Memorandum of Understanding  
between

Veterans Health Administration   
and

VA Office of Information and Technology

Authorizing the DSS DataBridge Interface

## PURPOSE

The purpose of this Memorandum of Understanding (MOU), between the Veterans Health Administration (VHA) and the Department of Veterans Affairs (VA) Office of Information and Technology (OI&T), is to concur on a risk-based decision to deploy and maintain the DataBridge Interface acquired from the vendor Decision Support Systems (DSS), under the direction of the Under Secretary for Health (10). This MOU permits implementation and maintenance of DataBridge on production Veterans Health Information Systems and Technology Architecture (VistA) systems as a Class II exemption. DataBridge is acquired, implemented and maintained by the Veterans Integrated Service Networks (VISNs) under an acquisition and implementation process established by the Deputy Under Secretary for Health for Operations and Management.[[1]](#footnote-1)

This MOU succeeds the MOU that initially authorized implementation of DataBridge, signed into effect July 7, 2010.[[2]](#footnote-2)

The signing of this MOU authorizes implementation and maintenance of DataBridge on VistA systems, by request of a VISN to its OI&T Region, subject to the listed Risks and Mitigations and other conditions specified herein.

## BACKGROUND

A Clinical Information System, Anesthesia Record Keeper and Analytics system, known as CIS-ARK and Analytics, is a VISN-wide system. Its use supports delivery of critical care to Veterans in Intensive Care Units (ICUs), Operating Rooms (ORs), Post-Anesthesia Care Units (PACUs) and other care settings.

Each VISN acquires, implements and maintains DataBridge as a component of its CIS-ARK and Analytics system. In addition, coordination among the VISNs is provided by the Office of Informatics and Analytics (OIA), and together are known as the CIS-ARK Program for the purposes of this MOU.

All VISNs have acquired, or are in acquisition for, CIS-ARK and Analytics systems. Two thirds of the VISNs, and more than half of all facilities, have DataBridge implemented and in maintenance.

DataBridge is a software component of a CIS-ARK Analytics system. It is installed as part of each VistA system of a VISN, and transfers data in both directions between the VistA systems and the CIS and ARK components, using Application Programming Interfaces (APIs) and Health Level-7 (HL7) messaging. DataBridge also transfers data in one direction from VistA to Analytics, using file transfer.

DataBridge is provided under contract by DSS to the VISNs. DSS releases DataBridge in versions, which have been tested by DSS, by OI&T and by the VISNs. Testing assures non-harm to VistA, and reliable transfer of data between VistA and the CIS-ARK systems, and from VistA to Analytics. For initial implementation of a CIS-ARK and Analytics systems, a VISN requests installation of DataBridge first on VistA test systems, and then on production VistA systems. For maintenance, a VISN follows the same process for each released version as performed for initial implementation. During operation and use of DataBridge, Biomedical Engineering, OI&T and DSS perform monitoring, support and service restoration.

The VISNs and CIS-ARK program direct and oversee change management for DataBridge versions.

## SCOPE

This MOU covers implementation, maintenance and support of DataBridge for transfer of data between VistA and the CIS and ARK components; and for transfer of data from VistA to Analytics. The scope of this MOU does not extend to use of DataBridge by systems other than CIS-ARK and Analytics.

## Risks and Mitigations

The following risks and corresponding mitigations have been identified by experience of the VISNs, of the CIS-ARK and Analytics program, and of OI&T with implementation and maintenance of DataBridge.

* 1. Risk: Changes to VistA. If changes are made to VistA, without prior notification and specification of the changes to enable prior testing of DataBridge with VistA, then capability for clinicians to provide and document care with CIS and ARK systems will be compromised.

***Mitigation:*** OI&T is to notify the CIS-ARK Program of planned changes to VistA, of technical specifications of the changes, of schedule for the changes, and of pre-release test versions of the changes, as needed for effective testing of DataBridge. In the event that testing identifies defects resulting from the changes, the vendors of DataBridge and of any CIS and ARK systems with the defects will implement, test and deliver fixes to the defects; and OI&T will manage back-out and re-deployment of the VistA changes to mitigate the defects during the time period of resolving the defects.

* 1. Risk: Changes to DataBridge. If changes are made to DataBridge, without testing and without planning for installation of new versions, then capability for clinicians to provide and document care with CIS and ARK systems will be compromised.

***Mitigation:*** The VISNs and the CIS-ARK Program are to specify and schedule version updates to DataBridge, in a change management process; test the versions with CIS and ARK systems of all vendors on a test VistA operated by OI&T prior to release; release the versions for installation on VistA systems of facilities of the VISNs. VISNs are to perform installation of the released versions on each VistA system, using best practices for testing on VistA test systems, then on VistA production systems with test data.

* 1. Responsible Organizations for Monitoring and Support. If organizational responsibility is not assigned as needed to perform all activities of monitoring and support to meet service levels, then the activities will not be performed reliably, and availability of CIS and ARK for clinical use will be compromised.  
     Mitigation: VISNs, Facilities, with responsible organizations (Biomedical Engineering, Clinical Application Coordinators (CACs), Clinical Informatics, Regional COTS Teams, VistA Applications Teams, and other OI&T organizations), are to plan and assign organizational responsibility among VHA and VA organizations and with DSS, as needed to perform all activities of monitoring and support; and assure performance of the responsibilities by the organizations. Responsibilities for monitoring and support among organizations will vary across OI&T Regions, and across VHA Regions, VISNs and Facilities, due to organizational and technical differences. Particular attention is required to assure that authority and relationships enable all parties to be effective in performing their roles and responsibilities.
  2. Risk: Maintaining Service Levels for Data Transfer. If the network does not meet service levels for data transfer between CIS and ARK with VistA, for responsiveness, for availability, and for management of outages and faults, then capability for clinicians to provide and document care with CIS and ARK will be compromised.  
     *Mitigation:* Organizations of VHA and OI&T, (see C, above), are to plan network capacity to meet service levels for responsiveness and for availability; implement, operate and monitor the networks; detect outages, faults and other loss of service; and, manage restoration of networks to full service levels.
  3. Risk: Monitoring for Outage and Restart of DataBridge. If an outage of DataBridge is not detected and DataBridge is not restarted, then transfer of data between DataBridge and CIS and ARK systems will not be performed, and capability for clinicians to provide and document care with CIS and ARK will be compromised.  
     *Mitigation:* OI&T is to provide or permit each VISN through responsible organizations (see C, above), to operate a 24/7/365 service to monitor DataBridge, and to restart DataBridge within 20 minutes.
  4. Risk: Production Data for Fault Analysis. If DSS cannot access production data to perform analysis of faults in data transfer, then it cannot properly identify and remedy defects.  
     *Mitigation:* OI&T is to provide through a Regional COTS Team or VistA Application Team, in collaboration with Biomedical Engineering, Clinical Applications Coordinators, and other organizations, as noted in (see C, above), services that permit DSS access to data as needed to perform fault analysis of defects.
  5. Risk: Permissions for Access to Monitor and Restart. If the responsible organizations are not granted permissions to access networks and VistA systems, as needed to monitor, perform fault analysis and to restart DataBridge (see e and f above), then capability for clinicians to provide and document care with CIS and ARK will be compromised.  
     Mitigation: OI&T is to grant and implement keys to responsible organizations (see C, above) for access as needed to perform support. See Appendix A.
  6. Risk: Non-Uniform Standard Operating Procedures for Monitoring and Restart. If standard operating procedures (SOPs) for monitoring and support are not defined and followed nationally, then organizations responsible for support will not be able to perform their responsibilities, and availability of CIS and ARK for clinical use will be compromised.  
     *Mitigation:* OI&T, Biomedical Engineering, VISNs and the CIS-ARK Program (see C, above) are to define, implement and follow SOPs for managing access to networks and VistA systems for the purposes of monitoring, fault analysis and restart of DataBridge. The SOPs are to specify monitoring and restart (see g, above), procedures for managing data for fault analysis (see f, above), with assignment of organizational roles and responsibilities (see b, above). The SOPs will recognize differences by VHA Region, VISN and Facility, and by OI&T Region.
  7. Risk: PHI Outside Security Perimeter. If DataBridge patient data from VistA to CIS and ARK systems, and to Analytics, is transferred outside the VA security perimeter (accreditation boundary), then the data is not protected as it is in a VistA system.

***Mitigation***: Transfer of data by DataBridge outside of VA security perimeter is implemented by contract with DSS, the CIS and ARK, and Analytics vendors to meet requirements of VA Handbook 6500.

* 1. **Risk: Data Transfer across Non-Secure Lines.** If data is transferred on non-secure wide area networks between VistA with CIS and ARK, and with Analytics, then the data may not be adequately protected.

***Mitigation:*** A VA waiver dated April 30, 2008, enables electronic transmission of PII/PHI among VistA systems within VA wide area network, and is applied to the transfer of data between VistA with CIS and ARK, and Analytics, systems, when those transfers are over wide area networks.

## SECURITY

Both parties agree to work together to mitigate risks to the data when transferred by DataBridge between VistA and the CIS and ARK systems, and from VistA to Analytics; and data stored on CIS, ARK and Analytics. Each party certifies that its respective system is designed, managed, and operated in compliance with all relevant federal laws, regulations, and policies with the exceptions noted herein.

## COMMUNICATION

Frequent, formal communications are essential to ensure the successful management and operation of the DSS DataBridge Interface and CIS/ARK system. The parties agree to maintain open lines of communication between designated staff at both the managerial and technical levels. All communications described herein must be conducted in writing, unless otherwise noted.

VHA and Ol&T agree to designate and provide contact information for technical leads for their respective systems, and to facilitate direct contacts between technical leads to support the management and operation of the interconnection. To safeguard the confidentiality, integrity, and availability of the connected systems and data, the parties agree to provide notice of specific events as indicated below:

1. Security Incidents: Technical staff will notify their designated VHA counterparts by telephone or e-mail within one hour when a security incident(s) is detected, in order for VHA to take steps to determine whether the system has been compromised and to take appropriate security precautions. The system owner will receive formal notification in writing within one business day of the detection of the incident(s).
2. Disasters and Other Contingencies: Technical staff will immediately notify their designated counterparts by telephone or e-mail in the event of a disaster or other contingency that disrupts the normal operation of one or both of the connected systems.
3. Material Change: Material changes are to be reviewed and assessed as modifications to this MOU by the VISNs, the CIS-ARK Program and by OI&T. Examples are: technical changes to VistA that impact DataBridge; technical changes to DataBridge that impact VistA; changes to procedures for management and testing of changes to DataBridge; changes to CIS and ARK systems that impact network loads between those systems and DataBridge operating on VistA systems; or changes to security policies and processes that impact setup and operation of DataBridge and its transfer of data with CIS and ARK systems. If the assessment determines that a modification constitutes a material change, then VHA and OI&T will change this MOU, per section Changes.

## AGREEMENT

The MOU of this document is effective upon the date of signature of the last party signing and will remain in effect for 3 years; or will terminate before 3 years upon agreement of OI&T and VHA.

## CHANGES

This MOU may be modified by mutual agreement of the signing parties, documented as changes, and signed by the signing parties, their designees, or their successors.

## SIGNATORY AUTHORITY

David J. Shulkin

Under Secretary for Health

Veterans Health Administration

Department of Veterans Affairs

Date:

Lavern H. Council

Assistant Secretary for Information and Technology and Chief Information Officer

Department of Veterans Affairs

Date:

Kurt Finke

Director, Office of Healthcare Technology Management

Veterans Health Administration

Department of Veterans Affairs

Date:

**Appendix A, Vendor VistA access for DSS DataBridge Support**

DSS Enterprise Manager is a GUI application to be used to monitor DSIH\* HL7 links. Access Code/Verify Code VISTA sign-on access and the below options and key are needed. Access needs to be granted for each vendor employee with individually identifiable accounts. Sharing of sign-on credentials is not allowed.

* Primary Menu: XMUSER (to be given as the Primary Menu)
* Secondary Menu: VEJDWPB CORE RPCS
* Security Key: VEJDENM MANAGER
* No additional VISTA Menu Options or Keys are needed for DSS DataBridge.
* No vendor VISTA programmer level (VISTA elevated privileges) access will be allowed.

Vendor Server Access. Vendor server access will be granted based on Windows Security Groups per the requirements stated in the terms of the contract. Access needs to be granted for each vendor employee with individually identifiable accounts. Sharing of sign-on credentials is not allowed.

1. Memorandum from the Deputy Under Secretary for Health for Operations and Management (10N), September 24, 2008, "VISN-Wide Acquisition and Implementation Process for Intensive Care Unit and Anesthesia Record Keeping Clinical Information Systems and Analytics System." [Click here.](https://vaww.portal.va.gov/sites/ARK/programsummary/basicMemos/Documents/memo_CIS-ARK_Implementation_Process_sep08.pdf) [↑](#footnote-ref-1)
2. Memorandum of Understanding Between The Veterans Health Administration And The Department of Veterans Affairs Office of Information and Technology [Authorizing the DSS DataBridge Interface], July 7, 2010. [Click here.](https://vaww.portal.va.gov/sites/ARK/programsummary/basicMemos/Documents/memo_Databridge_Shared_Risk_MOU_7July2010.pdf) [↑](#footnote-ref-2)