Medicaid Management Information System Replacement (MMISR) Project

Deliverable –

SI21 – Data Services (DS) Module Integration – Increment 2 – Update System Integration Platform (SIP) Configuration Designs

HSD Deliverable Owner: Paula Morgan

Contractor Deliverable Owner: Spruce-KPMG Team

Configuration Number: v2.0

Date: September 19, 2022

Table of Contents

Table of Tables

Table of Figures

1.0 Introduction

The New Mexico (NM) Human Services Department (HSD) has adopted the Health and Human Services (HHS) 2020 vision, a transformational, enterprise-wide approach to the HHS business. HHS2020 will move service delivery from a program-centric approach to a citizen-centric approach. In addition, HSD will migrate away from program and technology silos into an integrated, flexible framework that supports service delivery and stakeholder interaction across HHS programs and organizations. HHS2020 is technology-enabled, but includes rethinking organizational design, redesigning and streamlining business processes, and reducing barriers between organizations within the HHS enterprise. Please see Section 1: Introduction in Project Management Plan (PMO1) for a detailed Medicaid Management Information System Replacement (MMISR) project overview (link provided in Appendix C Section 13.3 of this document).

The NM HSD selected the Spruce-KPMG Team as its MMISR System Integrator (SI) to assess, evaluate, design, plan, and develop the integration platform for an information system to coordinate functions and operations between multiple agency systems and service modules.

2.0 Purpose

As part of the Spruce-KPMG Team Statement of Work (SOW), the Spruce-KPMG Team is providing Deliverable Number 21: Data Services (DS) Module Integration (SI21). The purpose of this deliverable for SI21 – Increment 2 – Update System Integration Platform (SIP) Configuration Designs is to update the SIP configuration designs relative to the integration of the DS Module, as well as complete a test plan for testing the SIP, integration, and performance related to the DS Module, as applicable. The intended audience for this document includes the HSD-designated reviewers of SI21 – DS Module Integration as defined in the Resource Needs spreadsheet (link provided in Appendix C Section 13.3 of this document).

3.0 Goal

The goal of the SI21 – Increment 2 – Update SIP Configuration Designs is to layout the designs of the SIP design configurations and the updates that will be made. This includes designing a backlog for SIP configuration changes and developing a test plan for SIP, integration, and performance testing, as applicable.

4.0 Scope

Based on the agreed-upon SOW, the scope of SI21 – Increment 2 – Update SIP Configuration Designs includes:

Table 1 – SOW Tasks

Task Item	Sub Tasks	Description
3.0 Update SIP Configuration Designs (Increment 2)		
	3.1	Phase 1 - Contractor will create a design backlog for SIP configuration changes across the scope areas identified in the Module Orientation and Discovery

Task Item	Sub Tasks	Description
		phase. Contractor will update designs aligned with the module integration phase.
	3.2	Phase 1 - Contractor will develop test plan for SIP testing, integration testing, and performance testing if applicable to align with module integration phase.
4.0 Review and Acceptance of Design Updates by Phase (Increment 2)		
	4.1	Contractor will deliver updated designs for SIP configuration and test plan for review and acceptance by Procuring Agency.

5.0 Approach

The SI team's approach for the updating the SIP Configuration Designs is to conduct weekly HSD-DS-SI meetings with the HSD and DS Module teams to socialize the integration points and understand the gaps. The SI team documented the gaps in the meeting minutes and created JIRA modification proposals and addressed the resolution in the JIRA tickets for each type of integration – Security and ICAM integration, Shared Services integration, Data integration which includes transactional data, reference data, master data and test data, and Service and Infrastructure Monitoring. Once all JIRA modification proposals were documented, these were reviewed in detail against the Requirements. Once these design specifications were approved by HSD, these were added to the design backlog.

6.0 Roles and Responsibilities

The table below lists the roles and responsibilities specific to the creation and review of this deliverable.

Table 2 – Roles and Responsibilities – Deliverable Development

Role	Responsibilities
SI Deliverable Team	• Conduct deliverable kickoff (in email form) • Develop Deliverable Expectations Document (DED) and obtain approval following the established review process • Perform the scope of work defined in the contract for the deliverable • Develop deliverable and coordinate with HSD throughout the established review process to address reviewer feedback
Deliverable Review Team	• Participate in knowledge transfer (KT) and other working sessions • Provide documentation and related information to SI Deliverable Team • Review deliverable in alignment with Amendment 1 and applicable decisions, the approved requirements in JAMA (link found in Appendix C Section 13.3), and the Deliverable Template
Enterprise Project Management Office (EPMO)	• Review the deliverable against the "Deliverable Standards Acceptance Criteria" checklist and provide comments, as applicable
Independent Verification and Validation (IV&V)	• Review deliverable in alignment with Amendment 1 and applicable decisions, the approved requirements in JAMA (link found in Appendix C Section 13.3), and the Deliverable Template

Role	Responsibilities
HSD Contract Manager	• Provide notification to the SI Deliverable Team of rejection or approval of the deliverable • Coordinate the completion of the Deliverable Approval Signature Form
HSD Project Manager (PM)	• Coordinate Subject Matter Expert (SME) reviews of the deliverable • Coordinate the submission and tracking of comments provided by reviewers on the deliverable • Communicate status of the deliverable to the HSD Contract Manager, SI Deliverable Team, Deliverable Review Team, EPMO, and IV&V

The table below lists the roles and responsibilities specific to the creation of and testing performed on the data provided to the DS Module Contractor.

Table 3 – Roles and Responsibilities - Test Data

Role	Responsibilities
SI Developer	• Generate comma-separated values (CSV) files from the ingested data based on approved layouts for unit testing • Resolve defects logged in the SI JIRA project by the SI Testing Team or the DS Module Contractor
SI Data Engineer	• Submit queries to HSD for production data files • Create the accompanying configuration file for each CSV file to be ingested by Deidentification of User Data for the deidentification tool • Access the de-identification tool to de-identify requested data • Coordinate with HSD for the de-identification tool's "Source System" and "Common Value Lists" for de-identification of data • Oversee ingestion process and load de-identified data and production files to the SIP
SI Test Engineer	• During Development, System Integration Testing (SIT), and Performance Testing phases, use a combination of python scripts, Alteryx workflows, structured query language (SQL) queries, and functional tests to perform manual and automatic integration testing • During Development, SIT, Performance Testing, and User Acceptance Testing (UAT) phases, compare data found in the Staging tables, Load Ready Tables and system-generated CSV files to the approved layouts, configurations present in this document, and NM KRIS Mapping Document (link provided in Appendix C Section 13.3 of this document) • During Development and Performance Testing phases, log Bug and Modification Proposal tickets in the SI JIRA project for any irregularities found during internal integration and performance testing

Role	Responsibilities
	• During SIT and UAT phases, liaise with HSD and the DS Module Contractor regarding any Bug or Modification Proposal tickets filed in the SI JIRA project • As needed through Development, Performance Testing, SIT, and UAT phases, conduct re-testing of issues to confirm resolution of reported issues • During SIT and UAT phases, report status and analysis of issues as requested during Daily and/or Weekly meetings with the DS Module Contractor • During SIT and UAT phases, present key blocking issues during Issue Review Meetings and provide insight into Modification Proposal tickets during Technical Change Review Board (TCRB) meetings, as applicable • During the SIT phase, review and triage Bugs logged by the DS Module Contractor • During the UAT phase, review and triage Bugs logged by HSD, and after initial triage by the DS Module Contractor, determined as caused by the SIP • During SIT and UAT phases, coordinate with the DS Module Contractor and HSD regarding issues reported by the DS Module Contractor or HSD
NM HSD	• Coordinate resolution of defects related to the issues raised by the Spruce-KPMG Team and/or DS Module Contractor attributed to source system data
Data Stewards	• Support analysis of any source system-related issues
DS Module Contractor	• Conduct initial triage of delivered data by comparing output against the integration design documents (IDDs), file lists, and approved requirements in JAMA (link found in Appendix C Section 13.3) for DS Module integration • Log suspected SIP Bugs in the SI JIRA project • Retest Bugs addressed by the SI Developers that were previously logged or reported by the DS Module Contractor

7.0 Risk Mitigation Methods

To help mitigate risks throughout the deliverable development process, the Spruce-KPMG Team maintained consistent and open communication with the DS Module Contractor, HSD PM, and other HSD key resources as defined in the PMO7 - Risk Management Plan (link provided in Appendix C Section 13.3 of this document). Any issues were immediately escalated to help ensure that completion of the deliverable would remain on schedule. The Spruce-KPMG Team also held regular meetings with the DS Module Contractor and HSD to track the progress of completing work on the deliverable and identify any challenges and cross-workstream dependencies.

8.0 Assumptions/Constraints/Risks

This section documents any assumptions made, constraints considered, and risks identified that affected the development of the deliverable.

8.1 Assumptions

- The Spruce-KPMG Team assumes that any change in future DS module contractor will not change the file layout format already agreed upon with HSD and the future DS module contractor will use the HSD agreed-upon format.
- The Spruce-KPMG Team assumes that incremental files are generated and provided by the source system vendor or module contractor. If such incremental files are not available, the Spruce-KPMG Team assumes that any periodic load will be a full load that overwrites the existing Staging data store.
- The Spruce-KPMG Team assumes that Staging zip files received will be archived per the HSD backup and archiving policy; however, data in Staging will be overwritten by future loads/updates.
- The Spruce-KPMG Team assumes that Omnicaid and Automated System Program and Eligibility Network (ASPEN) data extraction selection criteria to extract source data are identified and validated by HSD.
- The Spruce-KPMG Team assumes that business data quality validations (for example: max claim amount or drug price cap amount) will not be implemented within the extract, transfer, load (ETL) process; instead, the Spruce-KPMG Team will implement only data quality rules for format, structure, and data types.
- The Spruce-KPMG Team assumes that this document only addresses batch file-based data exchanges and not service-oriented architecture (SOA)-based exchanges.
- The Spruce-KPMG Team assumes that in the future, Omnicaid may be replaced with new modules and will provide the data to the DS Module through the SIP managed file transfer (MFT) platform.
- The Spruce-KPMG Team assumes that HHS2020 Integration Partners will use the SIP MFT solution to send the pass-through files to DS.
- The To-Be MFT process design is based on MFT leading practices and standards. It is subject to change based the NM adaption of standards.
- The Spruce-KPMG Team assumes that the source module/integration partner will send a notification via an additional trigger file once the data and control files have been submitted to SIP MFT. Control files include the record total for batch files exchanged from one system to another to validate all records are received or sent. A trigger file defines the list of files exchanged in a batch data transfer between one system to another to validate all files were received or sent.
- The Spruce-KPMG Team assumes the NM HSD Testing Team is responsible for conducting UAT as applicable, and the SI will support as needed.
- The Spruce-KPMG Team assumes DS Module SIT and HSD UAT will follow the same defect logging and triage process used during the previous data deliveries.
- The Spruce-KPMG (SI) Team assumes a user’s access in NM HSD Department of Information Technology (DoIT) Azure Active Directory and Data Services (DS) Module Active Directory (AD) are in sync.

- The Spruce-KPMG (SI) Team assumes Single Sign-On (SSO) will be only initiated through a Service Provider (SP). Service Provider in this context is the MMISR module web/mobile application to which the user is trying to gain access.
- The Spruce-KPMG Team understands and agrees to the decision regarding Federal Tax Information (FTI) data usage for SI, per decision #425 on 8/23/22 that states: "*It was confirmed that ASPEN and Omnicaid systems do not contain FTI data. This confirmation was needed by the System Integrator in order to ensure they remain in compliance with their contract. Due to this confirmation, the SI does not have access to FTI data via Omnicaid and ASPEN data handling. There was a question raised that there may be access to FTI via ASPEN as the ISD team accesses FTI but it was confirmed that a limited number of ISD (Income Support Division) resources access the FTI via a separate system (IEVS: Income Eligibility Verification System), not via ASPEN data or system. Future considerations for FTI data will come when CCSC/Consolidated Customer Service Center and CSED/Child Support systems are integrated into the SIP/System Integration Platform*". This decision is referenced in Appendix C Section 13.3.

8.2 Constraints

- The Spruce-KPMG Team will ingest incremental files from Omnicaid for Claims data and ingest incremental query extract from ASPEN. All other data sources are received as a full reload.
- The Spruce-KPMG Team will only be passing data through to the DS Module Contractor. Any defects within the data which originate from the source cannot be fixed by the SI.

8.3 Risks

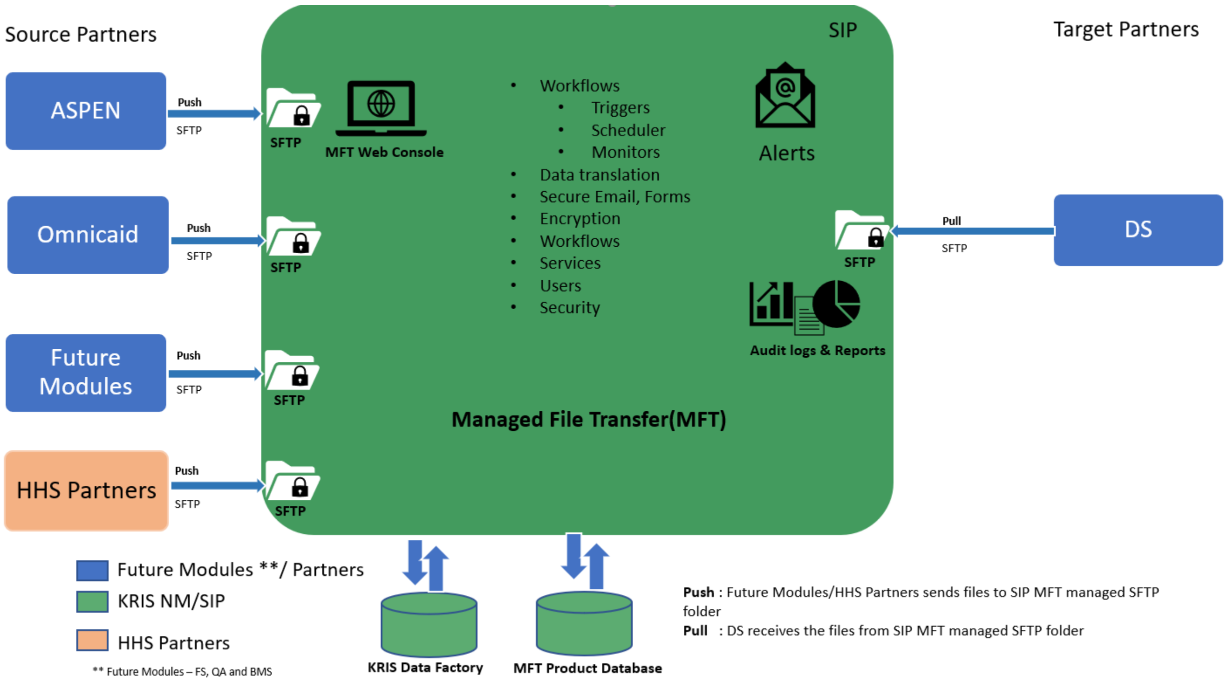
- Data sources and data files planned by the SI in 2023 and 2024 are requested by data-consuming modules (DS) sooner in 2022 as pass-through files. These additional requirements will need to be factored into the SI's project schedule to avoid delays in data delivery. To help mitigate this risk, the contents of pass-through files will not be altered by the SI.
- Data delivery of the full load of Omnicaid data and ASPEN data within the required service level agreements (SLAs) could be delayed if infrastructure capacity needs are not met in a timely manner.
- Data delivery of the full load of Omnicaid data and ASPEN data within the required SLAs could be delayed if there are data quality issues in the source system's data that need to be fixed in the source system, or if there is no clear interim resolution from HSD that could be implemented by the system migration repository (SMR) solution. Any Critical issues, Major issues, and Minor issues will be resolved within HSD-specified timeline guidance to meet the SLAs.
- If changes in layouts of data from source or consuming systems are not communicated to the SI before development begins, it could cause delays in data delivery.

9.0 Integration Services SIP Configuration Design Backlog

The Spruce-KPMG Team will implement a file-based integration to exchange the data from Omnicaid, ASPEN, and HHS2020 Integration Partners to the DS Module using the SIP MFT solution. For the early 2023 DS Module data release, file transfers will leverage existing file transfer services available from NM HSD. The following content shows the To-Be Architecture and design leveraging the KPMG Resource Integration Suite – Connected (KRIS-C) solution.

9.1 To-Be MFT-High Level Architecture

The following diagram shows the inbound and outbound file transfer flow from source to target (DS, Omnicaid, ASPEN, and future modules, respectively):



Push : Future Modules/HHS Partners sends files to SIP MFT managed SFTP folder
Pull : DS receives the files from SIP MFT managed SFTP folder

Figure 1 - File Transfer Flows

Following section focuses on To-Be File Integration Design based on the MFT architecture above. To-Be file integrations design components are divided into three (3) categories from SIP:

- Future Modules, Omnicaid, and ASPEN to SIP inbound file interfaces
- SIP to DS outbound file interfaces
- HHS Partners Pass-through file interfaces

9.2 Future Modules, Omnicaid, and ASPEN to SIP Inbound File Interfaces

The Spruce-KPMG Team will implement the inbound interfaces to transfer the full load and incremental load data files from future modules, Omnicaid, and ASPEN to the SIP (KRIS Data Factory) to perform the Data Acquisition phase and generate the DS Module data files with the expected format.

See KRIS Data Integration Factory Mapping Source tab for the full load and incremental load file list from Omnicaid and ASPEN inbound data files to the SIP (link found in Appendix C Section 13.3).

9.3 To-Be Interface Technical Details

9.3.1 Interface Data

The table below provides information about the data file. This includes the filename, file type, data record layout, delimiters, header, trailer, interface frequency, and schedule.

Table 4 - Interface File Information

#	Item	Description
1	Filename and Naming Pattern	Current Omnicaid to SIP inbound file format: See KRIS Data Integration Factory Mapping Source tab (link found in Appendix C Section 13.3). Current SIP to DS Outbound file format: See KRIS Data Integration Factory Mapping Target tab (link found in Appendix C Section 13.3) for Outbound file format list. Note: Omnicaid will not change the file naming standards and will follow as-is naming standards in the future. Also in the future, ASPEN data will load directly to the Amazon Web Service (AWS) staging database without the involvement of MFT.
2	File Type/File Format	CSV, Text (TXT)
3	Record Layout (data elements)	See DS File Layouts (link found in Appendix C Section 13.3) for Omnicaid control, data, and manifest files.
4	Field Delimiter	Encapsulated in double quotes (“”)
5	Record Delimiter	Comma-separated values
6	Include Header	Yes
7	Include Trailer	No
8	Frequency	Weekly

9.4 To-Be Interface Logging Specifications

The file interfaces will use the SIP’s KRIS-C MFT standard of writing the job event executions to logs.

9.5 To-Be Interface Auditing Specifications

The file interfaces will use the SIP default settings of the MFT event, filenames, source, destination, user, start time, and end time. All file job transaction details will be captured and stored into the database to track the update-to-date file transfer details.

9.6 To-Be Interface Operational Report Specifications

The SIP KRIS-C MFT will generate the operational report file for each day's transactions and share with the appropriate parties through email notifications based on allocated schedules.

The following fields will be captured in the operation report:

Table 5 – Operation Report Fields

#	Field Name	Field Type
1	ReportingEntity	String
2	FileInstanceID	Number
3	JobName	String
4	SourcePartner	String
5	TargetPartner	String
6	IntegrationID	String
7	SourcePartnerID	String
8	TargetPartnerID	String
9	FileName	String
10	SourceSubmissionTime	DateTime
11	Status	String

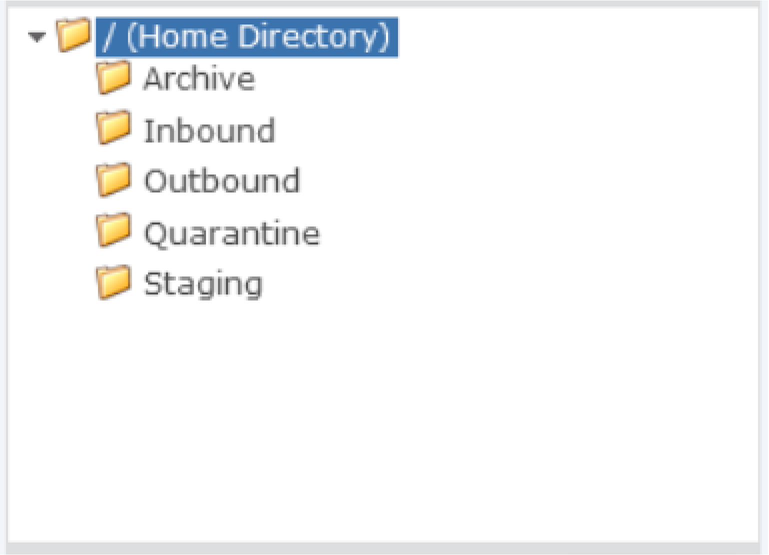
9.7 To-Be Interface Security Specifications

The communication between future modules, Omnicaid, ASPEN, HHS2020 Integration Partners, and the DS Module to the SIP utilizes the SFTP mechanism to send or receive files from the SIP platform, which is hosted in the KRIS-C environment. Partners will connect to the SIP KRIS-C MFT server to upload or download the data, control, acknowledgement, and trigger files.

When connecting to the MFT SFTP server, a username/password and key must be provided before the connection is fully established. If an incorrect username/password and key is received by the SIP MFT server, the server will not accept files for upload or allow download of any files.

9.8 To-Be SFTP Account Directory structure

Future Modules, Omnicaid, ASPEN, HHS2020 Integration Partners, and the DS Module SFTP account users will have a file directory structure of a main folder labeled Home Directory that contains subfolders of Archive, Inbound, Outbound, Quarantine, and Staging as shown in the below diagram in the SIP KRIS-C MFT solution.



/ (Home Directory)
Archive
Inbound
Outbound
Quarantine
Staging

Figure 2 - File Directory Structure Example

- **Archive**: the location of the inbound files after successful file transfer.
- **Inbound**: the location of the files after successful virus scan and where processes on the file will occur.
- **Outbound**: the location of files when they are ready to be transferred. HHS2020 Integration Partners' SFTP account users will have read permission.
- **Quarantine**: the location of files after an unsuccessful virus scan.
- **Staging**: the location where users will upload the files. HHS2020 Integration Partners' SFTP account users will have read/write permissions.

9.9 To-Be Notifications

9.9.1 Error Notification

Notifications for the errors in the process identified by the Interface Processing section (trigger file validation, data file validation error, and late submission) are sent to the submitting partners and Spruce-KPMG Team via email, and an incident is created in ServiceNow.

The following will generate an error email notification and create an incident in ServiceNow:

- Trigger file validation
- Incorrect file names
- Data and control files that are not submitted on scheduled timeframe or not matching with trigger file count
- Missing corresponding data file or control file
- Any System failures

9.9.2 Success Notification

HHS2020 Integration Partners to SIP Inbound files: The notification will be sent to the SIP (Spruce-KPMG Team Data Team) upon successful processing of the inbound data files to the KRIS Data Factory outbound directory.

SIP to DS Outbound files: The notification will be sent to the DS Module upon successful processing of the outbound data files to the DS outbound directory.

Pass-through files: The notification will be sent to the DS Module upon successful processing of the pass-through data files to the DS outbound directory from HHS2020 Integration Partners.

9.10 To-Be Trigger File format

For ASPEN, the SI is working with HSD to establish direct database-to-database connectivity across the SI and Deloitte AWS platforms to extract and load data. As such, there will not be a trigger file concept for ASPEN. There will also not be a trigger file needed for Omnicaid, since the data ingestion is being handled by the SI's data ingestion process.

The concept of a trigger file can be used to support processing control for multiple files within a group as MFT best practice and standards, add critical validations, managing files groups and processing , and deliver the multiple batch files to the downstream modules.

The following is a list of fields included in the trigger file:

Table 6 - Fields included in sample Trigger File

#	Field Name	Description	Field Type
1	SenderName	Source Partner Name/Partner Name	String
2	SenderPartnerID	Source Trading Partner ID	String
3	SubmissionDueDate	Date on which this data should reach the destination as per schedule	Date
4	FileCount	Number of files sent in for SIP	Number
5	DataFileCount	Number of data files sent to SIP	Number
6	ControlFileCount	Number of control files sent to SIP	Number

Example:

SenderName|SenderPartnerID|SubmissionDueDate|FileCount|DataFileCount|ControlFileCount

Omnicaid|SourcePartnerID|085082022|2|1|1

9.11 To-Be Functional and Technical Dependencies

The SIP KRIS-C MFT solution will perform the following functional/technical dependencies:

- For the future, the SIP will ask to provide the integration reference number and partner ID on the file name.
- The SIP will perform the zero-size file validation.
- The SIP will perform the virus scanning on all inbound files.
- The SIP will verify the control data file count sync with trigger file count.
- The SIP MFT solution will notify the source partner if files are missing.

- The SIP MFT solution will notify the source partner if files are not received within the scheduled window.
- The SIP MFT solution will archive the inbound files to re-execute the process in the event of any system errors.
- The Spruce-KPMG Team Operational Team and source partners will be notified of application errors.
- The SIP MFT solution will configure batch jobs based on future schedules.
- The SIP MFT solution will apply the rules related to the file acceptance criteria:
    - The manifest or control file is submitted with the extension ".txt"
    - The data file has the file extension ".csv"
    - The trigger file has the file extension ".txt"
    - File names for data and control/attestation files are correct
- The SIP MFT solution will check the file size minimum and maximum to determine capacity planning.

10.0 DS Module Data Delivery Backlog

10.1 Backlog

The SI has implemented the change requests/module modification proposals approved by HSD. All approved modification proposals are documented and the link is provided in Appendix C Section 13.3 of this document. Modification proposals include the following types of representative changes:

- File layout changes to specific columns for data type or length based on data received
- Legacy column removal for columns that are no longer relevant to the new software-as-a-service (SaaS) solution; for example, legacy MarkLogic internal keys for document model representation
- File layout consolidation for child tables that are combined with the parent table (flattening)
- File layout changes for data sourced from both ASPEN and Omnicaid Client and Managed Care Organization (MCO) domains; HSD recommended to keep the data separate instead of combining data from both systems into one (1) file
- Duplicate record removal based on composite business keys provided for the Omnicaid and ASPEN tables
- Updates to Business Keys (primary and foreign) as defined by the source system and SMEs, which the SI team will translate to the layout
- File format changes to handle special characters
- Record removal for records that have nulls in mandatory columns
- Additional tables to the model, which include ASPEN Living Arrangement data table, Omnicaid Provider MCO Network data table, and ASPEN Application data tables

11.0 DS Integration Test Plan

11.1 Types of Testing

This section describes the testing types specific to the DS Module integration to the SIP and leverages the testing approaches and types (inclusive of SIP testing, integration testing, and performance testing, if applicable) from the approved SI05 Test Management Plan (link provided in Appendix C Section 13.3 of this document). The Spruce-KPMG Testing Team will execute a series of manual and automated tests against the various stages of the SIP. Every test will utilize the mappings, values, and rules defined in the mapping document (link provided in Appendix C Section 13.3 of this document).

11.1.1 SIP Testing

11.1.1.1 Regression Testing

Before each data delivery and bug fix, the Spruce-KPMG Testing Team will load a series of mock source files into the SIP to execute both positive and negative testing. Positive tests will validate the SIP extracted, transformed, and loaded the records in an expected manner across the staging table, load ready table, and DS output files, and validate that the SIP updated the audit table appropriately. Negative tests will include records which trigger the SIP's data quality rules. These include but are not limited to:

No nulls
Uniqueness
Date check
Common format/pattern

11.1.2 System Testing

11.1.2.1 ICAM Testing

The previously submitted SI12A – SaaS Shared Services Designs – Address Standardization and Validation (ASV) and Identity, Credential, and Access Management (ICAM) – Task 5.0 – Shared Services Enablement Test Plan (link provided in Appendix C Section 13.3 of this document) provides an overview of the testing planned for the ICAM Shared Service. However, as a part of the DS Module Integration, the Spruce-KPMG Testing Team will execute a series of tests to validate the DS-specific configurations and user roles elaborated in Section 12.0 of this document. The tests will follow the same approach as those defined in the Shared Services Enablement Test Plan.

11.1.3 Performance Testing

The Spruce-KPMG Testing Team will execute a series of performance tests outlined in SI11 - SaaS Configurations for Enterprise Design – Increment 2 – Task 5.0 – Update Performance Test Plan (link provided in Appendix C Section 13.3 of this document) to validate the SLAs defined for the DS Module. Specifically, the Spruce-KPMG Testing Team will validate that the SIP shall access batch records from the data sources at no less than 100,000 records per minute on one-to-one mappings, and the SIP can generate a set of incremental files within a week's timeframe required for the weekly incremental data delivery to DS in production. The results of these tests will be documented in the future SI20 – Establish

SaaS Production Environment – Task 1.0 – Conduct Performance Testing deliverable (link provided in Appendix C Section 13.3 of this document).

The Spruce-KPMG Testing Team will describe additional stress tests on the SIP as a part of the SMR-specific test plan provided with the future SI19 – SaaS Establish SMR deliverable (link provided in Appendix C Section 13.3 of this document).

11.2 Testing Schedule

This section outlines the testing schedule for the in-scope items being developed and provided with this deliverable. The schedule shows testing milestones for the start and end of SIP integration testing, DS SIT, and UAT. Please refer to the most recent NM MMISR SI Schedule referenced in Appendix C Section 13.3 of this document for the detailed test schedule for SI21 - DS Module Integration.

12.0 Identity Credential and Access Management (ICAM) Integration

(Please note that this section was not included in the approved DED and was added to clarify and address ICAM integration.)

ICAM is a framework of business processes, policies, and technologies that facilitates the management of identities in the form of employees, contractors, vendors, and other state agency users. ICAM is used as an interface between NM MMISR applications and the Department of Information Technology (DoIT) Azure Active Directory (AAD) for providing authentication, authorization, and user access provisioning services for HSD internal users.

The Data Services (DS) Module applications will have two (2) primary areas of integration with ICAM:

- Access Management (AM)
- Identity Management

The DS Module application integration plan is listed in table below:

Table 7 - DS Application Integration Plan

Applications	Access Manager Integration	Identity Manager Integration
Cognos	Yes	Yes
Tableau (Browser Based)	Yes	Yes
Information Governance Catalog (IGC)	Yes	Yes
Structured Query Language (SQL) Developer Client	No	Yes

12.1 Identity Management (IDM)

IDM provides functionalities such as user access request and approval, provisioning/de-provisioning of users and access, and access request fulfillment. The user's access is being facilitated by DoIT Azure Active Directory group mapping. User and access provisioning will either be automated by ICAM using standard connectors or be manually provisioned by emailing the application administrations and assigning the fulfillment task in ICAM.

The following DS Module applications are targeted for IDM integrations:

- Cognos
- Tableau
- IGC
- SQL Developer Client

Note: Provisioning to DS Module applications is managed through DS Module AD group membership.

The DS Module applications will be onboarded by leveraging the Role-Entitlement Onboarding Template referenced in Appendix C Section 13.3.

12.1.1 IDM Use Cases

The ICAM solution offers Identity Governance and Administration capabilities that allow enterprises to manage the identities and access privileges of Organizational Users on a single platform. The following are some of the high-level capabilities provided by the ICAM solution:

- **Delegated Administration**: Allows users to manage the identities and access of other users, such as roles and accounts.
- **Synchronization**: Synchronizes identities from authoritative sources to process identity lifecycle events, such as hire, transfer, manager change, and separation from the organization. Appropriate action, including revoking access, can then be taken.
- **Provisioning and De-Provisioning**: Automates the process of creating, updating, and deleting users and their accounts, and granting/revoking of roles across applications hosted in the cloud, either using connectors to provision and de-provision with connected applications or using manual provisioning and de-provisioning in applications that do not support a connector (which are known as disconnected applications).

For DS Module applications, access is granted automatically in the DS Module AD roles based on the user's access granted in the DoIT Azure AD.

Table 8 - DS Module Application Use Cases

Use Case Specification	Use Case Reference(s)
Create User	UC.ICAM.002.1 Create User (Link found in Appendix C Section 13.3)
Modify User	UC.ICAM.002.2 Modify User (Link found in Appendix C Section 13.3)
Disable/Inactivate User	UC.ICAM.002.3 Disable/Inactivate User (Link found in Appendix C Section 13.3)

Use Case Specification	Use Case Reference(s)
Enable/Activate User	UC.ICAM.002.4 Enable/Activate User (Link found in Appendix C Section 13.3)
Delete User	UC.ICAM.002.5 Delete User (Link found in Appendix C Section 13.3)
Onboard Bulk Users	UC.ICAM.002.6 Onboard Bulk User (Link found in Appendix C Section 13.3)
Create a Role	UC.ICAM.004.1 Create a Role (Link found in Appendix C Section 13.3)
Modify A Role	UC.ICAM.004.2 Modify a Role (Link found in Appendix C Section 13.3)
Inactivate a Role	UC.ICAM.004.3 Inactivate a Role (Link found in Appendix C Section 13.3)
Delegated User Administration – View User Access	UC.ICAM.005.3 Delegated User Administration – View User Access (Role) (Link found in Appendix C Section 13.3)
Delegated User Administration – Assign Access to a User	UC.ICAM.005.4 Delegated User Administration – Assign Access (Role/Entitlement) to User (Link found in Appendix C Section 13.3)
Delegated User Administration – Revoke Access to User	UC.ICAM.005.5 Delegated User Administration – Revoke Access (Role/Entitlement) to User (Link found in Appendix C Section 13.3)

12.1.2 Identity Management Configuration Plan

The ICAM Solution will provide the capability for HSD administrators to onboard applications based on Active Directory group and manage the user life cycle based on DoIT Azure AD as an authoritative source of identities, including managing a user's access through AD group membership.

12.1.2.1 Onboard Application in ICAM

12.1.2.1.1 Create new role in ICAM

Create new role specific to the application in ICAM Identity Manager.

Table 9 - ICAM New Role Creation

Applications	Role Name	ICAM IDM role
Cognos	Analytic Explorer	Analytic_Explorer
	Analytic User	Analytic_User
	Analytic Viewer	Analytic_Viewer
Tableau	Desktop (only)	Desktop
	Creator (Desktop and Server)	Creator

Applications	Role Name	ICAM IDM role
	Explorer (Server)	Explorer
	Viewer (Server)	Viewer
IGC	Reader (aka Basic User)	Reader
SQL Developers	User	User

12.1.2.1.2 Role Mapping between DoIT Azure AD (AAD) Role to ICAM IDM Role

Configuration changes will be done to map the DoIT Azure AD role to ICAM role. The table below is a placeholder (until AAD Role Names are confirmed and finalized) table to show this mapping:

Table 10 - DoIT Azure AD and ICAM IDM Role Mapping

Applications	Role Name	DoIT Azure Active Directory Role Name*	ICAM IDM role
Cognos	Analytic Explorer		Analytic_Explorer
	Analytic User		Analytic_User
	Analytic Viewer		Analytic_Viewer
Tableau	Desktop (only)		Desktop
	Creator (Desktop and Server)		Creator
	Explorer (Server)		Explorer
	Viewer (Server)		Viewer
IGC	Reader (aka Basic User)		Reader
SQL Developers	User		User

*Please Note: The ICAM team has been unable to finalize DS specific information due to the fact we have not been able to meet with the DS Module team since August 3, 2022.

12.1.2.1.3 Role Mapping between ICAM IDM Role to DS Module AD role

Configuration changes will be done to map ICAM role to DS Module AD role. The table below is a placeholder (until role names are confirmed and finalized) table to show this mapping:

Table 11 - ICAM DS and Active Directory Role Mapping

Applications	Role Name	ICAM IDM role	DS AD role (Complete Organizational Unit (OU))*
Cognos	Analytic Explorer	Analytic_Explorer	
	Analytic User	Analytic_User	
	Analytic Viewer	Analytic_Viewer	
Tableau	Desktop (only)	Desktop	
	Creator (Desktop and Server)	Creator	
	Explorer (Server)	Explorer	
	Viewer (Server)	Viewer	
IGC	Reader (aka Basic User)	Reader	
SQL Developers	User	User	

*Please Note: The ICAM team has been unable to finalize DS specific information due to the fact we have not been able to meet with the DS Module team since August 3, 2022.

12.1.2.2 Onboard Users in ICAM

12.1.2.2.1 Reconcile Application Users to ICAM

DoIT Azure AD is the authoritative source for a user's account, therefore the first reconciliation is run against it to bring users into ICAM based on application group membership, as listed in the table below:

Table 12 - Reconcile Application Users to ICAM

Applications	Role Name	DoIT Azure Active Directory Role Name*	ICAM IDM role
Cognos	Analytic Explorer		Analytic_Explorer
	Analytic User		Analytic_User
	Analytic Viewer		Analytic_Viewer
Tableau	Desktop (only)		Desktop
	Creator (Desktop and Server)		Creator
	Explorer (Server)		Explorer
	Viewer (Server)		Viewer

Applications	Role Name	DoIT Azure Active Directory Role Name*	ICAM IDM role
IGC	Reader (aka Basic User)		Reader
SQL Developers	User		User

*Please Note: The ICAM team has been unable to finalize DS specific information due to the fact we have not been able to meet with the DS Module team since August 3, 2022.

12.1.2.2.2 Reconcile DS Module AD Users to ICAM

A user's application access is provisioned and managed by the DS Module AD, therefore additional reconciliation is run against it to bring DS Module AD information into ICAM based on AD role, as listed in the table below:

Table 13 - Reconcile DS Active Directory Users to ICAM

Applications	Role Name	ICAM IDM role	DS AD role (complete OU)*
Cognos	Analytic Explorer	Analytic_Explorer	
	Analytic User	Analytic_User	
	Analytic Viewer	Analytic_Viewer	
Tableau	Desktop (only)	Desktop	
	Creator (Desktop and Server)	Creator	
	Explorer (Server)	Explorer	
	Viewer (Server)	Viewer	
IGC	Reader (aka Basic User)	Reader	
SQL Developers	User	User	

*Please Note: The ICAM team has been unable to finalize DS specific information due to the fact we have not been able to meet with the DS Module team since August 3, 2022.

12.1.2.2.3 Data Cleanup

There is an assumption is that a user's access in DoIT Azure AD and DS Module AD are in sync, but there can be data discrepancies related to a user's access between these two (2) applications. Therefore, the SI team will perform data comparison and cleanup in two (2) stages as listed below:

- Before running reconciliations via ICAM: User's application access report should be compared between DoIT Azure AD and DS Module AD. Any data discrepancy identified must be cleaned up before running the actual reconciliations.
- After running the ICAM reconciliations: Discrepancy identified by ICAM during reconciliation needs to be cleaned up.

12.2 Access Management (AM)

AM provides functionalities such as authentication and coarse-grain authorization using industry standard federated protocols such as Security Assertion Markup Language (SAML) 2.0 for DS Module web applications. All internal HSD users will be authenticated against the DoIT Azure AD orchestrated by ICAM as an identity broker. Once the authentication is successful, ICAM will enforce coarse-grain authorization to make sure internal HSD users have required application access. Fine-grain authorization will be handled by the individual DS Module application.

The web applications below are targeted for AM integrations using extensible markup language (XML)-based open standard SAML:

- Cognos
- Tableau
- IGC

Note: Access to the non-human user accounts such as service/system accounts are enforced outside ICAM.

12.2.1 Access Management Use Cases

The ICAM Solution is an enterprise level security solution that provides a full range of web-perimeter security functions and web SSO service including identity context, authentication and authorization, policy administration, auditing, and logging functions by managing sessions and identity context and providing restricted access to confidential information.

Following are some of the high-level capabilities provided by the ICAM solution:

- **SSO, Authentication, and Authorization** allows users to access multiple applications after authentication, eliminating the need for multiple sign-on and sign off requests.
- **Identity Federation** provides cross-domain SSO support using open federation protocol standards such as SAML. This service can act as an Identity Provider (IdP) hosting user identity for authentication as well as a Service Provider (SP) protecting applications that require the cross-domain SSO functionality.
- **Identity Context**: Allows organizations to provide context-aware security policy management that enables administrators to control the level of security imposed in an application.

The below table outlines the SSO AM Capabilities for the various access channels and user types. Please note External Users are not in scope.

Table 14 - SSO Access Management Capabilities

Access Management Capabilities	Platform(s)	User Types
User Authentication	NM HSD DoIT Azure Active Directory (AAD)	Organizational Users
Coarse Grained Authorization	ICAM Solution	Organizational Users
Fined Grained Authorization	Application Level	Organizational Users
Session Management	ICAM Solution	Organizational Users
Single Sign On	ICAM Solution/NM HSD DoIT AAD	Organizational Users
Single Log Out	ICAM/NMHSD DoIT AAD/Applications	Organizational Users

Table 15 - ICAM Use Case Specifications

Use Case Specification	Use Case Reference(s)
Authenticate a User	UC.ICAM.006.1 Federated Authentication and Authorization Use Case (Link found in Appendix C Section 13.3)
Authorize a User	UC.ICAM.006.1 Federated Authentication and Authorization Use Case (Link found in Appendix C Section 13.3)
Organizational User Logout	UC.ICAM.006.2 Organizational User Logout (Link found in Appendix C Section 13.3)

13.0 Appendices

13.1 Appendix A: Deliverable Record of Changes

The deliverable will include a record of changes in the following form:

Table 16 – Deliverable Record of Changes

Version Number	Date	Author/Owner	Description of Change
0.1	8/18/2022	Spruce-KPMG Team	The initial draft for internal review
1.0	8/24/2022	Spruce-KPMG Team	Initial draft submitted to NM Deliverable Review Team
2.0	9/15/2022	Spruce-KPMG Team	Final document submitted to NM Deliverable Review Team

13.2 Appendix B: List of Acronyms

A list of project-specific acronyms will be maintained on the MMISR SharePoint site.

Table 17 – List of Acronyms

Acronym	Definition
AAD	Azure Active Directory
AD	Active Directory
AM	Access Management
ASPEN	Automated System and Program Eligibility Network
ASV	Address Standardization and Validation
AWS	Amazon Web Service
CCSC	Consolidated Customer Service Center
CSED	Child Support Enforcement Division
CSV	Comma-Separated Values
DED	Deliverable Expectation Document
DoIT	Department of Information Technology
DS	Data Services
EPMO	Enterprise Project Management Office
ETL	Extract, Transfer, Load
FTI	Federal Tax Information
HHS	Health and Human Services
HSD	Human Services Department
ICAM	Identity, Credential, and Access Management
IDM	Identity Management
IDP	ICAM Identity Provider
IEVS	Income Eligibility Verification System
IGC	Information Governance Catalog
ISD	Income Support Division
IV&V	Independent Verification and Validation
KRIS-C	KPMG Resource Integration Suite – Connected
KT	Knowledge Transfer
MCO	Managed Care Organization
MFT	Managed File Transfer
MMISR	Medicaid Management Information System Replacement
NM	New Mexico
OU	Organizational Unit
PM	Project Manager
PMO1	Project Management Office Deliverable 1 Project Management Plan
SaaS	Software-as-a-Service
SAML	Security Assertion Markup Language
SFTP	Secure File Transfer Protocol
SI	System Integrator
SIP	System Integrator Platform
SIT	System Integration Testing

Acronym	Definition
SI05	SI05 - Group 5 Plans Designs – Part B Test Management Plan
SLA	Service Level Agreement
SME	Subject Matter Expert
SMR	System Migration Repository
SOA	Service-Oriented Architecture
SOW	Statement of Work
SP	Service Provider
SQL	Structured Query Language
SSO	Single Sign On
TCRB	Technical Change Review Board
TXT	Text
UAT	User Acceptance Testing
XML	Extensible Markup Language

13.3 Appendix C: Referenced Documents

Upon contract award, the selected vendor will be provided access to additional information, as needed.

13.4Appendix D: Deliverable Approval Form

Upon approval of the SI21 – DS Module Integration – Increment 2 – Update SIP Configuration Designs deliverable, the Deliverable Approval Signature Form must be filled out, where appropriate, printed, and routed for signature. Once all signatures are provided, the Deliverable Approval Signature Form must be uploaded to SharePoint in its respective deliverable folder.