new "AHS Global Administration" folder in the Task Scheduler Library folder in the Task Scheduler msc.
    b. Using the GA hub as a template, install the Start_SQL_Server.bat and Start_SQL_ServerAgent.bat files in the C:\Program Files\Microsoft SQL Server root directory, then export/import the two scheduled GA tasks to consume the files using the same parameters as on the GA hub. NOTE: Be sure to update the applicable login to the appropriate SQL Agent service account.
15. Update the firewall to allow the incoming port of 1433. Name the rule "SQL Server Inbound (1433)".
16. Reboot the server

17. From the server (remoting), enable Named Pipes from SQL Server Configuration Manager
18. Restart SQL Server
19. Add the new server to the Central Management Server Global Administration node.
20. Configure security logging for both failed and successful logins
21. Restart SQL Server
22. Create the DBA Operator

    Run the following script: STEP_01_Create_DBA_Operator.sql
23. Create Alerts

    Run the following script: STEP_02_CreateAlerts.sql
24. Set Up Database Mail

    Run the following script: STEP_03_SetUpDatabaseMail_EDIT_ME_FIRST.sql

    NOTE: You must enter the SQL Agent service account and password before executing the script!
25. Create User-Defined Error Messages

    Run the following script: STEP_04_CreateUserDefinedErrorMessages.sql
26. Set SQL Agent Alert System Properties
    a. Enable Database Mail System and DBA Profile
    b. Enable Fail Safe Operator to DBA Operator
    c. Select Token Replacement

    (2012 only): Run the following script: STEP_05_Set_SQL_AgentProperties.sql
27. **(2012 only):** Update Registry Keys

    Run the following script: STEP_06_UpdateRegistryKeys.sql
28. **(2012 only):** Move / adjust number of files in the tempdb

    Run the following script: STEP_07_MoveTempDB.sql
29. **(2012 only):** Restart SQL Server
30. **(2012 only):** Delete the defunct tempDB .mdf file from the T:\SQL_Temp folder on the server
31. Enable OLE, Ad Hoc Distributed Queries and SQL startup procedures options

Run the following script: STEP_08_Enable_OLE_and_StartupProceduresOptions.sql

32. Create the dbGlobalAdmin Database (empty database). NOTE: Be sure to place the files in the D:\SQL_Data\dbGlobalAdmin folder and select the Simple recovery model.
33. Restore the GA Database from another GA server. NOTE: There is an apparent glitch in the 2012+ SSMS Restore Database dialog box—the File page sometimes does not display the database files right away (please wait).
34. Drop all non-Microsoft-shipped users from GA database
35. Truncate all GA log and inventory tables

    Run the following script: STEP_09_Truncate_GA_InventoryLogTables.sql
36. Create the GA Database Owner

    Run the following script: STEP_10_Create_GA_DatabaseOwner_EDIT_ME_FIRST.sql

    NOTE: You must enter the DBO_dbGlobalAdmin password before executing the script!
37. Create the GA Server Triggers

    Create the following server triggers using the GA hub server as a model:

    a. Send_SA_ConnectionAlert

    b. SendDatabaseCreationAlert

    c. SendDatabaseDropAlert

    d. SendEventActivityAlert
38. Create the GA Deadlock Structure

    Create the following objects using the GA hub server as a model:

    a. Capture_GA_DeadlockEvent (job)

    b. CaptureDeadlockEvent (alert)

    NOTE: Delete the @job_id from the script before running. Also, after creating the alert, update it to respond to the Capture_GA_DeadlockEvent job!
39. Create the GA Jobs

    Create the following jobs using the GA hub server as a model:

    a. Check_GA_AvailableDiskSpace *

    b. Check_GA_Jobs *

c. Check_GA_LogSchemaChangeExists *

d. Check_GA_RolesExist *

e. Delete_GA_DB_Mail *

f. Execute_GA_ServerReboot *

g. Execute_GA_StartupOptions *

h. IndexUserDatabases *

i. Insert_GA_Inventory *

j. Insert_GA_Logs

k. Purge_GA_Logs *

l. Synchronize_GA_DatabaseExtendedProperties *

m. TruncateDatabaseLogs(SimpleRecovery) *

40. Test the GA jobs marked with an asterisk (*) above

41. Establish GA tool acces

    Run the following script: STEP_11_Set_GA_ToolAccess.sql

42. Create the Server, Backups and MaintenanceLogs directories in the AHS SQL backup area

43. Create the following database maintenance plans using the GA hub server as a model:

    a. BackupSystemDatabases(Full)

    b. BackupUserDatabases(Full)

    c. BackupUserDatabases(TransactionLogs) **NOTE: Production Database Services servers only!**

    d. CheckSystemDatabaseIntegrity

    e. CheckUserDatabaseIntegrity

    f. DeleteHistory

    NOTE: The plan within the maintenance plans must be named “RunPlan”. All maintenance plans must log to the designated AHS log area. Very large databases may have specific maintenance plans that should be excluded from the above list as necessary—these must include the name of the respective department / agency acronym and the name of the respective database.

44. Change the maintenance plan ownership to the SQL Agent account

    Run the following script:

    STEP_12_ChangeMaintenancePlanOwnership.sql

45. Update all jobs to have the proper SQL Agent account owner, a description, and notification settings

    Run the following script:

    STEP_13_UpdateJobOwnerDescriptionNotification_RUN_SUB-SCRIPT.sql

    NOTE: There is a SELECT statement in the script that should be run first to create the EXEC statements that should subsequently be run to perform the job updates!

46. Disable the ‘sa’ login and set server backup compression default.

    Run the following script:

    STEP_14_Disable_SA_Login.sql

47. Test the maintenance jobs. Validate files are going to the correct backup and log folders.

48. Create the GA Audit and Audit Policy. **NOTE: SQL 2012+ Developer and Enterprise Editions only!**

    Run the following script:

    STEP_15_Create_GA_AuditPolicy.sql

49. Create the GA System Manager and System Steward server roles (and logins if server is a Database Services engine (OLTP/OLAP databases). **NOTE: SQL 2012+ only, and if it’s a production instance, the server roles will be created but the System Manager and System Steward Windows logins will not be!**

    Run the following script:

    STEP_16_Create_GA_ServerRoles.sql

50. Assign the msdb permissions. **NOTE: SQL 2012+ only, and if server is a DEV or TEST Database Services engine!**

    Run the following script:

    STEP_17_Assign_msdb_Permissions.sql

51. Create the four master database stored procedures (RunServerBlitz, GenerateLoginSyntax, ConvertHexadecimal, Start SQL_Agent) using the GA hub server as a model

52. Set the Send_DBA_ServerStartupEmail stored procedure to run at startup.

    Run the following script:

    STEP_18_Set_SQL_StartupProcedure_RESTART_AFTER_ME.sql

53. Restart SQL Server

54. Create the PreventNonSystemAdministrator_DDL_Events database trigger on the master database using the GA hub server as a model

55. Set the master database trigger order.

    Run the following script:

    STEP_19_Set_master_DB_TriggerOrder.sql

56. Move master encryption key backup file to the C:\Temp directory on the server (copy the file from \\ahs\ahsfiles\AHS ALL SHARE\AHS IT DBA\SQL_GlobalAdministration\GA_SMK_KeyBackup

57. Create the 2 logins necessary for GA deployment automation and restore the master encryption key (MEK).

    Run the following script:

    STEP_20_Create_GA_DeploymentLoginsRestore_MEK.sql

58. Delete MEK backup file from the C:\Temp directory on the server

59. Set the model database to Simple recovery

60. Add the "SQL_Managers_[SERVERNAME]" and "SQL_Stewards_[SERVERNAME]" users to the model database and grant the "db_owner" role to both. **NOTE: SQL 2012+ only, and if server is a DEV or TEST Database Services engine!**

61. Update the "AUDIT-SECURITY", "SERVER-SPOKE" and "VERSION" codesets **(on HUB server)**

    1. Add the new server to the CodeValueServer table.
    2. Increment the VERSION / CODESET codes in the CodeValue table.
    3. Add the new "SQL_Admins_[SERVERNAME]" Windows security group to the "AUDIT-SECURITY" codeset in the CodeValue.
    4. Run the Synchronize_GA_CodesetConstrained job on AHSSQLI01P to publish codesets to all spoke servers.

==

SSRS Installation Only

1. Using SSRS Configuration Manager (on the server)…

    a. Backup SSRS Encryption Key to Y:\AHS ALL SHARE\AHS IT DBA\SQL_Server\SQL_2012\SSRS\EncryptionKeyBackups\[ServerName] NOTE: Use the password from the ahs.sql.reports service account.

    b. Configure email settings using the DoNotReply@vermont.gov account as the Sender Address and "relay.vermont.gov" as the SMTP server

c. Configure the execution account using the “AHS\ahs.sql.reports” account

2. Using SSRS Reports Manager (web interface), create the following report folders: AHS, AHSCO, DAIL, DCF, DMH, DOC, DVHA, VDH. Be sure to supply folder descriptions
3. Add the “SQL_SSRS_ContentManagers_[SERVERNAME]” security group to the Content Manager role in the Home folder. **NOTE: DEV and TEST servers only!**
4. If the SSRS server is a production instance; using SSMS (SSRS Connection), update the “ExecutionLogDaysKept” setting on the Advanced tab of the server’s properties to be “365” (the default is “60”)
5. Enable SSRS HTTP logging. Update the SSRS configuration file (**ReportingServicesService.exe.config**) located here: C:\Program Files\Microsoft SQL Server\MSRS11.MSSQLSERVER\Reporting Services\ReportServer\bin\.

   Overwrite the <RStrace> section with the following (**NOTE: The KeepFilesForDays attribute should be set to 90 for DEV and TEST servers and 365 for PROD servers**):

```
  <RStrace>
    <add name="FileName" value="ReportServerService_" />
    <add name="FileSizeLimitMb" value="32" />
    <add name="KeepFilesForDays" value="90" />
    <add name="Prefix" value="appdomain, tid, time" />
    <add name="TraceListeners" value="debugwindow, file" />
    <add name="TraceFileMode" value="unique" />
    <add name="HttpTraceFileName" value="ReportServerService_HTTP_" />
    <add name="HttpTraceSwitches" value="date,time,
clientip,username,serverip,serverport,host,method,uristem,uriquery,protocolst
atus,bytesreceived,timetaken,protocolversion,useragent,cookiereceived,cookies
ent,referrer" />
    <add name="Components" value="all:3,http:4" />
  </RStrace>
```

   Save the file.

===

SSIS Installation Only

1. Using SSMS (SSIS Connection), create a “SSIS_Packages” folder in the Stored Packages \ MSDB folder, then create the following package folders in the “SSIS_Packages” directory: AHS, AHSCO, DAIL, DCF, DMH, DOC, DVHA, VDH
2. Create the “SQL_SSIS_Admins_[SERVERNAME]” login and assign the msdb “db_ssisadmin” database role. **NOTE: DEV and TEST servers only!**

3. Assign the msdb permissions to the "SQL_SSIS_Admins_[SERVERNAME]" login. **NOTE: DEV and TEST servers only!**

   Edit and run the following script (Changing references of "SQL_Managers_" to be "SQL_SSIS_Admins_" and commenting-out all references of "SQL_Stewards_" code:

   STEP_17_Assign_msdb_Permissions.sql

4. Create a share on the new server of the \\[ServerName]\C$\SSIS-Config directory. Allow the SQL_SSIS_Admins_[ServerName] security group access to the share.

5. Grant "SQL_SSIS_Admins_[SERVERNAME]" access to the Integration Services service. **NOTE: DEV and TEST servers only!**

   a. Run Dcomcnfg.exe. Dcomcnfg.exe provides a user interface for modifying certain settings in the registry.

   b. In the Component Services dialog, expand the Component Services > Computers > My Computer > DCOM Config node.

   c. Right-click Microsoft SQL Server Integration Services 11.0, and then click Properties.

   d. On the Security tab, click Edit in the Launch and Activation Permissions box and add "SQL_SSIS_Admins_[SERVERNAME]" and check all permissions, and then click OK.

   e. On the Security tab, click Edit in the Access Permissions box and add "SQL_SSIS_Admins_[SERVERNAME]" and check all permissions, and then click OK.

   f. On the Security tab, click Edit in the Configuration Permissions box and add "SQL_SSIS_Admins_[SERVERNAME]" and check all permissions, and then click OK.

   g. Click Apply, then OK, then close the Component Services window.

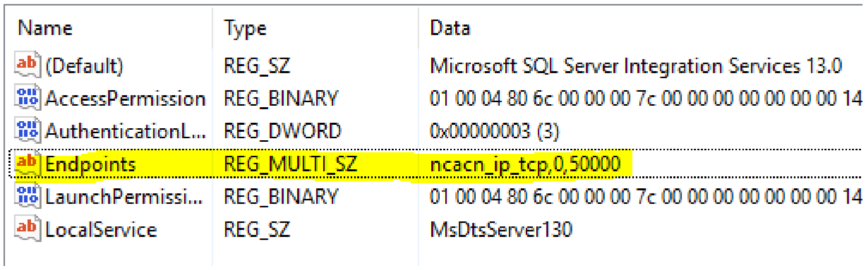
   h. Open Computer Management \ Local Users and Groups

   i. Add the "SQL_SSIS_Admins_[SERVERNAME]" group to the "Distributed COM Users" and "Remote Desktop Users" groups, then click OK.

   j. Reboot the server.

6. Update the server's registry.

a. Add an “Endpoints” Multi-String type with the value of “ncacn_ip_tcp,0,50000” to the applicable SSIS key.



Name	Type	Data
(Default)	REG_SZ	Microsoft SQL Server Integration Services 13.0
AccessPermission	REG_BINARY	01 00 04 80 6c 00 00 00 7c 00 00 00 00 00 00 00 14
AuthenticationL...	REG_DWORD	0x00000003 (3)
Endpoints	REG_MULTI_SZ	ncacn_ip_tcp,0,50000
LaunchPermissi...	REG_BINARY	01 00 04 80 6c 00 00 00 7c 00 00 00 00 00 00 00 14
LocalService	REG_SZ	MsDtsServer130

Figure 1 - Registry Update

7. Add two inbound Firewall rules on server.

a. Rule 1: Port-based (135), titled “SQL Server SSIS Inbound (135)”

b. Rule 2: Executable-based (MsDtsSrvr.exe), titled “SSIS Service Exception”

===

SSAS Installation Only

1. Log on to the server and update the firewall to allow the incoming port of 2383. Name the rule “SQL Server Inbound (2383)”.
2. Restart the server
3. Add the “SQL_SSAS_Admins_[SERVERNAME]” security group to the Server Administrator role. **NOTE: DEV and TEST servers only!**

7.2 Ad-Hoc Backup Database Procedure

7.2.1 Assumptions

- The SQL Server is running, operational and connected to the network
- You have the “sysadmin” server role privileges
- You have access to the designated AHS backup area
- The database to be backed up is operational

7.2.2 Backing up a SQL 2005+ or 2000 Database to an Existing Backup Set

Most often, backing up to an existing backup set will suffice the need for a backup (if not, reference the following sections on backing up to an alternate backup set). To backup a SQL 2005+ or 2000 database, perform the following:

1. Open SSMS or EM respectively and navigate to the database to be backed up

2. Right click on the database and select the ‘Tasks / Back Up’ (SQL 2005+) or ‘All Tasks / Backup Database’ (SQL 2000) context menu option (the backup database dialog box will appear)
3. Leave all fields defaulted—just click OK (the database will then be backed up…you should receive a confirmation once SQL server has completed the backup)

7.2.3 Backing up a SQL 2005+ Database to an Alternate Backup Set

Perform the following:

1. Open SSMS
2. In the ‘Object Explorer’ panel, right click the database to be backed up and select the ‘Tasks / Back Up’ context menu option
3. Enter an optional description of the backup in the ‘Description’ text box
4. Select the type of backup in the ‘Backup Type’ combo box. NOTE: ‘Full’ is the default and for most situations, this option will suffice.
5. Do not use the existing selected destination; you will need to remove it. Click Remove (the selection will be removed from the ‘Backup to’ field
6. Click Add… (the ‘Select Backup Destination’ dialog box will appear)
7. In the ‘File name’ field, enter the UNC path to where the backup is to be created. NOTE: Ensure the backup is created in the designated VDH SQL backup directory and has a file extension of ‘.BAK’. E.g. \\Nessie\sqlbackup$\[ServerName]\[DatabaseName]\[FileName].BAK
8. Click OK (the ‘Select Backup Destination’ dialog box will close)
9. Click OK (the database will then be backed up…you should receive a confirmation once SQL server has completed the backup)

7.2.4 Backing up a SQL 2000 Database to an Alternate Backup Set

Perform the following:

1. Open EM
2. In the left-hand panel, navigate to and expand the ‘Databases’ folder of the SQL server that hosts the database to be backed up
3. Right click on the database to be backed up and select the ‘All Tasks / Backup Database’ context menu option (the ‘SQL Server Backup - [DatabaseName]’ dialog box will appear)
4. Enter an optional description of the backup in the ‘Description’ text box
5. Select the type of backup in the ‘Backup’ section. NOTE: ‘Database – complete’ is the default and for most situations, this option will suffice.
6. Do not use the existing selected destination; you will need to remove it. Click Remove (the selection will be removed from the ‘Backup to’ field
7. Click Add… (the ‘Select Backup Destination’ dialog box will appear)
8. In the ‘File name’ field, enter the UNC path to where the backup is to be created. NOTE: Ensure the backup is created in the designated VDH SQL

backup directory and has a file extension of '.BAK'. E.g. \\Nessie\sqlbackup$\[ServerName]\[DatabaseName]\[FileName].BAK

9. Click OK (the 'Select Backup Destination' dialog box will close)
10. Click OK (the database will then be backed up…you should receive a confirmation once SQL server has completed the backup)

7.3 Ad-Hoc Restore Database Procedure

7.3.1 Assumptions

- The SQL Server is running, operational and connected to the network
- You have the "sysadmin" server role privilege
- If restoring from a SQL backup, you have access to the database and transaction log SQL backup files (.BAK and .TRN) located in the AHS backup area
- SQL Server maintenance plan log files, which are very useful for debugging job failures, are located in the AHS log area

NOTE: Before restoring any database, all users (except yourself) should be logged off of the applicable database. Before restoring any system database, all users (except yourself) should be logged off of the applicable SQL server because a reboot is required. For SQL 2000 system database issues, be sure system databases and objects are visible in EM for the respective server on which the system database is to be restored (see APPENDIX B on how to view/hide system databases and objects in EM). Take the necessary steps to alert all users in advance that the respective database and/or server will be unavailable.

7.3.2 Restoring a Database from SQL Backups (.BAK and .TRN files)

Perform the following:

1. Open SSMS or EM respectively and navigate to and expand the 'Databases' folder of the SQL server that hosts the database to be restored
2. Right click on the database to be restored and select the 'Tasks / Restore / Database' (SQL 2005+) or 'All Tasks / Restore Database' (SQL 2000) context menu option (the 'Restore Database' dialog box will appear)

   NOTE: In the 'Type' column in the grid, notice the two types of backups. These are called 'backup sets.' There may be no transaction logs to back up, as in the case of system databases, or there may be multiple transaction logs backed up. You must determine the appropriate backup set to restore the database in order to prevent a loss of data and/or prevent a recreation of why the database needed to be restored in the first place.

3. Select the appropriate backup sets to be restored. If you need to restore the database to a specific point in time, you must first ensure the backup sets selected coincide with the desired point in time (**uncheck all others**)! Next, click the … button next to the 'To a point in time' field (SQL 2005+) or the 'Point in time restore' check box (SQL 2000) and select the appropriated date and time in the 'Point in Time Restore' dialog box. Again, the point in time must coincide with the selected backup sets (SQL Server will warn you if your point in time does not coincide).
4. Click OK.
5. Click the 'Options' tab
6. Ensure the 'Overwrite the existing database' (SQL 2005+) or 'Force restore over existing database' (SQL 2000) option is selected
7. Click OK (the database will then be restored…you should receive a confirmation once SQL server has completed the restoration)

7.3.3 Restoring a Database from Device (.MDF and .LDF files)

Perform the following:

1. Open SSMS or EM respectively and navigate to and expand the 'Databases' folder of the SQL server that hosts the database to be restored
2. Right click on the database to be restored and select the 'Tasks / Restore / Database' (SQL 2005+) or 'All Tasks / Restore Database' (SQL 2000) context menu option (the 'Restore Database' dialog box will appear)
3. Select the 'From Device' option
4. For SQL 2005+, click the … button next to the 'From Device' field (the 'Specify Backup' dialog box will appear). For SQL 2000, click Select Devices… (the 'Choose Restore Devices' dialog box will appear)
5. Click the Add… button (for SQL 2005+ the 'Locate Backup File' dialog box will appear; for SQL 2000 the 'Choose Restore Destination' dialog box will appear)
6. For SQL 2005+, enter the UNC path in the 'Selected path' field. For SQL 2000, ensure the 'File name' option is selected. NOTE: It is not necessary to select the 'Backup device' option; it adds two additional steps!
7. In the 'File name' field: For SQL 2005+, enter the file name of the .MDF file from which you are performing the restore or for SQL 2000, enter the complete UNC file path/name of the .MDF file from which you are performing the restore.
8. Click OK
9. Click OK
10. Click the 'Options' tab
11. Ensure the 'Overwrite the existing database' (SQL 2005+) or 'Force restore over existing database' (SQL 2000) option is selected

12. Ensure the drive letters and file paths are correct in the grid. These are the respective database's .MDF and .LDF files that are to be restored from the .MDF file selected in step 8 above. It is important that the file paths be exact, as an error will occur or you may overwrite the wrong database. Make changes as necessary.
13. Click OK (the database will then be restored…you should receive a confirmation once SQL server has completed the restoration)

7.4 Rebuild SQL Server Procedure

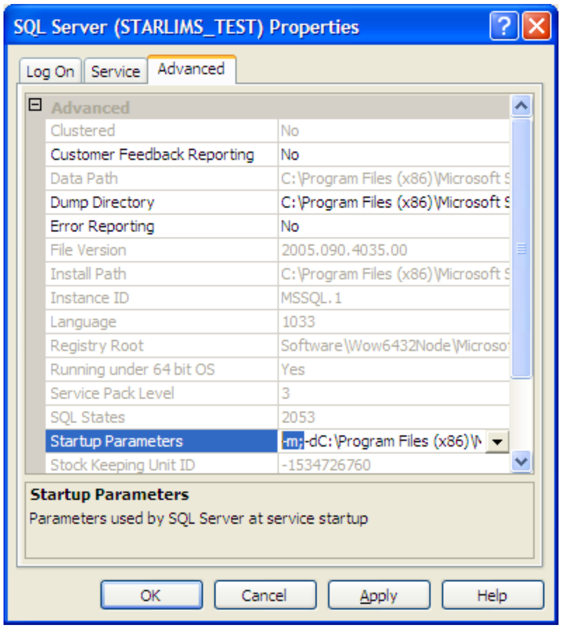
7.4.1 Assumptions

- Windows Server and SQL Server have been installed on the respective machine with all patches/hot fixes (hopefully exactly as the machine was prior to the rebuild). NOTE: This is an absolute necessity in order for the rebuild to be successful. Work with AHS Computer Operations as to ensure this is carried out.
- The server is running on the network
- The SQL_Admins_[ServerName] security group is in the Administrators group on the server
- The D, F, L and T drives were created (F is optional)
- You have access to the SQL Server and Agent service account passwords
- The *most recent* backups of all system and user databases are available for restoration. Ideally, full backups of all the databases should be taken before the server that requires rebuilding is taken offline.

7.4.2 Rebuild the SQL Server

Once AHS Computer Operations has installed the OS and all appropriate patches and hotfixes, perform the following:

1. Ensure the default drives and
2. Install SQL Server (**only steps 1 – 7 in the procedure above**)
3. Copy all system and user database backups to the server's C:\Temp directory (ensure the system backups are named "master.bak", "model.bak" and "msdb.bak" respectively)
4. Remote to the server
5. Open SSCM.
6. Click "SQL Server [YYYY] Services" in the left-hand navigation panel.
7. Stop all SQL Server services listed in the right-hand panel by right clicking on each and selecting "Stop" from the context menu.
8. Temporarily set the SQL Server to start in Single User mode by right clicking on "SQL Server ([ServerName])" in the right-hand panel and selecting "Properties" from the context menu (the SQL Server Properties dialog box will appear).
    i. Click on the "Advanced" tab.
    ii. Enter "-m;" at the front of the Startup Parameters string.



Advanced	
Clustered	No
Customer Feedback Reporting	No
Data Path	C:\Program Files (x86)\Microsoft S
Dump Directory	C:\Program Files (x86)\Microsoft S
Error Reporting	No
File Version	2005.090.4035.00
Install Path	C:\Program Files (x86)\Microsoft S
Instance ID	MSSQL.1
Language	1033
Registry Root	Software\Wow6432Node\Microso
Running under 64 bit OS	Yes
Service Pack Level	3
SQL States	2053
Startup Parameters	-m;-dC:\Program Files (x86)\M
Stock Keeping Unit ID	-1534726760

Startup Parameters
Parameters used by SQL Server at service startup

Figure 2 - SQL Server Properties (from SSCM)

iii. Click OK

9. Right click "SQL Server ([ServerName])" and select "Start" from the context menu option (the SQL Server will start in Single User mode).
10. Open a command window (leave SSCM open, but minimize it).
11. Change directories to C:\Temp (type "cd C:\Temp").
12. Run the following command to restore the master database:

    sqlcmd –S .\[InstanceName]–e –q "RESTORE DATABASE master FROM DISK = 'C:\Temp\master.bak' WITH REPLACE;"

    NOTE: Wait for the command to finish!

13. Type "exit" and press ENTER.
14. Minimize command window and maximize SSCM.
15. Restart the SQL Server by right clicking on "SQL Server ([ServerName])" and selecting "Restart" from the context menu.
16. Right click "SQL Server Browser" and select "Start" from the context menu to start the service.
17. Minimize SSCM and maximize command window
18. Run the following command to disable all server triggers (this is needed to restore the model and msdb databases):

    sqlcmd –S .\[InstanceName] –A –e –q "DISABLE TRIGGER ALL ON ALL SERVER;"

NOTE: Wait for the command to finish!

19. Type “exit” and press ENTER.
20. Remove the “-m;” Startup Parameter entered in step 17 above (reverse the step).
21. Reboot the server (remote desktop window will close).
22. Open SSMS.
23. Connect to the server.
24. Run the following query to restore the model database:

```
RESTORE DATABASE model FROM DISK = ‘C:\Temp\model.bak’
WITH REPLACE;
```

25. Run the following query to restore the msdb database:

```
RESTORE DATABASE msdb FROM DISK = ‘C:\Temp\msdb.bak’
WITH REPLACE;
```

26. Remote to the server.
27. Reboot the server (remote desktop window will close).
28. Open SSMS.
29. Validate SQL Server configuration (i.e. jobs, alerts, operators, etc. should all be present).
30. Execute the following query to restore the GA database:

```
RESTORE DATABASE dbGlobalAdmin FROM DISK =
‘C:\Temp\dbGlobalAdmin_backup_[time-stamp].bak’ WITH REPLACE;
```

NOTE: If applicable, be sure to replace the [time-stamp] portion of the query above with how it is specified in the name of the backup file.

31. Restore all remaining user databases from the query window.
32. Reenable server triggers by executing the following query:

```
ENABLE TRIGGER ALL ON ALL SERVER;
```

33. Ensure all applicable software applications are able to connect to the SQL Server.
34. Monitor SQL Server for at least one full job cycle and make adjustments as necessary.

7.5 Database / Report Development & Defect Resolution Procedures

7.5.1 New Work & Enhancements

Adhering to the AHS SQL Server Environment Standards and Policies documents, the database developer will…

1. Identify the need—server and / or database objects / code that must be created, updated or deleted based on a thorough analysis of a use case (UC) or a business requirements document (BRD). If report(s) is/are to be developed, Report Specification(s) must be completed. **Under no circumstance should development proceed unless all respective requirements are throroughly documented and analyzed.**
2. Ensure the DBA has been copied on all requirements
3. Ensure the DBA is involved in the analysis
4. Develop the database and/or report(s) according to requirements
5. Create a DAD either using the Data Services template, or have the DBA execute RedGate SQL Doc on the respective database. If the DAD template is used, follow all instructions contained therein (in italicized text) to avoid resubmissions. All DADs must be saved in the applicable project folder within the AHS Data Services documentation library folder for DADs: Y:\AHS ALL SHARE\AHS IT DBA\DocumentationLibrary\DADs. The DBA initially reviews the DAD (the DBA submits it to the Data Services Director for review and approval).
    a. Approval process is necessary to effectively manage change
    b. Changes may be recommended
    c. Approved DADs are posted to the Data Services web portal by the DBA
6. All source code is to be placed under source control. If no source control solution is in place, source code should be saved to the AHS SQL Script Library: Y:\AHS ALL SHARE\AHS IT DBA\SQL_ScriptLibrary.
7. Unit test all applicable objects / code
8. Ensure function testing is undergone by respective application development staff
9. Schedule and attend a code review (for review and approval) with the DBA (using the DAD as a blueprint)
    a. Changes to code / DAD may be recommended
        i. Retesting may be necessary
        ii. Another review may be necessary

iii. Reposting DAD may be necessary

10. Complete Database Deployment Plan (DDP) to move database objects / code to test environment using the Database Deployment Procedure
    a. Submit DDP to DBA for review and approval
11. Schedule and communicate test deployment to respective users and DBA
12. After deployment, communicate status to and ensure UA testing is undergone by respective users / stakeholders
    a. Changes to code / DAD may be necessary
        i. Retesting may be necessary
        ii. Another review may be necessary
        iii. Reposting DAD may be necessary
        iv. Redeployment to test environment may be necessary
13. Upon user-acceptance, create production Database Deployment Plan (DDP) using the test DDP as the basis (update as necessary)
    a. Submit DDP to DBA for review and approval
14. Schedule and communicate production deployment to respective users and DBA
    a. After deployment, communicate status to respective users

7.5.2 Defects

Adhering to the AHS SQL Server Environment Standards and Policies documents, the database developer will…

1. Make sure the defect was logged in at least one of the State's tracking systems (LANDesk and/or Jira)
2. Perform a thorough analysis in the development environment
3. Determine if the defect is database / report related, if not STOP HERE!
4. Determine if the PROD copy database on the development server needs to be refreshed
5. Work with the application developer to recreate the error on the PROD copy database on the DEV server
6. Determine if the behavior functions as designed
7. Work with the business analyst as needed for additional requirements (or clarity of requirements)
8. Update database objects and/or data to eradicate the defect on PROD copy database
9. After validation (unit testing), update all applicable objects on primary development database and/or VisualStudio (if SSRS report update is necessary)

10. Determine if the update involved schema / code changes and update DAD and/or RS documents accordingly
11. Complete and submit a Database Deployment Plan (DDP) to the DBA (DBA to review all artifacts—may result in QA check by Data Director)
12. Work with DBA to schedule deployment (DBA moves code to TEST server(s) and notifies users)
13. After deployment, remain available for QA / UA testing outcome
14. Upon successful QA and UA testing, update the DDP to deploy to PROD server and transmit to the DBA (DBA to review all artifacts—may result in QA check by Data Director)
15. Work with DBA to schedule deployment (DBA moves code to PROD server(s) and notifies users)
16. Developer updates AHS tracking system with notes on defect resolution

For more details on new work, enhancement and production defect workflows, follow the diagrams below.

7.5.3 Workflows

7.5.3.1 New Work & Enhancements: Getting from Request to Test

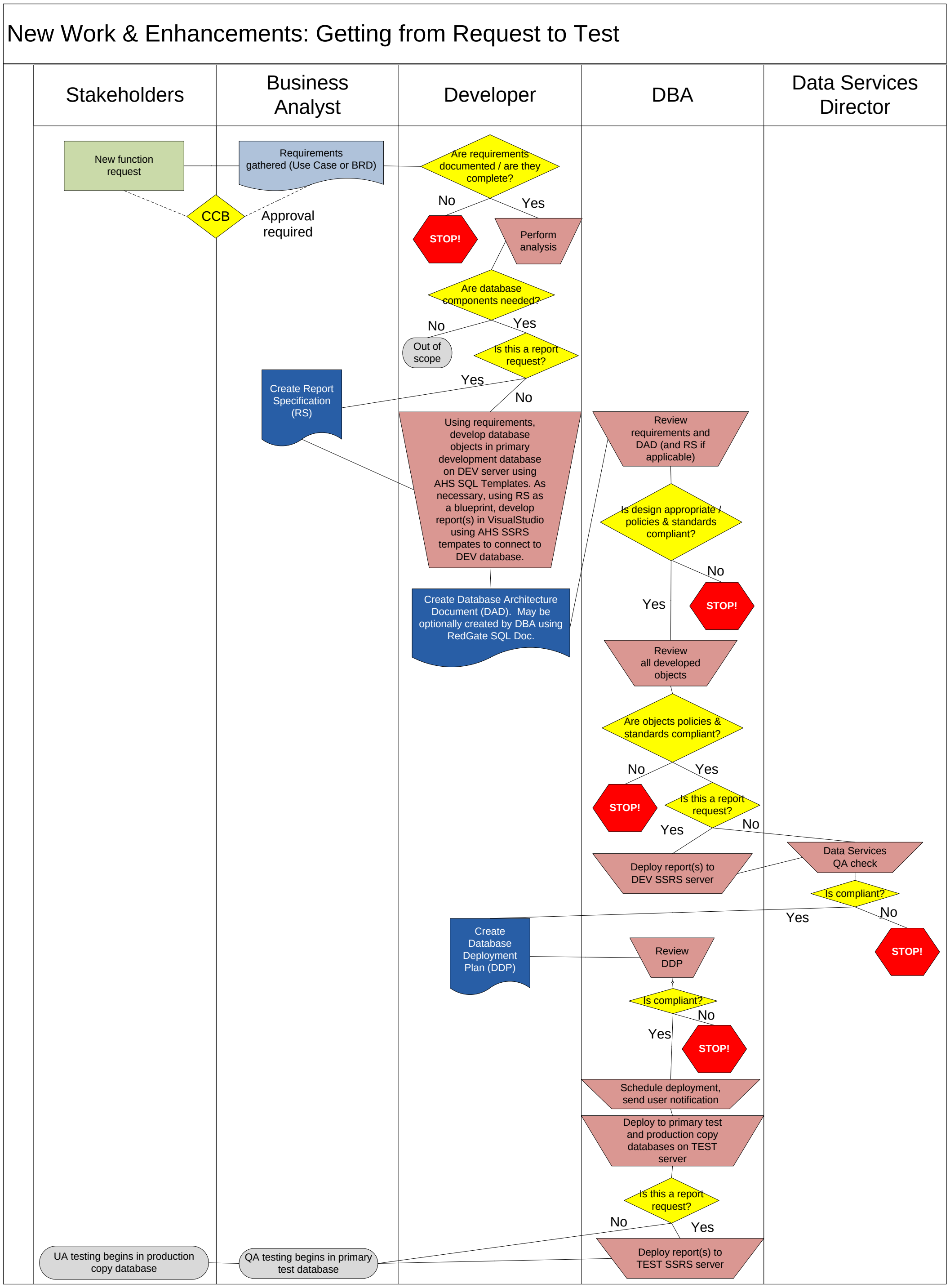

New Work & Enhancements: Getting from Request to Test
Stakeholders
Business Analyst
Developer
DBA
Data Services Director
New function request
Requirements gathered (Use Case or BRD)
CCB
Approval required
Are requirements documented / are they complete?
No
Yes
STOP!
Perform analysis
Are database components needed?
No
Yes
Out of scope
Is this a report request?
Yes
No
Create Report Specification (RS)
Using requirements, develop database objects in primary development database on DEV server using AHS SQL Templates. As necessary, using RS as a blueprint, develop report(s) in VisualStudio using AHS SSRS tempates to connect to DEV database.
Create Database Architecture Document (DAD). May be optionally created by DBA using RedGate SQL Doc.
Review requirements and DAD (and RS if applicable)
Is design appropriate / policies & standards compliant?
No
Yes
STOP!
Review all developed objects
Are objects policies & standards compliant?
No
Yes
STOP!
Is this a report request?
Yes
No
Deploy report(s) to DEV SSRS server
Data Services QA check
Is compliant?
Yes
No
STOP!
Create Database Deployment Plan (DDP)
Review DDP
Is compliant?
No
Yes
STOP!
Schedule deployment, send user notification
Deploy to primary test and production copy databases on TEST server
Is this a report request?
No
Yes
Deploy report(s) to TEST SSRS server
UA testing begins in production copy database
QA testing begins in primary test database

Figure 3 - New Work & Enhancements: Test Workflow *

7.5.3.2 Production Defects: Getting from Ticket to Test

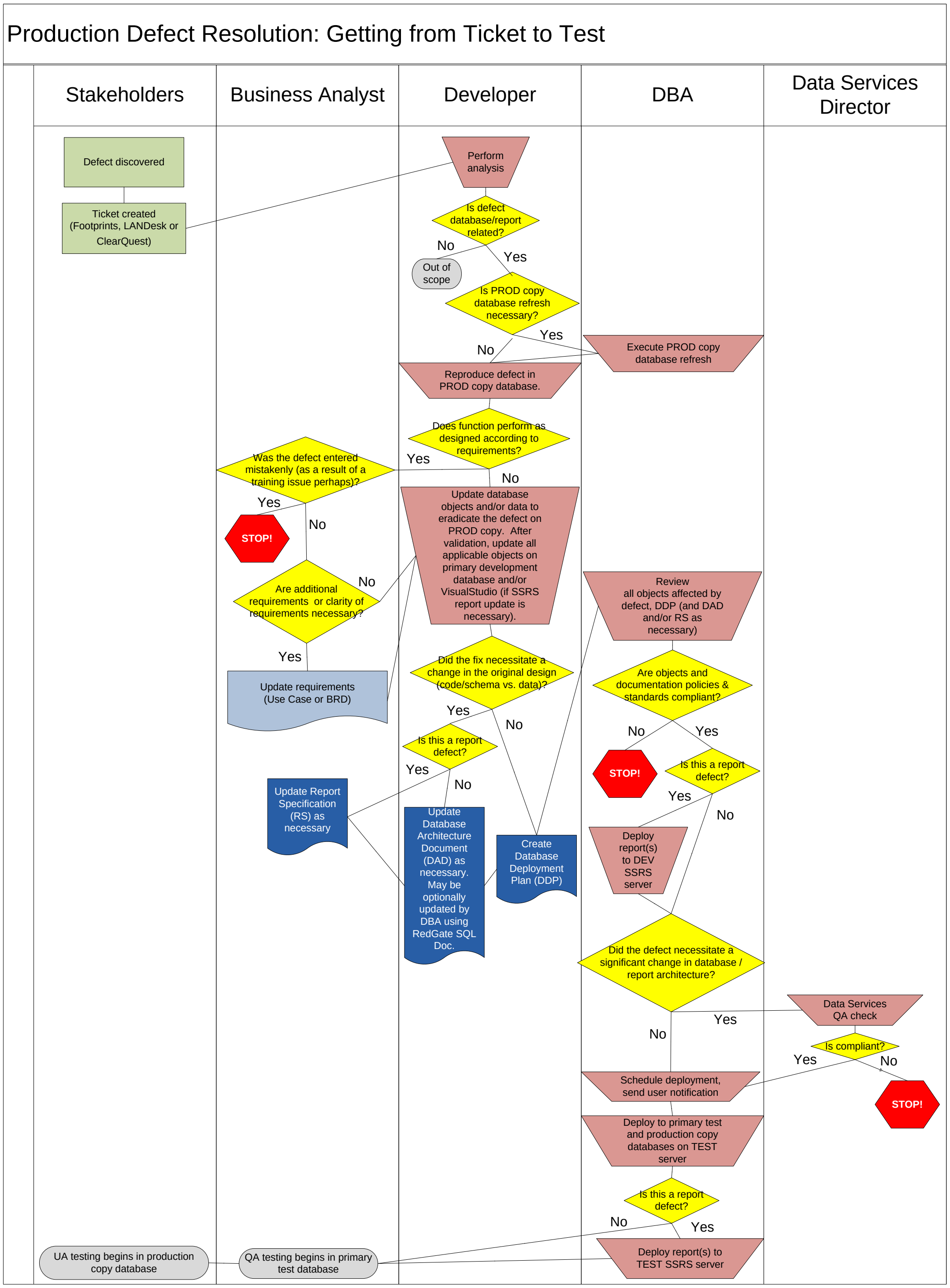

Production Defect Resolution: Getting from Ticket to Test
Stakeholders
Business Analyst
Developer
DBA
Data Services Director
Defect discovered
Ticket created (Footprints, LANDesk or ClearQuest)
Perform analysis
Is defect database/report related?
No
Out of scope
Yes
Is PROD copy database refresh necessary?
Yes
Execute PROD copy database refresh
No
Reproduce defect in PROD copy database.
Does function perform as designed according to requirements?
Yes
Was the defect entered mistakenly (as a result of a training issue perhaps)?
Yes
STOP!
No
Are additional requirements or clarity of requirements necessary?
No
Yes
Update requirements (Use Case or BRD)
No
Update database objects and/or data to eradicate the defect on PROD copy. After validation, update all applicable objects on primary development database and/or VisualStudio (if SSRS report update is necessary).
Review all objects affected by defect, DDP (and DAD and/or RS as necessary)
Did the fix necessitate a change in the original design (code/schema vs. data)?
Yes
No
Is this a report defect?
Yes
No
Update Report Specification (RS) as necessary
Update Database Architecture Document (DAD) as necessary. May be optionally updated by DBA using RedGate SQL Doc.
Create Database Deployment Plan (DDP)
Are objects and documentation policies & standards compliant?
No
STOP!
Yes
Is this a report defect?
Yes
Deploy report(s) to DEV SSRS server
No
Did the defect necessitate a significant change in database / report architecture?
Yes
Data Services QA check
Is compliant?
Yes
No
STOP!
No
Schedule deployment, send user notification
Deploy to primary test and production copy databases on TEST server
Is this a report defect?
No
Yes
Deploy report(s) to TEST SSRS server
UA testing begins in production copy database
QA testing begins in primary test database

Figure 4 - Production Defects: Test Workflow *

7.5.3.3 New Work, Enhancements, Defects: Getting from Test to Production

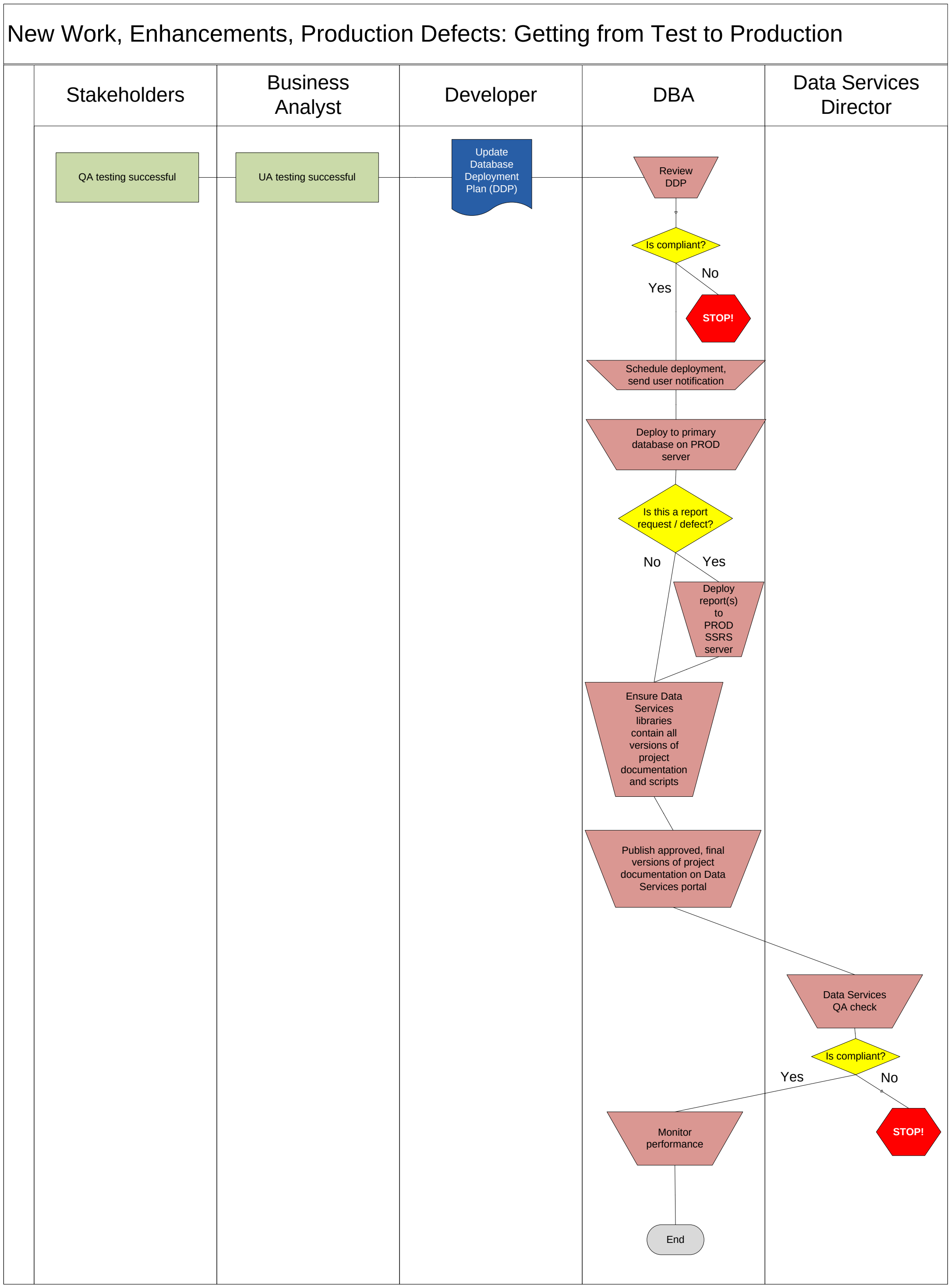

New Work, Enhancements, Production Defects: Getting from Test to Production
Stakeholders
Business Analyst
Developer
DBA
Data Services Director
QA testing successful
UA testing successful
Update Database Deployment Plan (DDP)
Review DDP
Is compliant?
No
Yes
STOP!
Schedule deployment, send user notification
Deploy to primary database on PROD server
Is this a report request / defect?
No
Yes
Deploy report(s) to PROD SSRS server
Ensure Data Services libraries contain all versions of project documentation and scripts
Publish approved, final versions of project documentation on Data Services portal
Data Services QA check
Is compliant?
Yes
No
STOP!
Monitor performance
End

Figure 5 - New Work, Enhancements, Production Defects: Production Workflow *

* NOTE:

1. Function Requests should be divided up into the smallest, easiest-to-consume work units possible so as to not bottleneck the development pipeline. If a Function Request yields multiple work units, only one work unit (or those dependent on one another) should be put into the development pipeline at a time.
2. The Business Analyst (BA) role may be performed by the Lead Stakeholder, i.e. the Subject Matter Expert (SME)
3. The Developer role may be performed by a DBA, in which case the DBA role will be performed by another DBA (separation of duties)
4. A Change Control Board (CCB) may exist between the Stakeholder and BA swim lanes. If so, the BA must be granted approval via the CCB to proceed.
5. Dark blue documents indicate Data Services templates
6. If a Project Manager is assigned, it is assumed s/he will span all swim lanes
7. Any STOP in workflow may cause rework within the previous swim lane(s) in order to address any deficiencies
8. Defects discovered as a result of QA/UA testing must undergo the same workflow—all documentation must be updated to reflect reality

7.6 Database Deployment Procedure

To deploy database changes, determine whether or not the deployment is appropriate to be processed through the GA tool (contact the respective DBA if uncertain). As a rule of thumb, deployments that encompass many phases should not be processed through the GA tool, rather through the DDP procedure.

7.6.1 GA Tool Deployments

Please reference the Quick Reference Guide under the Help \ Database Deployments menu in the GA tool.

7.6.2 DDP Procedure

Following the standards and policies as outlined in the AHS SQL Server Environment Standards and Policies documents, the database developer will…

1. Create a Database Deployment Plan (DDP) using the latest template found on the Data Services web portal and submit it to the DBA for review and approval. Follow all instructions contained therein (in italicized text) to avoid resubmissions. All DDPs must be saved by the DBA in the applicable project folder within the AHS Data Services documentation library folder for DDPs: Y:\AHS ALL SHARE\AHS IT DBA\DocumentationLibrary\DDPs.
    a. The DDP shall be completed in its entirety to represent all database objects required to be deployed. The DBA should not have any questions about what is involved and why the deployment needs to occur.

i. Approval process is necessary to effectively manage change

ii. Changes may be recommended

iii. Approved DDPs are save in the documentation library by the DBA

2. Work with the DBA and respective users to schedule the deployment

   a. DBA will communicate the deployment using the Data Services Update Notice email template to all respective development staff, users and stakeholders. The DDP will be attached to the notice (or referenced within the documentation library).

   b. If the DDP references any SQL scripts, all script files must be saved by the DBA to the AHS SQL Script Library: Y:\AHS ALL SHARE\AHS IT DBA\SQL_ScriptLibrary.

   c. Depending on the scope of the deployment, it may require off-hours work

   d. Developer attendance during the deployment may be recommended

   e. Upon completion of the deployment, the DBA will communicate the status to all respective development staff, users and stakeholders

   f. The DBA will monitor performance and may recommend optimization strategies

      i. Database development may need to occur (see Database Development Procedure)

7.7 Database Migration Procedure

Following the standards and policies as outlined in the AHS SQL Server Environment Standards and Policies documents, the DBA will…

1. Create a Database Migration Plan (DBMP) using the latest template found on the Data Services web portal and submit it to the Director of Data Services for review and approval. Follow all instructions contained therein (in italicized text) to avoid resubmissions. All DBMPs must be saved in the applicable project folder by the DBA within the AHS Data Services documentation library folder for DBMPs: Y:\AHS ALL SHARE\AHS IT DBA\DocumentationLibrary\DBMPs.

   a. The DBMP shall be completed in its entirety to represent all database endpoints and their configuration specifics. The DBA should not have any questions about what is involved and why the migration needs to occur.

      i. Approval process is necessary to effectively manage change

ii. Changes may be recommended

iii. Approved DBMPs are posted to the Data Services web portal by the DBA

2. Work with the Data Services Director and respective users to schedule the migration

   a. DBA will communicate the migration using the Data Services Update Notice email template to all respective development staff, users and stakeholders. The DBMP will be attached to the notice (or referenced within the documentation library).

   b. If the DBMP references any SQL scripts, all script files must be saved by the DBA to the AHS SQL Script Library: Y:\AHS ALL SHARE\AHS IT DBA\SQL_ScriptLibrary.

   c. Depending on the scope of the migration, it may require off-hours work

   d. Developer attendance during the migration may be recommended

   e. Upon completion of the migration, the DBA will communicate the status to all respective development staff, users and stakeholders

   f. The DBA will monitor performance and may recommend optimization strategies

7.8 Database Cataloging Procedure

Through the use of database extended properties, there are eight metadata elements that each user (non-system *) SQL database must employ. Database cataloging is to be maintained in the GA environment through the “DATABASE” codeset. The following are the extended property titles and descriptions of what need to be cataloged **:

Extended Property Title	Description
Applications	A comma-delimited list of all software executables that use the respective database as their data source
BusinessContacts	A comma-delimited list of fully-qualified email distribution groups (including the “@state.vt.us” suffix) of business personnel that should be contacted in the event of a database or server update. NOTE: Do not use security groups—use Exchange distribution groups. Do not list IT personnel unless the respective database fulfills an IT-only purpose.
Exports	A comma-delimited list of all batch export processes that obtain data from the respective database
Imports	A comma-delimited list of all batch import processes that insert data into the respective database
IT_Contacts	A comma-delimited list of fully-qualified email addresses of IT personnel, i.e. team leaders, supervisors, managers, etc., (including the “@state.vt.us” suffix) that should be contacted in

Extended Property Title	Description
	the event of a database or server update. NOTE: These individuals will be responsible for reviewing database deployment requests—list the email addresses in order of precedence. Do not list DBAs.
MS_Description	A thorough description of what data are contained within the respective database. The who, what, why, where, when and how the database fulfills its purpose. NOTE: This is the default extended property title—it is reserved for base object descriptions in SQL Server.
Owner	A comma-delimited list of Agency and/or Department acronyms that reflect data ownership (most often one department). See naming standards for list of approved acronyms.
Reports	A comma-delimited list of all reports that obtain data from the respective database

* System databases that do not require cataloging are as follows:

master
model
msdb
tempdb
ReportServer
ReportServerTempDB

** All eight properties must be created. If a database doesn't have imports, exports or reports, the respective property should still be created and its value should be blank.

Although SQL databases can be cataloged either through the Database Properties dialog box within SQL Server Management Studio (SSMS), through scripting, or through the GA tool (DBAs only), they must be maintained by the DBA via the GA Tool. The "DATABASE" codeset is synchronized across all GA servers so as to ensure consistency and accuracy.

NOTE: A database must be cataloged and the "DATABASE" codeset synchronized in order for a database to be created on a given GA server.

7.8.1 The Database Properties Dialog Box Method

1. Open SSMS and navigate to the server and database to be cataloged
2. Right click on the respective database and select the "Properties" context menu option (the Database Properties dialog box will open)

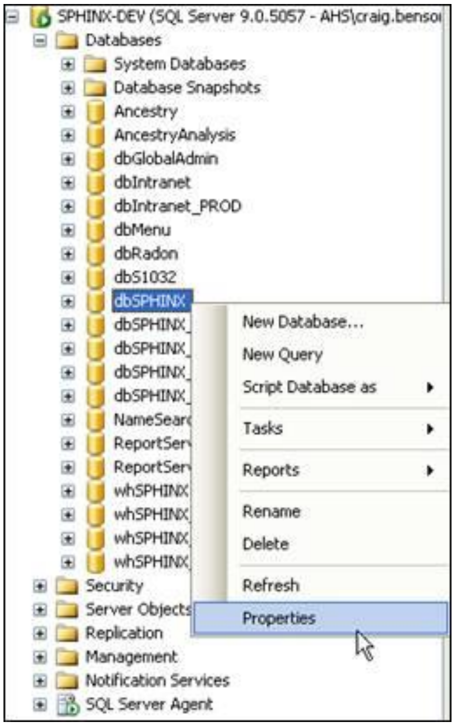
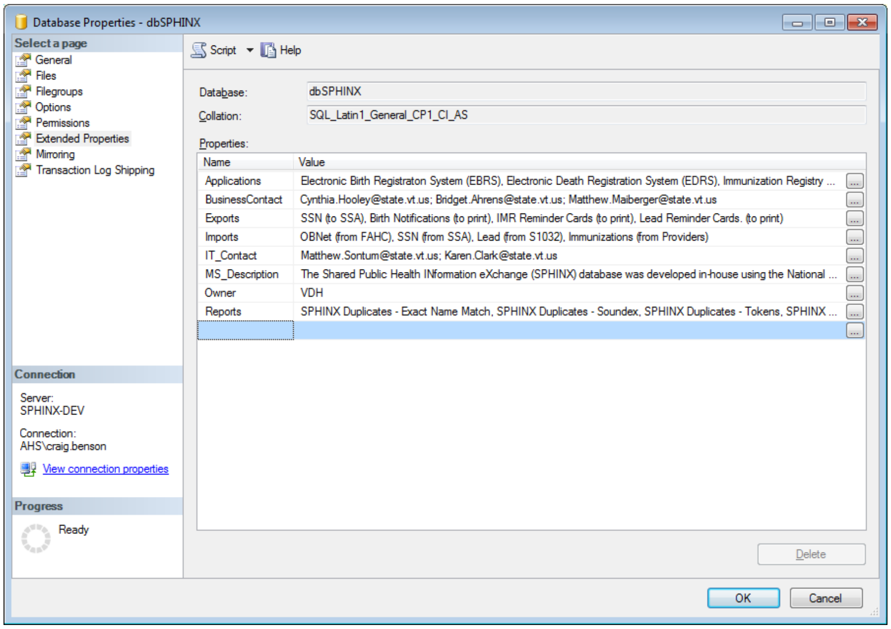


Figure 6 - Database Properties Context Menu Option

3. In the Database Properties dialog box, select the Extended Properties page. Add the eight extended properties for the database as described in the table above.



Server:
SPHINX-DEV

Connection:
AHS\craig.benson

Database: dbSPHINX

Collation: SQL_Latin1_General_CP1_CI_AS

Properties:

Name	Value
Applications	Electronic Birth Registraton System (EBRS), Electronic Death Registration System (EDRS), Immunization Registry ...
BusinessContact	Cynthia.Hooley@state.vt.us; Bridget.Ahrens@state.vt.us; Matthew.Maiberger@state.vt.us
Exports	SSN (to SSA), Birth Notifications (to print), IMR Reminder Cards (to print), Lead Reminder Cards. (to print)
Imports	OBNet (from FAHC), SSN (from SSA), Lead (from S1032), Immunizations (from Providers)
IT_Contact	Matthew.Sontum@state.vt.us; Karen.Clark@state.vt.us
MS_Description	The Shared Public Health INfomation eXchange (SPHINX) database was developed in-house using the National ...
Owner	VDH
Reports	SPHINX Duplicates - Exact Name Match, SPHINX Duplicates - Soundex, SPHINX Duplicates - Tokens, SPHINX ...

Figure 7 - Database Properties Dialog Box

4. Click OK
5. Repeat steps 1 through 4 for all user databases on the respective server

7.8.2 The SQL Script Method

1. Open SSMS and navigate to the server and database to be cataloged
2. Right click on the respective database and select the "New Query" context menu option (a new query window will open)
3. Copy and paste the following query to the new query window. Update the query to add the applicable metadata to each respective variable and then execute the query. NOTE: This query can be used to update any preexisting values as well.

```
DECLARE  @Applications     VARCHAR(2000),
         @BusinessContacts VARCHAR(2000),
         @Exports          VARCHAR(2000),
         @Imports          VARCHAR(2000),
         @IT_Contacts      VARCHAR(2000),
         @MS_Description   VARCHAR(2000),
         @Owner            VARCHAR(2000),
         @Reports          VARCHAR(2000);

SELECT /*Enter a comma-delimited list of all software executables
        that use the respective database as their data source */
         @Applications    = '',

       /*Enter a comma-delimited list of fully-qualified email
         addresses of business personnel that should be contacted
         in the event of a database or server update */
         @BusinessContacts = '',

       /*Enter a comma-delimited list of all batch export processes
         that obtain data from the respective database */
         @Exports      = '',

     /*Enter a comma-delimited list of all batch import processes
       that insert data into the respective database */
       @Imports      = '',

     /*Enter a comma-delimited list of fully-qualified email
       addresses of IT personnel (developers, IT managers, etc.)
       that should be contacted in the event of a database or
       server update.  NOTE: Do not list DBAs. */
       @IT_Contacts    = '',

     /*Enter a thorough description of what data are contained
       within the respective database.  The who, what, why, where,
       when and how the database fulfills its purpose.
       NOTE: This is the default extended property title—it is
       reserved for base object descriptions in SQL Server. */
       @MS_Description   = '',

     /*Enter a comma-delimited list of Agency and/or Department
       acronyms that reflect data ownership (most often one
       department).  See naming standards for list of approved
       acronyms. */
       @Owner          = '',

    /* Enter a comma-delimited list of all reports that obtain
       data from the respective database */
       @Reports      = '';

IF NOT EXISTS(SELECT 1 FROM sys.extended_properties WHERE class_desc = 'DATABASE' AND [name] = 'Applications')
      EXEC sys.sp_addextendedproperty @name = N'Applications', @value = @Applications;
ELSE
      EXEC sys.sp_updateextendedproperty @name = N'Applications', @value = @Applications;

IF NOT EXISTS(SELECT 1 FROM sys.extended_properties WHERE class_desc = 'DATABASE' AND [name] = 'BusinessContacts')
      EXEC sys.sp_addextendedproperty @name = N'BusinessContacts', @value = @BusinessContacts;
ELSE
      EXEC sys.sp_updateextendedproperty @name = N'BusinessContacts', @value = @BusinessContacts;

IF NOT EXISTS(SELECT 1 FROM sys.extended_properties WHERE class_desc = 'DATABASE' AND [name] = 'Exports')
      EXEC sys.sp_addextendedproperty @name = N'Exports', @value = @Exports;
```

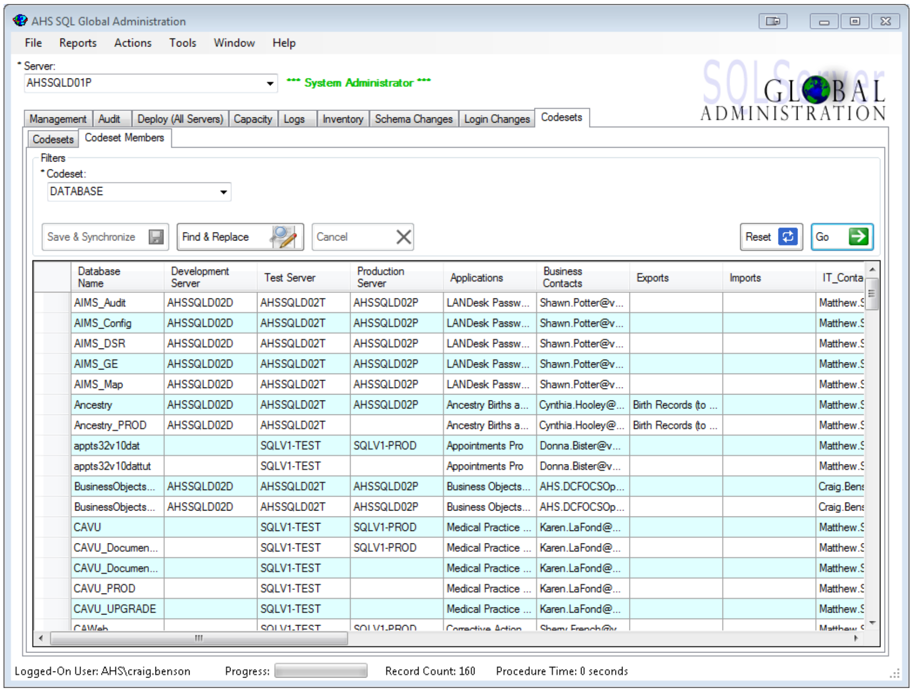
```
ELSE
      EXEC sys.sp_updateextendedproperty @name = N'Exports', @value = @Exports;

IF NOT EXISTS(SELECT 1 FROM sys.extended_properties WHERE class_desc = 'DATABASE' AND [name] = 'Imports')
      EXEC sys.sp_addextendedproperty @name = N'Imports', @value = @Imports;
ELSE
      EXEC sys.sp_updateextendedproperty @name = N'Imports', @value = @Imports;

IF NOT EXISTS(SELECT 1 FROM sys.extended_properties WHERE class_desc = 'DATABASE' AND [name] = 'IT_Contacts')
      EXEC sys.sp_addextendedproperty @name = N'IT_Contacts', @value = @IT_Contacts;
ELSE
      EXEC sys.sp_updateextendedproperty @name = N'IT_Contacts', @value = @IT_Contacts;

IF NOT EXISTS(SELECT 1 FROM sys.extended_properties WHERE class_desc = 'DATABASE' AND [name] = 'MS_Description')
      EXEC sys.sp_addextendedproperty @name = N'MS_Description', @value = @MS_Description;
ELSE
      EXEC sys.sp_updateextendedproperty @name = N'MS_Description', @value = @MS_Description;

IF NOT EXISTS(SELECT 1 FROM sys.extended_properties WHERE class_desc = 'DATABASE' AND [name] = 'Owner')
      EXEC sys.sp_addextendedproperty @name = N'Owner', @value = @Owner;
ELSE
      EXEC sys.sp_updateextendedproperty @name = N'Owner', @value = @Owner;

IF NOT EXISTS(SELECT 1 FROM sys.extended_properties WHERE class_desc = 'DATABASE' AND [name] = 'Reports')
      EXEC sys.sp_addextendedproperty @name = N'Reports', @value = @Reports;
ELSE
      EXEC sys.sp_updateextendedproperty @name = N'Reports', @value = @Reports;
GO
```

Figure 8 - Database Extended Properties SQL Query

4. Repeat steps 1 through 3 for all user databases on the respective server

7.8.3 The GA Tool Method (DBAs Only)

1. In the GA Tool, select the HUB server, AHSSQLD01P
2. Navigate to the Codesets \ Codeset Members tab
3. Select the "DATABASE" codeset
4. Click the Go button
5. Add / Update / Delete database properties as needed
6. Click the Save & Synchronize button



* Server: AHSSQLD01P

*** System Administrator ***

* Codeset: DATABASE

Database Name	Development Server	Test Server	Production Server	Applications	Business Contacts	Exports	Imports	IT_Conta
AIMS_Audit	AHSSQLD02D	AHSSQLD02T	AHSSQLD02P	LANDesk Passw...	Shawn.Potter@v...			Matthew.S
AIMS_Config	AHSSQLD02D	AHSSQLD02T	AHSSQLD02P	LANDesk Passw...	Shawn.Potter@v...			Matthew.S
AIMS_DSR	AHSSQLD02D	AHSSQLD02T	AHSSQLD02P	LANDesk Passw...	Shawn.Potter@v...			Matthew.S
AIMS_GE	AHSSQLD02D	AHSSQLD02T	AHSSQLD02P	LANDesk Passw...	Shawn.Potter@v...			Matthew.S
AIMS_Map	AHSSQLD02D	AHSSQLD02T	AHSSQLD02P	LANDesk Passw...	Shawn.Potter@v...			Matthew.S
Ancestry	AHSSQLD02D	AHSSQLD02T	AHSSQLD02P	Ancestry Births a...	Cynthia.Hooley@...	Birth Records (to ...		Matthew.S
Ancestry_PROD	AHSSQLD02D	AHSSQLD02T		Ancestry Births a...	Cynthia.Hooley@...	Birth Records (to ...		Matthew.S
appts32v10dat		SQLV1-TEST	SQLV1-PROD	Appointments Pro	Donna.Bister@v...			Matthew.S
appts32v10dattut		SQLV1-TEST		Appointments Pro	Donna.Bister@v...			Matthew.S
BusinessObjects...	AHSSQLD02D	AHSSQLD02T	AHSSQLD02P	Business Objects...	AHS.DCFOCSOp...			Craig.Bens
BusinessObjects...	AHSSQLD02D	AHSSQLD02T	AHSSQLD02P	Business Objects...	AHS.DCFOCSOp...			Craig.Bens
CAVU		SQLV1-TEST	SQLV1-PROD	Medical Practice ...	Karen.LaFond@...			Matthew.S
CAVU_Documen...		SQLV1-TEST	SQLV1-PROD	Medical Practice ...	Karen.LaFond@...			Matthew.S
CAVU_Documen...		SQLV1-TEST		Medical Practice ...	Karen.LaFond@...			Matthew.S
CAVU_PROD		SQLV1-TEST		Medical Practice ...	Karen.LaFond@...			Matthew.S
CAVU_UPGRADE		SQLV1-TEST		Medical Practice ...	Karen.LaFond@...			Matthew.S
CAWeb		SQLV1-TEST	SQLV1-PROD	Corrective Action	Sherry.French@v			Matthew.S

Logged-On User: AHS\craig.benson   Record Count: 160   Procedure Time: 0 seconds

Figure 9 - GA Tool Codeset Members Tab

7.9 Secret Server SQL Password Management Procedure

Secret Server is to be used to maintain all passwords associated with AHS SQL Server accounts. To gain access to Secret Server for this purpose, you must be approved by the Data Services Director and a Secret Server account must be created for you by the DII Server Team.

There are 24 Secret Server "Secret" types, of which **only the following 3** are to be used for AHS SQL Server account passwords:

7. *** NEW * Active Directory Account** (for SQL Server service accounts, e.g. SSDS enging, SQL Agent, SSRS engine, SSAS engine, SSIS engine)
8. *** NEW * SQL Server Account** (for all SQL logins, e.g. the "sa" account, etc.)
9. *** NEW * Windows Account** (for local, non-domain Windows accounts--very rare!)

NOTE: Currently, there exist SQL secrets that are of other types than the 3 listed above. This is a known issue that will be addressed over time. All new secrets must employ one of the 3 types listed above.

To maintain a SQL account password in Secret Server, perform the following steps:

1. Log in to the Secret Server at the following URL:

https://secret/SECRET/Login.aspx?ReturnUrl=%2fsecret%2fDefault.aspx

2. Search for the secret. Click the "Browse" tab and then click the "SQL" folder. All the SQL secrets will appear to the right of the Search/Browse panel.

   NOTE: All 3 types of SQL secrets are to be saved in the "SQL" folder!

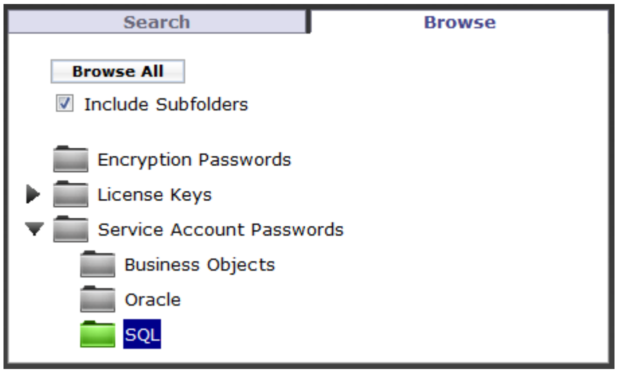
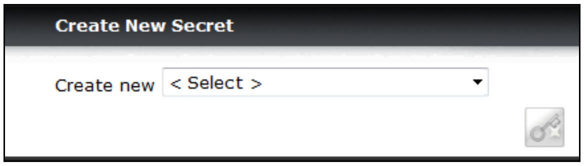


Figure 10 - Secret Browse Tab

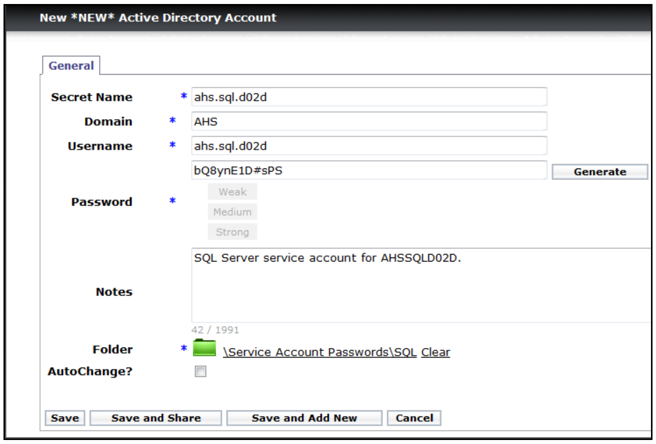
3. If the SQL secret doesn't exist, create the appropriate type. Click the "Create new" combo box in the right corner and select the appropriate secret type (one of the three allowed for SQL).


Create New Secret

Create new: < Select >

Figure 11 - "Create new" Combo Box

   a. For a "*** NEW * Active Directory Account**", complete the form using the same format as follows:


New *NEW* Active Directory Account

General

Secret Name * ahs.sql.d02d

Domain * AHS

Username * ahs.sql.d02d

Password * bQ8ynE1D#sPS

Notes: SQL Server service account for AHSSQLD02D.

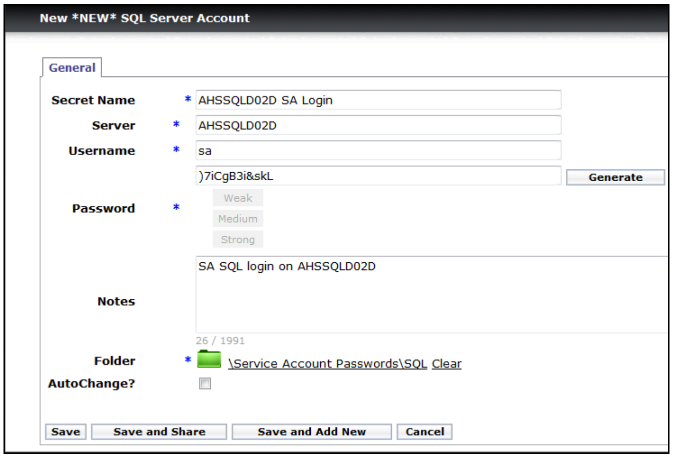
42 / 1991

Folder * \Service Account Passwords\SQL

AutoChange? □

Figure 12 - * NEW * Active Directory Account

b. For a "*** NEW * SQL Server Account**", complete the form using the same format as follows:



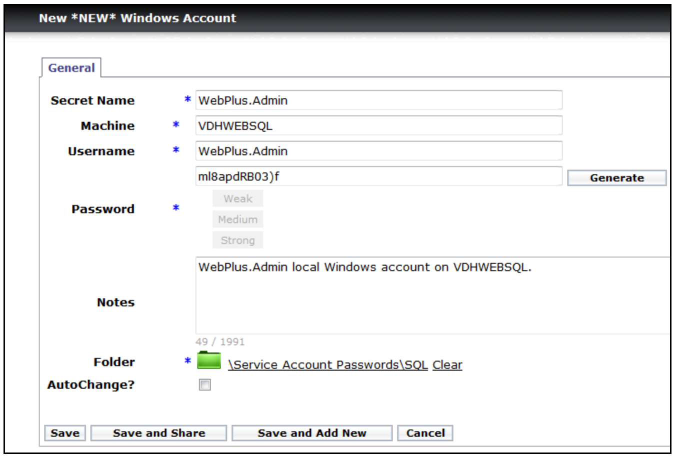
New *NEW* SQL Server Account

General

Secret Name *	AHSSQLD02D SA Login
Server *	AHSSQLD02D
Username *	sa
Password *	)7iCgB3i&skL
Notes	SA SQL login on AHSSQLD02D
	26 / 1991
Folder *	\Service Account Passwords\SQL Clear
AutoChange?	□

Figure 13 - * NEW * SQL Server Account

c. For a "*** NEW * Windows Account**", complete the form using the same format as follows:



New *NEW* Windows Account

General

Secret Name *	WebPlus.Admin
Machine *	VDHWEBSQL
Username *	WebPlus.Admin
Password *	ml8apdRB03)f
Notes	WebPlus.Admin local Windows account on VDHWEBSQL.
	49 / 1991
Folder *	\Service Account Passwords\SQL Clear
AutoChange?	□

Figure 14 - * NEW * Windows Account

4. If the secret already exists, maintain the password according to the screenshots in step 3 above.

   NOTE: If the secret does not use one of the 3 approved types, you must recreate the record using the appropriate secret type and then deactivate the old record. To deactivate a record, put a checkmark next to the secret (in the grid) and select "Deactivate" in the combo box at the bottom of the screen.

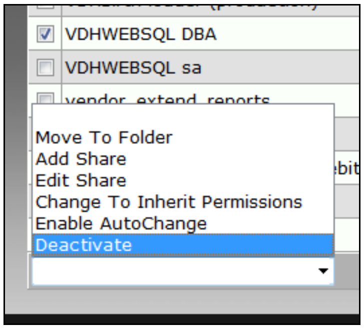


Figure 15 - Deactivate Secret

7.10 Add Data Disk Procedure

DII imposed a 2TB limit on virtual server disk drives. When a designated data drive on a given SQL server is near full, a new disk drive must be added to the server in order to balance database storage. The following steps should be taken so as to ensure consistency across GA servers when new data drives must be added.

1. Determine the drive letter of the new drive to be added. NOTE: Begin with the letter “G” and omit “H” (the state employee Home drive). Each new drive should be incremented thereafter as needed.
2. Determine the size of the new drive based on the size of the database(s) that will reside on it. Allow appropriate room for growth.
3. Enter a LanDesk ticket for the drive creation using the information from step 2. DII will create a new, raw disk.
4. After the new drive is created, bring it online via Disk Management in the Computer Management console
5. Once the disk in online, initiate the disk using the defaults provided by the OS
6. Create a partition on the disk and label it with the appropriate drive letter from step 1 and a name (the name should be Data(N) where N is the number of the data disk).
7. Create a “SQL_Data” folder on the new drive root
8. Create a junction from the D drive that points to the new drive by running the following command on the server *:

```
MKLink /j D:\SQL_Data\SQL_Data G:\SQL_Data
```

9. Deploy, migrate and/or detach/re-attach databases to the new drive as necessary

* NOTE: Each new drive added will necessitate a new, cascaded junction. For example, if there were three new drives added to a server (G, I and J respectfully), the junction structure would look like this:

```
D:\SQL_Data\SQL_Data\SQL_Data\SQL_Data
D:\[root]  \[G junc]\[I junc]\[J junc]
```

7.11 SSAS Data Cube Development Procedure

When users require more than what SSRS reports can deliver, follow these foolproof steps to develop a SSAS data cube (hereinafter referred to as “cube”) through which users can perform unlimited ad hoc queries in an Excel pivot table.

NOTE: It is assumed that the developer has a working knowledge of data warehousing concepts, specifically data de-normalization and star schemas, i.e. the Ralph Kimball model. Developers without this knowledge should be prepared to do a lot of background study before this procedure should be attempted. At any time, Contact the AHS Data Services Director for assistance as needed.

1. **Requirements Phase**

   Requirements, requirements, requirements! Without detailed requirements, the cube development effort will surely falter, if not outright fail. Under no circumstances should the developer proceed unless the following vetted/approved documents are supplied:

   - Data Dictionary (DD): This document details the data source and each data element to be contained in the cube. The DD must be created using the AHS Data Dictionary Template, or any other format that supplies the same level of detail.
   - Use Case (UC) or Business Requirements Document (BRD): This document details the business rules that apply to the cube. For example: date/time granularity, record age, filtering, applied calculations and/or aggregations, availability, refresh rate, permissions, etc.

2. **Analysis Phase**

   The developer must perform a deep dive into the DD, UC (or BRD) and the associated physical schema in effort to learn ***and document*** the following regarding the source database:

   a. The type of database (OLTP or OLAP)
   b. The schema structure (star vs. snowflake)
   c. The complete parent-to-child hierarchy of all subject data tables
   d. The primary key structure on tables containing subject data elements
   e. The physical vs. logical primary-foreign key constraints (and potential orphans created through badly-enforced logical constraints)

f. The classification and grouping of data elements—which will become facts (measures), and dimensions (measure attributes)

If the developer is lucky, physical primary-foreign key constraints exist in the database. As such, the developer should create one or more database diagrams in the database of the subject tables, as they will come in handy later in the procedure.

NOTE: If the subject tables do not contain primary keys, do not proceed; a cube cannot be developed (and shame on the database developer for building tables without primary keys)!

Figure 16 - Do Not Proceed Without Primary Keys!

3. Star Schema Design Phase

If the subject tables are designed as a star schema, skip to the **Cube Design Phase**. If not, the developer must create a series of views that yield a star schema. Under no circumstances should any schema design be considered other than a star schema, as SSAS relies on it explicitly.

The following diagram illustrates a star schema:

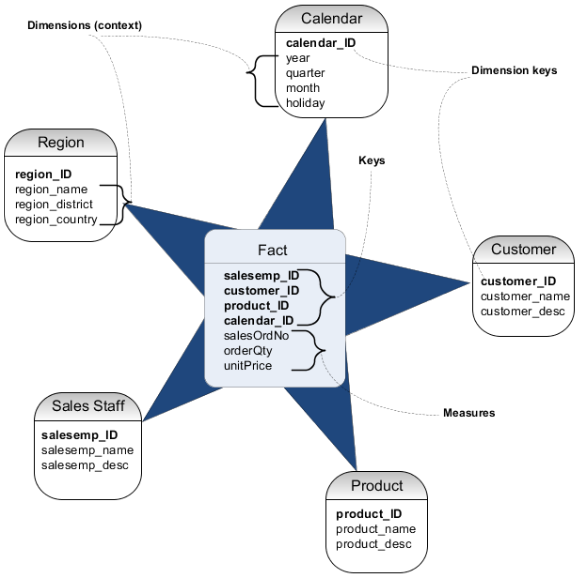


Figure 17 - Star Schema

1. All AHS policies and standards are applicable, e.g. use of AHS templates, extended property creation, etc.
2. The developer must decide where to develop the star schema.
   - If the subject database is a vendor-developed OLTP database, a new, separate "wh[Name]" database must be created on an AHS warehouse server to house the objects to be developed.
   - If the subject database is a vendor-developed OLAP database, a new, separate "wh[Name]" database must be created on the same AHS warehouse server to house the objects to be developed.
   - If the subject database is a state-developed OLTP or OLAP database, a new schema, e.g. "star", must be created in the database to house the objects to be developed.
3. Create a "CodeValueDate" table and "D_Date" view that consumes it in the target database from a pre-existing SSAS data source. Be sure to include a "0" row.
4. If needed based on granularity, create a "CodeValueTime" table and "D_Time" view that consumes it in the target database from a pre-existing SSAS data source. Be sure to include a "0" row.
5. If needed, create one or more "CodeValue[Name]" tables and "D_[Name]" views in the target database for related data that spans multiple selections. For example, "Race." A person can have multiple races, so the CodeValueRace table should contain pivoted records that represent all possible combinations of race. Be sure to include a "0" row.
6. Having classified and grouped all subject data elements, the developer is ready to build "load" views or scripts. Load views or scripts will be used as an ETL source to load "staging" tables of the same structure. The developer must now choose between developing load views or load scripts based on where they need to be created.
   - If the subject database is a vendor-developed OLTP database, load scripts (as opposed to views) will then be developed.
   - If the subject database is a vendor-developed OLAP database, load views (as opposed to scripts) will then be developed. **NOTE: These views will use distributed queries that consume the subject database on the same server.**
   - If the subject database is a state-developed OLTP or OLAP database, load views (as opposed to scripts) will then be developed.

   Each grouping (measure, or fact) of data will have its own load view or script (and subsequent staging table and subsequent fact and dimension views), e.g. Appointment, Birth, Case, Enrollment, Interview, Pregnancy, etc.

NOTE: Name the load views or scripts with an "L_" prefix (for "load").

When designing a load view or script, the following objectives must be met:

a. The load view or script will contain all the data elements necessary that constitute a single fact and its associated dimensions. Join all respective tables, from parent-most to child-most, to ensure all data elements are contained. **NOTE: Most often, LEFT joins are used to join child tables to build a complete data set.**

b. Numeric and date/time data elements will eventually make up a fact view; all other data elements will eventually make up one or more dimension views that relate to the fact.

c. De-normalization is achieved. All code columns must have an associated description column immediately following it. These columns should be aliased as [ColumnName]Code and [ColumnName]Description respectively.

d. The specified granularity and filtering is achieved through WHERE clauses.

e. All specified aggregations and calculations are applied.

f. A special "0" row is included to represent facts for which no associated dimension data is relevant. A UNION ALL clause is used to append the "0" row to the data set.

g. NULLs are eliminated. Use the ISNULL() function to replace numeric NULLs with a zero and to replace textual NULLs with an empty string. This is what SSAS expects.

h. CTEs are leveraged to form the necessary relationships without the overhead of full table joins. A final CTE is used on the full data set and then a SELECT statement references it using the ROW_NUMBER() and OVER() functions so that a unique, derived, surrogate primary key column is added. **NOTE: Title the key column "Row_id".**

i. Group the columns in the following order:

  - Row_id column
  - Primary / foreign key ID columns
  - Bit "Indicator" columns
  - Code / Description columns (by pair)

- Text columns
- Date / Time column IDs (by pair)
- Numeric (measure) columns

j. To ensure high usability, append all BIT column names with an "Indicator" suffix, and implement CASE statements to preset "True", "False" and "Not Indicated" text values.

k. To ensure high usability, assign all columns a "friendly" alias. Abbreviations are eliminated. Acronyms that are not universally known are spelled out. Remember—no spaces in names (SSAS will recognize PascalCase and insert spaces for you).

7. After all load views or scripts are completed and thoroughly tested, the developer is ready to create the staging tables.

   NOTE: If there are less than 20 subject data elements, staging tables and an ETL SSIS package that loads them may not be required. The cube refresh time will dictate whether these objects are necessary or not.

   For each load view or script, create a staging table of the same name, but with an "S_" prefix instead of an "L_" prefix.

   NOTE: It is critical that the exact order and data type of elements in the staging table match that of the view or script. Do not guess—be certain!

8. Next, the developer is ready to develop an ETL SSIS package that uses each "L_" view or script as a source and each "S_" staging table as a destination.

   NOTE: It is critical that staging tables be loaded in a parent-to-child order so that the respective derived surrogate keys within the views or scripts are accurate across the entire data set.

   Once the SSIS package is developed and tested, deploy it to the development SSIS server and run it to propagate the staging tables.

9. Next, the developer is ready to create fact and dimension views from each staging table.

   When designing fact and dimension views, the following objectives must be met:

   a. Fact views contain the following columns in the order specified:

   - Row_id column
   - Date / Time column IDs (by pair)
   - Numeric (measure) columns

b. A fact view has the same name as its staging table, but with an "F_" prefix instead of an "S_" prefix.

c. Dimension views contain the following columns in the order specified:

- Row_id column
- Primary / foreign key ID columns
- Bit "Indicator" columns
- Code / Description columns (by pair)
- Text columns

d. Dimension views should include a grouping CTE against the same staging table in effort to supply a "IsLatest[ViewName]Indicator" column using the ROW_NUMBER() and OVER(PARTITION BY…) functions. This aids the user when applying filters in SSAS to achieve measure specificity.

e. A given fact row must relate to ***one and only one*** dimension row (by its Row_id).

f. A dimension view has the same name as its staging table, but with a "D_" prefix instead of an "S_" prefix, plus a "Details" suffix.

g. Fact and Dimension views must employ a "SELECT TOP 100 PERCENT" statement so that the view can be ordered. These views should be ordered by the "Row_id" column.

After all the fact and dimension views are completed and tested, the developer is ready to develop the cube.

4. Cube Design Phase

1. Create a new SQL Data Tools "Analysis Services Multidimensional and Data Mining" project. Give it the same name as the source database, but without the "wh" prefix.

   All remaining steps will be executed from within the SSAS project file in the Visual Studio IDE.

2. Update the project properties by right-clicking the project object at the very top of the Solution Explorer and selecting the "Properties" option (the Property Pages dialog box will appear). Select "Deployment" in the Configuration Properties list. Select "Deploy All" in the Server Mode field. Enter "AHSSQLA01D" in the Server field. Click the OK button.

3. Create a new data source in the Solution Explorer panel by right-clicking on the Data Sources folder and selecting the "New Data Source…" option (the Data Source Wizard will appear). Connect to the development data source where the star schema resides using your Windows credentials. Give it the same name as the source database, e.g. wh[DatabaseName].ds

4. Create a new data source view in the Solution Explorer panel by right-clicking the Data Source Views folder and selecting the "New Data Source View…" option (the Data Source View Wizard will appear). Use the data source created in the previous step. Select all "D_" and "F_" views. Give it the same name as the source database, but without the "wh" prefix. Upon saving the .dsv file, the <All Tables> diagram will appear.

5. Because views were used as data containers in the source database, the developer will need to build primary keys and relationships in SSAS. For each view on the diagram, select the column that represents the primary key, right-click it and select the "Set Logical Primary Key" option. A key icon will appear to the left of the primary key column name. **NOTE: Use the "Row_id" surrogate key created earlier in the star schema design phase.**

6. To create the view relationships, click and drag the respective columns from the "F_" views to their associated "D_" view columns. Be sure to select the primary key columns on which to build the relationships. **NOTE: If there are multiple facts in the SSAS project, it is recommended to create a new diagram for each fact, as the <All Tables> diagram will quickly become unwieldy.**

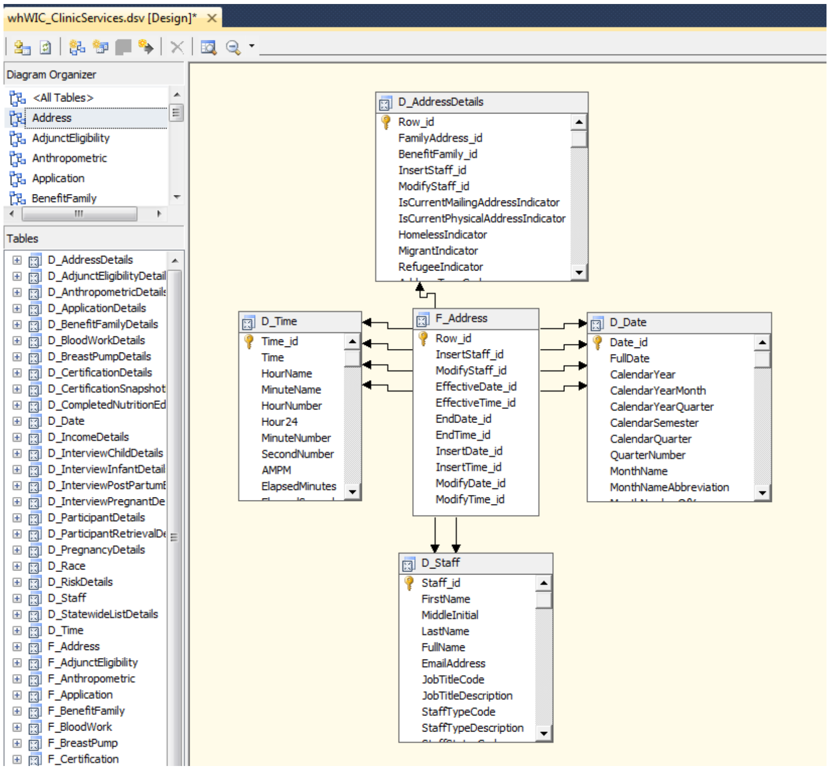


Figure 18 - New Diagram / Relationship Creation Example

7. For each "D_" view in the SSAS project, create a new dimension in the Solution Explorer panel by right-clicking the Dimensions folder and selecting the "New Dimension…" option (the Dimension Wizard will appear). Use the default settings for the creation method and click the Next button. Select the applicable "D_" view from the "Main table" combo-box and click the Next button. Select all attributes and click the Next button. Give it the same name as the "D_" view, but without the "D_" prefix. **NOTE: Attribute hierarchy warnings may appear; these will be addressed next.**

8. For each dimension, create optional attribute hierarchies and relationships to aid cube performance and usability. For example, a date dimension could have a hierarchy of Year > Quarter > Month > Week > Day.

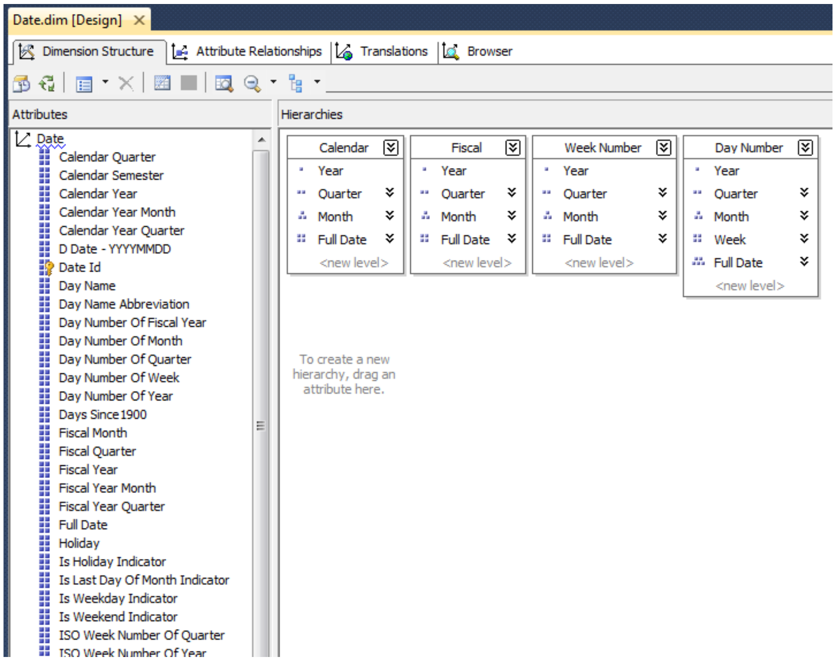


Figure 19 - Attribute Hierarchy Example

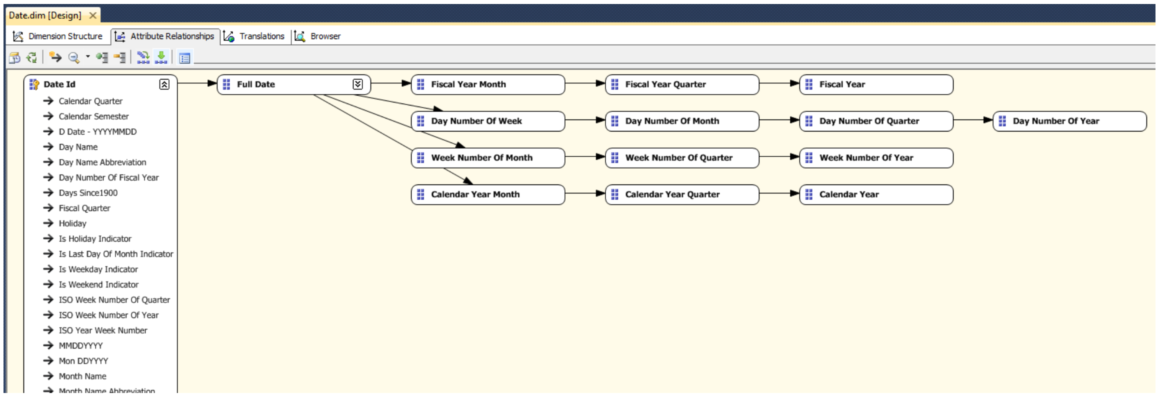


Figure 20 - Attribute Relationship Example

NOTE: Not all dimensions will have attribute hierarchies, as they sometimes don't make sense within the context of their data. As such, the hierarchy warnings will persist—this is OK.

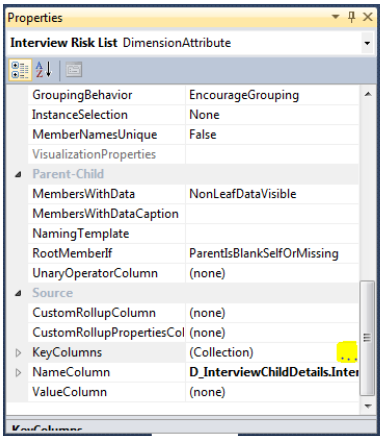
9. Process each dimension (one at a time) by right-clicking on it in the Solution Explorer panel and selecting the "Process…" option (with the first dimension you process, you will be prompted to deploy the SSAS database and you may be prompted to supply impersonation information).

NOTE: Depending on the data in each dimension, you may receive duplicate attribute errors on certain columns. This error is caused by a

lack of uniqueness based on the attribute itself over the entire data set. To fix this behavior, identify the column that contains the duplicates from the error message and then add one or more other columns to its KeyColumns structure (collection) by performing the following:

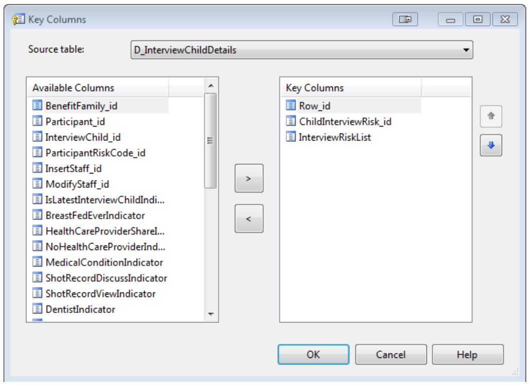
a. Open the affected dimension by double-clicking on it from the Solution Explorer panel.

b. On the Dimension Structure tab, select the affected attribute and reference its properties. Click the “KeyColumns” ellipsis (the Key Columns dialog box will appear).



GroupingBehavior	EncourageGrouping
InstanceSelection	None
MemberNamesUnique	False
VisualizationProperties	
MembersWithData	NonLeafDataVisible
MembersWithDataCaption	
NamingTemplate	
RootMemberIf	ParentIsBlankSelfOrMissing
UnaryOperatorColumn	(none)
CustomRollupColumn	(none)
CustomRollupPropertiesCol	(none)
KeyColumns	(Collection) ...
NameColumn	D_InterviewChildDetails.Inte
ValueColumn	(none)

Figure 21 - KeyColumns Attribute Property



Source table: D_InterviewChildDetails

Available Columns:
BenefitFamily_id
Participant_id
InterviewChild_id
ParticipantRiskCode_id
InsertStaff_id
ModifyStaff_id
IsLatestInterviewChildIndi...
BreastFedEverIndicator
HealthCareProviderShareI...
NoHealthCareProviderInd...
MedicalConditionIndicator
ShotRecordDiscussIndicator
ShotRecordViewIndicator
DentistIndicator

Key Columns:
Row_id
ChildInterviewRisk_id
InterviewRiskList

Figure 22 - Key Columns Dialog Box

c. Add the necessary ID columns (before the attribute itself) that will ensure uniqueness. Click the OK button.

d. Update the NameColumn property by clicking on its ellipsis and selecting the name of the applicable attribute that was receiving the duplicate error.

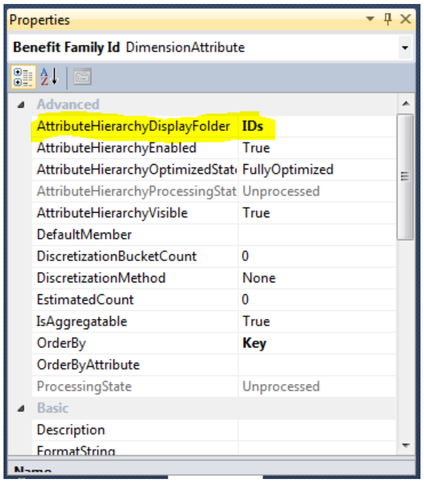
e. Reprocess the dimension; repeat these sub-steps to resolve ***all*** duplicate attribute errors as they are incurred.

10. Add usability to dimensions by grouping attributes into folders. For each dimension in the SSAS project, perform the following from the dimension designer, “AttributeHierarchyDisplayFolder” property:

    a. Assign an “IDs” folder to all attributes with an “_id” suffix.

    b. Assign an “Indicators” folder to all attributes with an “Indicators” suffix.

    c. Assign a “Codes & Descriptions” folder to all attributes with a “Code” or “Description” suffix.



Properties

Benefit Family Id DimensionAttribute

Advanced

AttributeHierarchyDisplayFolder	**IDs**
AttributeHierarchyEnabled	True
AttributeHierarchyOptimizedStat	FullyOptimized
AttributeHierarchyProcessingStat	Unprocessed
AttributeHierarchyVisible	True
DefaultMember	
DiscretizationBucketCount	0
DiscretizationMethod	None
EstimatedCount	0
IsAggregatable	True
OrderBy	**Key**
OrderByAttribute	
ProcessingState	Unprocessed

Basic

Description	
FormatString	

Figure 23 - AttributeHierarchyDisplyFolder Property

11. Determine how many cubes to build. For performance reasons, it’s best not to have too many facts in any given cube—generally, no more than five facts. This poses no problem for users, as they can bring data together from multiple cubes in Excel with ease. As a rule of thumb, group facts together in cubes based on their data classification, for example facts could be grouped / classified by Demographics, Medical, Cases, Appointments, etc.

    For each cube to be developed, perform the following:

    a. Right-click on the Cubes folder in the Solution Explorer panel and select the “New Cube…” option (the Cube Wizard will appear). Use the default settings for the creation method and click the Next button. Select the applicable measure group tables (facts) and click the Next button. Click the Next button. Ensure all related dimensions are selected and click the Next button. Assign a meaningful cube name and click the Finish button (the cube designer will display).

b. For usability, remove all instances of the "F_" and "D_" prefixes in the Measures and Dimensions panels. Be sure to expand each measure to look for prefixes.

c. Process the cube by right-clicking on it in the Solution Explorer panel and select the "Process…" option (with the first cube you process, you will be prompted to deploy the SSAS database and you may be prompted to supply impersonation information).

12. Once all cubes are developed, perform a full deployment of the SSAS project by right-clicking on the project and selecting the "Deploy" option (you may be prompted to supply impersonation information).

13. The developer is now ready to affix permissions. From SSMS, connect to the AHSSQLA01D Analysis Services instance. Expand Databases, [Your SSAS_DatabaseName] database and right-click the "Roles" folder and select the "New Role…" option (the Create Role dialog box will appear). On the General tab, assign a "Browser" role name. On the Membership tab, add the applicable "SQL_SSAS_AHSSQLA01D_[SSAS_Database]" group. On the Cubes tab, select the Access of "Read" and the Local Cube/Drillthrough of "Drillthrough" for each cube. Click the OK button. The cubes are now available for access.

Attachment 7

IRB Approval

Section 1-5-7

Agency of Human Services
280 State Drive
Waterbury, VT 05671-1000
www.humanservices.vermont.gov

[phone] 802-241-0440

AHS Health Care Operations,
Compliance, and Improvement

Date: August 15, 2017

Peggy Brozicevic
VT Department of Health
Division of Health Surveillance
108 Cherry Street
Burlington,VT 05402

Subject: AHS IRB FWA# 00000759
AHS IRB IRB# 00001538

Dear Peggy,

I am writing in response to your revised modifications to the March of Dimes Study (AHS IRB #s AHS IRB FWA# 00000759 and AHS IRB IRB# 00001538). As of August 3, 2017, both the primary and secondary reviewers feel that you have adequately responded to the conditions set forth by the Committee's initial review and you have AHS IRB final approval to conduct your study.

If you have any questions, please contact me directly via email or by calling 802-241-0440.

Sincerely,

Shawn E. Skaflestad, Ph.D.
Chair, AHS IRB

Please note that IRB approval does not supersede state law, as such it will up to the individual departments involved in your study to assure that the access that your team requests meets all applicable Vermont state law and practices.