Common Key Service
Implementation Guide

Version 26
June 19th, 2024

Document History

Date	Version	Sections Revised	Description	Modifier
04/17/19	22	All	Revised into new template	S. Southard
01/06/20	22	All	Proof and edits	A. Jones
11/03/20	23	1.3.1	Update to notification types that receive common keys	M. Allen
06/08/22	24	2.4	Revised CK delete report submission instructions. Added 2.4.1 regarding CK delete report format specifications.	H. Burseth
04/17/24	25	1.3.1	Updated the patient information requirement.	A.Pacheco
6/16/2024	26	All	Edited for branding and formatting	E. Mata

Table of Contents

1. Introduction

1.1 Purpose of Data Exchange Solution

Provides a consistent and reliable way to match patients with their electronic health information across multiple organizations, applications, and services.

Patient-matching is very difficult due to the many ways patient information is stored in different computer systems and networks. For example, one hospital registration/ admission system may show gender as “Male,” “Female,” and “Unknown,” while a primary care doctor’s office system may simply list “M,” “F,” and “U.” And while this simple difference can be quickly understood, the problem can be much more complex. A patient’s name may be entered as Maryann Anthony at the hospital, Marianne Anthony in her primary care physician’s system, and Mary Anthony in her specialist’s system.

To make the issue more confusing, Maryann’s address in one system may be her most recent, while another system still lists the address of her previous home. There may be another “Maryann Anthony” with the same birth date living in the same city or county. Newborn infants that aren’t named immediately may be entered into the birthing hospital’s system as simply “Baby Girl Anthony.” In a case like that, if there is a twin, Maryann’s lab results could be added to her twin sister Merry’s medical record instead of hers.

The implications of an incorrect treatment as a result of these errors could cause serious adverse downstream effects for patients. Failures of care coordination cost $35 billion in annual healthcare waste and can cause complications, hospital readmissions, declines in functional status, and increased dependency (especially for the chronically ill for whom care coordination is essential). Average annual costs to correct mismatching errors range from $500,000 to well over $1 million on human resources alone.

To streamline the exchange of health information, electronic healthcare systems require reliable patient-matching tools to ensure the right information is attributed to the right patient every time. The Common Key Service (CKS) Data Exchange Solution utilizes multiple methods to link health information to individuals, such as:

1. The CKS uses proven matching criteria to ensure patient details (such as last name, date of birth, and phone number) positively and accurately identify

the patient.

2. The CKS connects with a Master Person Index (MPI) to manage information about patients and to eliminate duplicate entries with great accuracy.
3. The MPI uses an industry best-practice formula to determine that Maryann Anthony, Marianne Anthony, and Mary Anthony are in fact the same person based on her other details (such as last name, date of birth, and last four digits of her Social Security Number).
4. The CKS assigns a unique key that is stored and attached to the patient in the MPI and shared with all systems exchanging information about that patient. Each system can link their respective medical record number to the same common key and then include the common key when exchanging information about the patient.

Essentially, the CKS strengthens matching by providing consistent and accurate detail (the individual patient's common key) that each system can rely on.

This reliable matching capability improves patient safety and data integrity in all data exchange solutions when information is shared about a specific patient. Combining the common key with a second factor (such as birth date or last four digits of Social Security Number) can increase patient privacy by de-identifying messages while still reliably associating the information to the right patient whenever the information is exchanged.

Over time, as CKS adoption grows throughout the state and more and more local systems link patients to a common key, it may no longer be necessary to include all a patient's demographic information when exchanging their medical information. This would further improve the privacy and security of the information exchange as well by de-identifying the message.

Participating organizations send various patient roster files and/or notification messages via a Trusted Data Sharing Organization (TDSO) to Michigan Health Information Network Shared Services (MiHIN). The CKS passes the patient list and notification messages to the MPI which validates that the data is complete and properly formatted. The MPI uses the patient's demographic information to match the patient to existing entities in the MPI. A successful integrated approach can improve efficiency and completeness of care coordination, safety of patients, quality of care, prevention of fraud, accuracy of information exchanged, and ease of participation by smaller organizations. It can help organizations prepare for future requirements, realize potential cost savings, improve data integrity, and drive standardization.

1.2 Message Content

The Use Case Exhibit (UCE) for this data exchange solution defines message content as all data as defined in the Implementation Guide containing Common Key.

For the purposes of implementation of this data exchange solution, Message Content means a unique patient identifier provided by MiHIN for use in system-to-system patient matching.

The current message formats supported by the IIS are HL7 v2.5.1 (preferred) and HL7 v2.3.1. Future versions of HL7 messages may be implemented and supported in the future, such as the Fast Healthcare Interoperability Resources (FHIR). For more information, refer to http://www.hl7.org/implement/standards/fhir.

1.3 Data Flow

1.3.1 Functional Data Flow

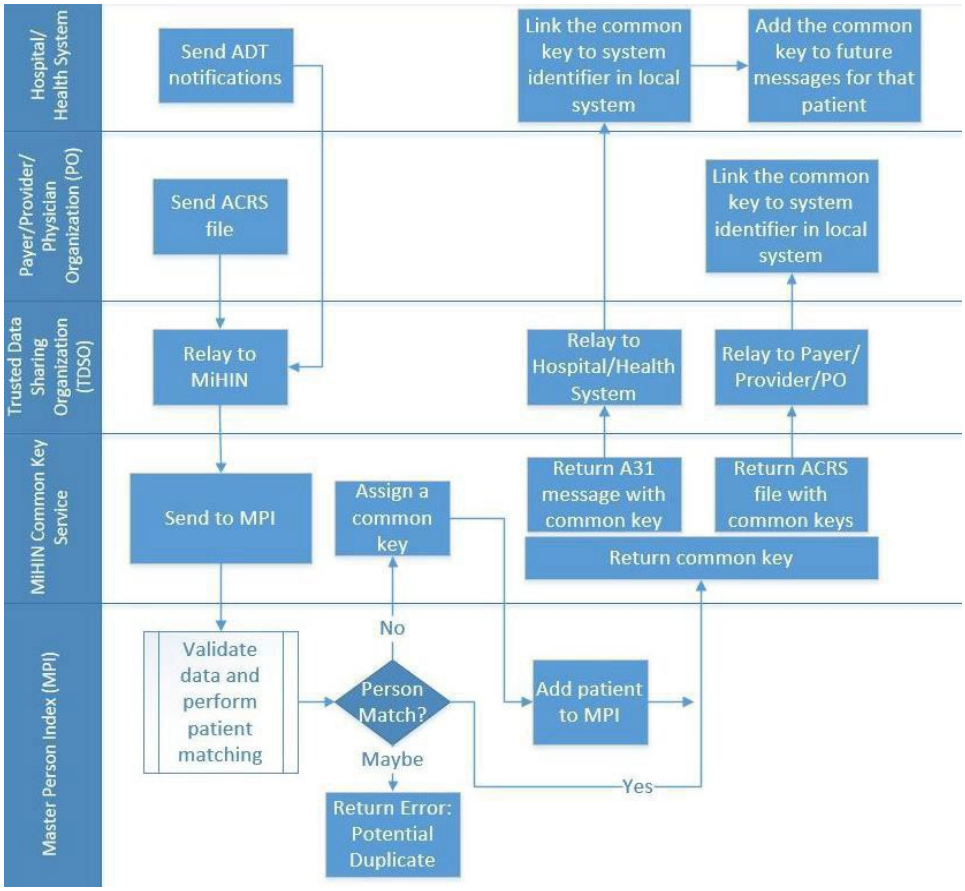

Figure 1. Common Key Service Data Flow

When a patient's information is sent to MiHIN from a healthcare provider (such as a doctor, hospital, etc.), that patient record will be processed through the CKS to facilitate better patient matching with existing records. The following fields of patient information are required to receive a common key for any given patient:

- Provider organization name
- Unique patient ID (source identifier, Medical Record Number)
- Given name
- Family name
- Gender
- Date of birth
- SSN or Address or Phone Number

One of three results are possible for each patient processed through the CKS:

Match = "No"

If the patient is not found in the MPI, the MPI will invoke the CKS to assign the patient a common key. The patient and the assigned common key are added to and stored in the MPI.

Match = "Yes"

If a person is found in the MPI, it returns the common key that has been previously assigned to that patient by the CKS to ensure accurate mapping across systems.

Match = "Maybe"

If a potential match is identified, but it cannot be determined with a high level of confidence whether the patient does or does not exist in the MPI (that is, the algorithm results in a score between predefined minimum "no match" and maximum "match" score thresholds), a "possible duplicate" result is generated. A common key is not assigned until a definitive determination can be made to ensure the integrity and reliability of the common key.

The MPI then adds the common key to the patient list or notification message and returns it to the CKS. The common keys are then passed back to the participating organization via the TDSO so the common key(s) can be linked to the local identifier in their source system.

Senders can subsequently add the common key to future messages for that patient, providing an additional attribution to help strengthen patient matching by the receiver of the message. Receivers participating in the CKS may also link their local system identifier for a patient to the same common key and can now be much more certain to which patient the information in the message pertains.

Participating organizations may send patient information to be assigned common keys via the following mechanisms:

1. *Active Care Relationship Service (ACRS) file:* An ACRS file format is sent to MiHIN to be assigned common keys. See the ACRS file format available on the MiHIN website for more information on this format.
2. *Admission, Discharge, Transfer (ADT) Notifications:* A01, A03, and A04 notifications received by MiHIN will be assigned common keys. See the ADT Notifications Implementation Guide on the MiHIN website for details on the required format.

Facilities may receive common keys via the following mechanisms:

1. *ACRS:* An ACRS 2.0 format file is returned with common keys filled in for the patient(s). The common key will be in the "common key" column, or empty if unable to assign.
2. *HL7 v2.5.1:* An A31 ADT message is sent to the receiving system to alert the end system to common keys for the user, and to communicate changes to common keys.

Facilities may query dynamically for common keys via the following mechanism:

1. *HL7 FHIR:* An organization can request the common key for a set of demographics using a RESTful FHIR-like query to the common key service.

1.3.2 Actors

- **Actor:** Hospital/Health System
    - *Role:* Sends ADT notifications to MiHIN and receives back an A31 message with the patient's common key (if one is assigned); stores common key in local system to be included in exchanged healthcare data for other MiHIN data exchange solutions.
- **Actor:** Provider/Physician Organization
    - *Role:* Sends ACRS files to MiHIN and receives them back with the patient's common key (if one is assigned); stores common key in local system for use as an additional attribute for matching patients when receiving messages to MiHIN.
- *Actor:* Trusted Data Sharing Organization
    - *Role:* Routes messages to and from MiHIN.

- **Actor:** MiHIN
    - *Role*: Receives patient information from sending systems; invokes CKS on this data to assign common keys to patients.
- **Actor:** Master Person Index
    - *Role:* Maintains consistent, accurate and current demographic data on the patients seen and managed by the Hospital/Health System.

The data exchange solution summary is available online at https://mihin.org/common-key-service-use-case/

You can contact MiHIN at www.mihin.org/requesthelp for more information.

2. Onboarding

2.1 Prerequisites

Participating organizations should begin two parallel onboarding tracks simultaneously:

- Obtain, review, and execute legal agreements, and
- Establish technical transport and testing.

2.1.1 Universal Legal Prerequisites

The following legal documentation will need to be executed prior to any connectivity being established between MiHIN and participating organizations.

- Statement of Work (SOW)
- MiHIN's Exhibit A Agreement (Found on the MiHIN Legal Portal)
- Participant Agreement (Found on the MiHIN Legal Portal)
- Must select the appropriate data exchange solution (Common Key Service) on the MiHIN legal portal in addition to the above agreements.

To initiate the legal onboarding contact, email help@mihin.org.

2.1.2 Technical Requirements

The following data exchange solution implementations and technical requirements will need to be conducted for (Name of the Data Exchange Solution) to function.

2.1.2.1 Data Exchange or Application Requirements

It is assumed that the participating organization has onboarded to ACRS and ADT Notification Data Exchange Solutions.

2.1.2.2 Other Requirements

- Organizations sending common key messages must have onboarded to a data exchange solution that allows them to send messages to MiHIN (ADT, ORU, etc.) and must be able to ingest returned A31 messages with common keys and link them to system identifiers in their local system and add those common keys to future messages.
- Organizations receiving common keys must have submitted a valid ACRS file with the names of patients they share an active care relationship with that they would like to receive common keys for and must be able ingest returned

ACRS files enriched with common keys into their local system and link them with their system identifiers for those patients.

- Organizations must be able to connect with MiHIN via Direct Secure Messaging or via SFTP to be able to submit delete reports or alert MiHIN of splits/merges. More information on this process is provided in Section 3.

2.2 Common Key Service Onboarding Process

2.2.1 Sender Onboarding Process

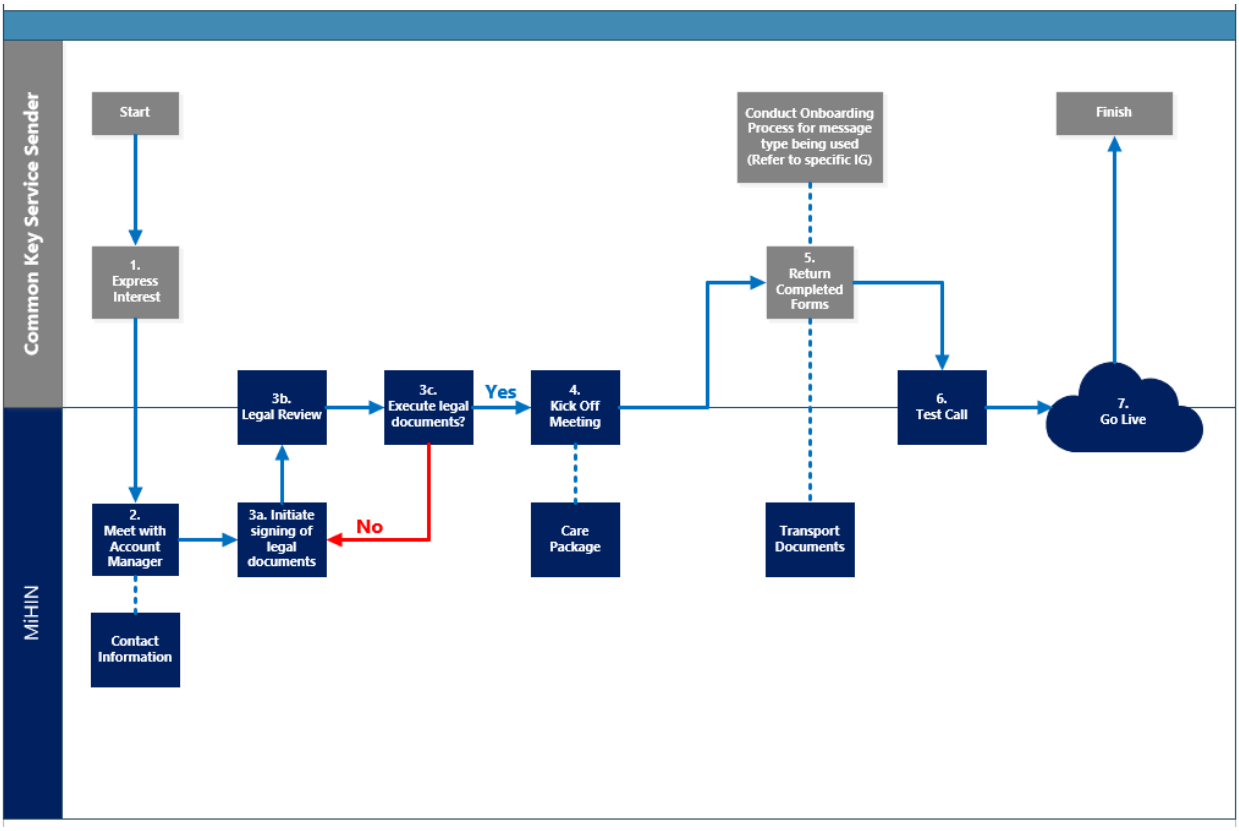

Figure 2 Common Key Service Sender Onboarding Workflow

- Express interest in participating in the use data exchange solution
- Meet with Account Manager
    - Exchange contact information
- Legal Review
- Execute legal documents
- Kick Off Meeting
- Distribute Common Key Care Package
- Exchange required documents

- Transport Document
  - DSM Request Form or,
  - SFTP Request Form

- Complete onboarding process for specific message types to be used for the common key service
- Testing
- Go Live

2.2.2 Receiver Onboarding Process

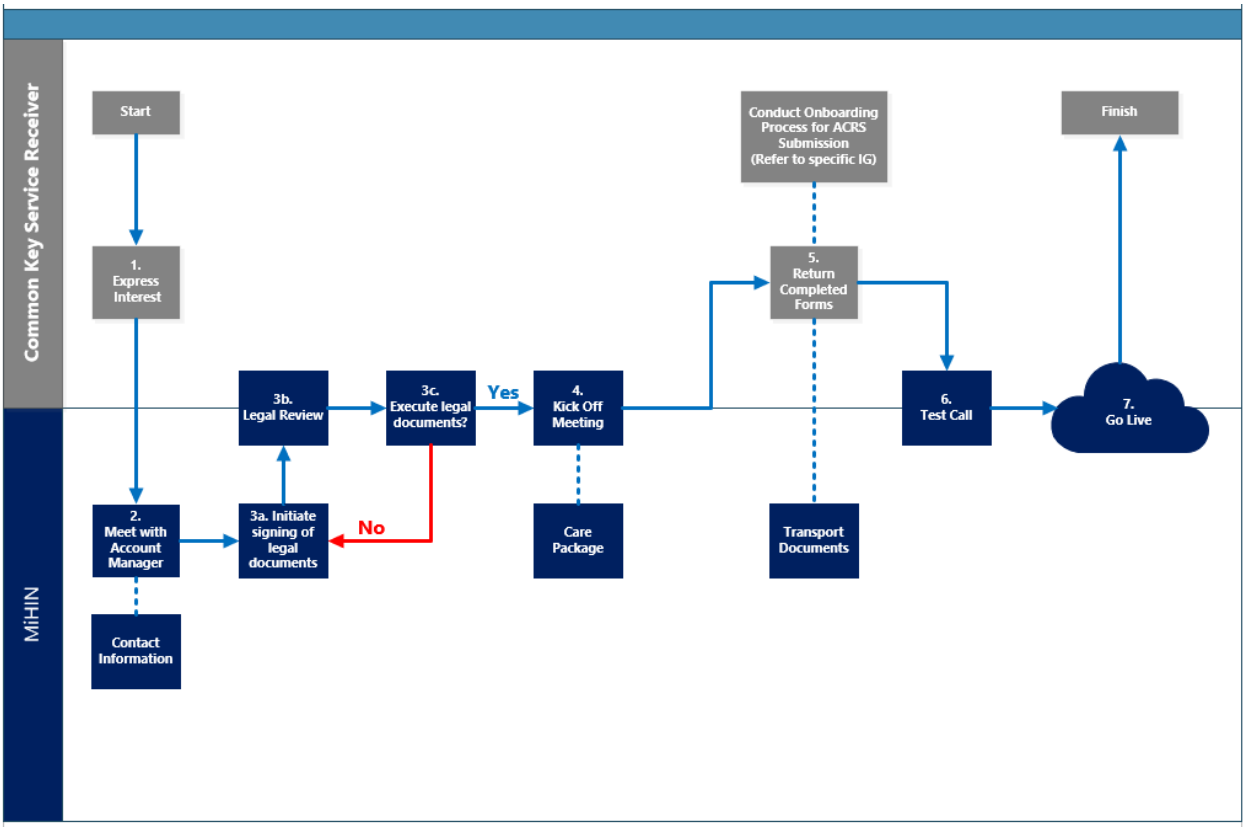

Figure 3 Common Key Service Receiver Onboarding Workflow

- Express interest in participating in the use data exchange solution
- Meet with Account Manager
  - Exchange contact information
- Legal Review
- Execute legal documents
- Kick Off Meeting
- Distribute Common Key Care Package
- Exchange required documents

    - Transport Document
        - DSM Request Form or,
        - SFTP Request Form
- Complete onboarding process for ACRS submission and successfully submit valid ACRS file
- Testing
- Go Live

2.3 Technical Connectivity Process

MiHIN considers itself "transport agnostic" and offers multiple options for organizations to establish technical connectivity to transport data to HIN. Organizations should select one or more connectivity methods for message transport based on their technical capabilities and should communicate the selection(s) to www.mihin.org/requesthelp early in the onboarding process. Currently the ONLY transport methods the HIN accepts are:

- **DSM –** Direct Secure Messaging
- **SFTP –** Secure File Transfer Protocol

Additional transport methods may be added in the future. These can include NwHIN, XCA, FHIR, and others.

The following steps describe the technical onboarding process. However, MiHIN typically conducts "onboarding kickoff" meetings with new organizations to go through each of these steps in detail and answer any questions.

1a. For Common Key Service Senders, organizations will need to complete onboarding steps to fully set up and test the data exchange solution they will be leveraging for the Common Key Service. Please refer to the specific Implementation Guide for that data exchange solution for process instructions.

1b. For Common Key Receivers, organization will need to complete onboarding steps to facilitate the submission of a valid ACRS file for patients they share an active care relationship with and would like to receive common keys for prior to set and testing of the Common Key Service.

1. The organization selects one or more supported transport methods that they will use to send notice of split/merge deletions of common keys in their local

system and establishes connectivity with MiHIN. This step varies based on the method selected:

a. **Direct Secure Messaging** – MiHIN accepts Direct Secure Messages from Health Internet Service Provider (HISPs) that have EHNAC-DTAAP (DirectTrust) accreditation. Test messages are sent to verify HISP connectivity ("ping pong"). The Message Header section in the test messages is verified for appropriate routing configuration.

b. **Secure File Transfer Protocol** – The SFTP Request form must be filled out and returned. MiHIN will return file path information and account login credentials via email and cell phone for security purposes. Connectivity is verified by onboarding organization by confirming the presence of the appropriate file paths and folders.

2. Once prerequisite feeds or ACRS files have been established and/or submitted, Test messages will be sent to confirm connectivity.

    a. For Sending Organizations:
        i. Sending organizations will generate Test messages to send to MiHIN via configured transport method. MiHIN will confirm receipt of messages and the organization will confirm receipt of any applicable ACKs returned to them.
        ii. MiHIN will confirm that test messages have been sent to MPI and will confirm the creation of a common key and the generation and return of an A31 message with the generated common key to the onboarding organization
        iii. The onboarding organization will confirm receipt of A31 message with common key and ingestion of the common key into their system. They will send another test message for the test patient to MiHIN, who will confirm receipt and the presence of the assigned common key on the received message.

    b. For Receiving Organizations:
        i. Once the onboarding organization has successfully submitted an ACRS attribution file, MiHIN will process said ACRS file and return it via established transport.
        ii. Organization will confirm receipt of ACRS file and whether it has been enriched with common keys. They will also confirm that the file

has been ingested into their local system and that present common keys have been linked to system identifiers.

3 Specifications

3.1 Overview

3.1.1 Environments

- MiHIN Pre-Production
- MiHIN Production

3.2 General Specifications

3.2.1 Common Key Assignment

MIHIN's role in the context of this implementation guide requires that MIHIN will, at a minimum, send the Message Header (MSH), Event Type (EVN), and Patient Identification (PID) segments with the associated demographics. The common key and local identifier(s) are located in PID-3 (section 4.2). For more information on MSH and EVN requirements, please see the MiHIN Admission Discharge Transfer Notifications Implementation Guide for HL7 Messages. All segments and fields will be present and populated according to the requirements of the MiHIN Common Key Service Implementation Guide.

3.2.2 Common Key Change Events

Common keys may be updated from time to time as a result of ongoing de-duplication and data cleansing activities. Participating organizations (POs) and PO participants will receive CKS change ADT notifications to be aware of these changes. PO and PO participants will propagate changes to common keys throughout their health information systems within 14 calendar days of receipt of these updates. See Section 4.2.1 for more details on common key de-duplication and data cleansing activities.

3.2.3 Merge/Split at Participating Organization

Sometimes records requiring a merge, or a split are identified within a PO's local system. When a PO identifies two or more separate records in their local system as belonging to the same person (requiring a merge of these records), and each of those records has been assigned a different common key, the participating organization must delete these common keys from their local system and inform MiHIN of the common key deletion. **If the records have the same common key assigned by MiHIN, no action is required.**

This also applies to records which have been identified as requiring a split (a single record in the local system which belongs to one or more patients and must be parsed out). If a common key has been assigned to the original record requiring a split, this common key must be deleted from the local system and MiHIN informed of the deletion.

The PO will inform MiHIN daily of the deletion by sending a Direct Secure Message to commonkeyservice@direct.mihin.net with the common key(s) to delete attached. Secure File Transfer Protocol (SFTP) is also an option for organizations to send a daily report of internal merge/splits. MiHIN will retire the common key(s) and delete the associated record from the MPI. This update will be broadcasted in a change notification to all POs (whichever organizations have ever received that specific common key) requiring the common key to be DELETED in their local systems as well.

3.2.3.1 Common Key Deletions Report Format

When submitting via Direct Secure Message or SFTP, the common key(s) to delete should be listed within a CSV file with file name “Common Keys to Delete”. The file should contain a single column list of the common key value(s) with a header value of "Common Keys to Delete". No additional data elements should be included in the file. When submitting via SFTP, common key delete files must be placed in the INPUT folder within the assigned directory for automatic pickup.

3.3 Specific Segment and Field Definitions

3.3.1 PID-2 (Patient ID)

The historical intent of this field is to contain an identifier for the patient at an institution or facility other than the institution or facility at which the event occurred. Previous to HL7 Version 2.3.1, it was referred to as “external ID.” It is recommended that identifiers for the patient be sent in occurrences of PID-3-patient identifier list rather than in fields PID-2- patient ID, PID-4-alternate patient ID-PID, or PID-19-SSN-patient, all of which were deprecated as of HL7 Version 2.3.1.

The data type of PID-2-patient ID is CX, whose components are as follows:

Cmp	DT	Usage	TBL#	Element Name	Comments
1	ST	R		ID	The full, unique identifier value for the patient.

2	ST	O		Check Digit	
3	ID	O	0061	Code Identifying the Check Digit Scheme Employed	
4	HD	O	0363	Assigning Authority	The system, organization, agency or department that created this patient identifier.
5	IS	O	0203	Identifier Type Code	What kind of identifier this is: local, facility, state or national, Social Security, Medicare, etc.
6	HD	O		Assigning Facility	The place or location where the identifier was first assigned to the patient.

3.3.2 PID-3 (Patient Identifier List)

This field, which allows for up to 99 occurrences, contains at least the identifier for the patient at the institution or facility at which the event occurred. The common key will be placed in PID-3 as one of these occurrences, in combination with the original patientID from the ADT^A03 supplied by the sender. It is recommended that any other identifiers for the patient be sent in additional occurrences of PID-3-patient identifier list.

The data type of PID-3-patient identifier list is CX, whose components are as follows:

Cmp	DT	Usage	TBL#	Element Name	Comments
1	ST	R		ID	The full, unique identifier value for the patient.
2	ST	O		Check Digit	Restatement of the check digit portion, if any, of the ID number in component 1.
Cmp	**DT**	**Usage**	**TBL#**	**Element Name**	**Comment**
3	ID	O	0061	Code Identifying the Check Digit Scheme Employed	

4	HD	O	0363	Assigning Authority	The system, organization, agency or department that created this patient identifier.
5	IS	RE	0203	Identifier Type Code	What kind of identifier this is: local, facility, state or national, CKS, Medicare, etc.
6	HD	O		Assigning Facility	The place or location where the identifier was first assigned to the patient.

NOTE: The identifier type for component 5 when the identifier is a common key will be "CKS". Because the common key identifier is alphanumeric, the <check digit> and <code identifying check digit scheme> components may be left blank.

- Example PID-3: agsehodt6wzrdzey5uabkxib7ug37hccd6w4m5e7^^^^CKS

Example PID-3 showing an imaginary source identifier from the original system, with the common key:

- 10006579^^^1^MRN^1 ~agsehodt6wzrdzey5uabkxib7ug37hccd6w4m5e7^^^^CKS

NOTE: If there is no common key available, no A31 message will be sent.

3.3.2.1 Special Handling of ADT^A31s

When an organization receives an A31 with ZCK and ZAD segments present this is an indicator that the CKS identifier sent in ZCK-2 should be deleted from your source system.

For example, if two patients who were assigned two different common keys were later found to be the same person, then those patients would be merged in the MPI and a new common key would be assigned to the new merged record.

NOTE: This does not mean a user must merge in their local system; however, the obsolete common keys for those two old separate records must now be removed in the source system.

MiHIN would send out two A31 messages, one for each patient. The ZCK-2 field of the A31 would include the common key to be unmapped where it may be stored by the sender.

If the common key is no longer or not present in a user's system, they can ignore the A31 message

3.3.2.2 Message Example

An example A31 change message conformant to this specification can be found in Appendix A (minimum requirements):

3.3.3 PID-4 (Alternate Patient ID)

The historical intent of this field is to contain one or more identifiers for the patient other than the principal patient identifier carried in PID-3. It is recommended that identifiers for the patient be sent in occurrences of PID-3-patient identifier list rather than in fields PID-2- patient ID, PID-4-alternate patient ID-PID, or PID-19-SSN-patient, all of which were deprecated as of HL7 Version 2.3.1.

The data type of PID-4-alternate patient ID-PID is CX, whose components are as follows:

Cmp	DT	Usage	TBL#	Element Name	Comments
1	ST	R		ID	The full, unique identifier value for the patient.
2	ST	O		Check Digit	
3	ID	O	0061	Code Identifying the Check Digit Scheme Employed	
4	HD	O	0363	Assigning Authority	The system, organization, agency or department that created this patient identifier.
5	IS	O	0203	Identifier Type Code	What kind of identifier this is: local, facility, state or national, Social Security, Medicare, etc.
6	HD	O		Assigning Facility	The place or location where the identifier was first assigned to the patient.

4. Production Support

	Severity Levels			
	1	***2***	***3***	***4***
Description	***Critical Impact/ System Down:*** Business critical software is down or critical interface has failed. The issue is impacting all production systems, causing all participating organizations' or other organizations' ability to function to be unusable.	***Significant Business Impact:*** Software component severely restricted. Entire organization is unable to continue business functions, causing all communications and transfer of messages to be halted.	**Partial Failure or Downtime:** Program is useable and less significant features unavailable. The service is online, though may not working as intended or may not currently working as intended or may not currently be accessible, though other systems are currently available.	**Minimal Business:** A non-critical software component is malfunctioning, causing minimal impact, or a test system is down.
Example	All messages to and from MiHIN are unable to be sent and received, let alone tracked	MiHIN cannot communication (send or receive) messages between single or multiple participating organizations, but can still successfully communicate with other organizations.	Messages are lost in transit; messages can be received but not sent.	Additional feature requested.
Primary Initiation Method	***Phone:*** (517) 336-1430	***Phone:*** (517) 336-1430	Web form at http://mihin.org/requesthelp	Web form at http://mihin.org/requesthelp
Secondary Initiation Method	Web form at http://mihin.org/requesthelp	Web form at http://mihin.org/requesthelp	Email to help@mihin.org	Email to help@mihin.org
Tertiary Initiation Method	Email to help@mihin.org	Email to help@mihin.org	N/A	N/A
Initial Response	Within 2 hours	Within 2 hours	1 business day	1 business day
Resolution Goal	24 hours	24 hours	3 business days	7 business days

A list of common questions regarding the Common Key Service Data Exchange Solution can be found at:

https://mihin.org/common-key-service-use-case/

If you have questions, please contact the MiHIN Help Desk:

- www.mihin.org/requesthelp
- Phone: (517) 336-1430
- Monday – Friday 8:00 AM – 5:00 PM (Eastern)

5. Legal Advisory Language

This reminder applies to all use cases covering the exchange of electronic health information:

The Data Sharing Agreement (DSA) establishes the legal framework under which participating organizations can exchange messages through the MiHIN Platform, and sets forth the following approved reasons for which messages may be exchanged:

a. By health care providers for Treatment, Payment and/or Health Care Operations consistent with the requirements set forth in HIPAA
b. Public health activities and reporting as permitted by HIPAA and other Applicable Laws and Standards
c. To facilitate the implementation of "Meaningful Use" criteria as specified in the American Recovery and Reinvestment Act of 2009 and as permitted by HIPAA
d. Uses and disclosures pursuant to an Authorization provided by the individual who is the subject of the Message or such individual's personal representative in accordance with HIPAA
e. By Data Sharing Organizations for any and all purposes, including but not limited to pilot programs and testing, provided that such purposes are consistent with Applicable Laws and Standards
f. For any additional purposes as specified in any use case, provided that such purposes are consistent with Applicable Laws and Standards

Under the DSA, "***Applicable Laws and Standards***" means all applicable federal, state, and local laws, statutes, acts, ordinances, rules, codes, standards, regulations and judicial or administrative decisions promulgated by any governmental or self-regulatory agency, including the State of Michigan, the Michigan Health Information Technology Commission, or the Michigan Health and Hospital Association, as any of the foregoing may be amended, modified, codified, reenacted, promulgated or published, in whole or in part, and in effect from time to time. "Applicable Laws and Standards" includes but is not limited to HIPAA; the federal Confidentiality of Alcohol and Drug Abuse Patient Records statute, section 543 of the Public Health Service Act, 42 U.S.C. 290dd-2, and its implementing regulation, 42 CFR Part 2; the Michigan Mental Health Code, at MCLA §§ 333.1748 and 333.1748a; and the Michigan Public Health Code, at MCL § 333.5131, 5114a.

It is each participating organization's obligation and responsibility to ensure that it is aware of Applicable Laws and Standards as they pertain to the content of each

message sent, and that its delivery of each message complies with the Applicable Laws and Standards. This means, for example, that if a use case is directed to the exchange of physical health information that may be exchanged without patient authorization under HIPAA, the participating organization must not deliver any message containing health information for which an express patient authorization or consent is required (e.g., mental or behavioral health information).

Disclaimer: The information contained in this implementation guide was current as of the date of the latest revision in the Document History in this guide. However, Medicare and Medicaid policies are subject to change and do so frequently. HL7 versions and formatting are also subject to updates. Therefore, links to any source documents have been provided within this guide for reference. MiHIN applies its best efforts to keep all information in this guide up-to-date. It is ultimately the responsibility of the participating organization and sending facilities to be knowledgeable of changes outside of MiHIN's control.

6. Appendices

6.1 Appendix A – Message Examples

An example A31 change message conformant to this specification is below (minimum requirements):

MSH|^~\&|2.16.840.1.113883.3.1481.00.1032|2.16.840.1.113883.3.1481||2.16.840.1.113 883.3.137|20180129110722||ADT^A31|34676344|T|2.5.1

EVN|A31|20180129110722

PID|||8764333^^^^MRN|| ZCK||ah088b7140ff9840368455be6871637395

ZAD|ALICE|VARGAS|19900510|F|4520 Lincoln Drive^^Brighton^MI^48114|1153

* yellow highlight indicates common key

7. Acronyms and Abbreviations Guide

ACK	HL7 Acknowledgment message
ACRS	Active Care Relationship Service
API	Application Programming Interface
CCHD	Critical Congenital Heart Disease
CMS	Centers for Medicare & Medicaid Services
DDE	Direct Data Entry
DQA	Data Quality Assurance
EHR	Electronic Health Record
FHIR	Fast Healthcare Interoperability Resources
HIE	Health Information Exchange
HIN	Health Information Network
HISP	Health Internet Service Provider
HL7	Health Level Seven
HPD	Health Provider Directory
MDHHS	Michigan Department of Health and Human Services
MIDIGATE	Medical Information Direct Gateway
MiHIN	Michigan Health Information Network Shared Services
MUCA	Master Use Case Agreement
NACK	Negative Acknowledgement
NBS	Newborn Screening
NwHIN	Nationwide Health Information Network
OID	Object Identifier
PO	Participating Organization
RAS	Registration and Attestation System
REST	Representational State Transfer
SAML	Security Assertion Markup Language
SMTP	Simple Mail Transfer Protocol
SOM	State of Michigan
TDSO	Trusted Data Sharing Organization
UCE	Use Case Exhibit
UCS	Use Case Summary
VPN	Virtual Private Network
XCA	Cross-Community Access
XDS	Cross-Enterprise Document Sharing

8. Definitions

Active Care Relationship (ACR). (a) For health providers, a patient who has been seen by a provider within the past 24 months, or is considered part of the health provider's active patient population they are responsible for managing, unless notice of termination of that treatment relationship has been provided to MiHIN; (b) for payers, an eligible member of a health plan;(c) an active relationship between a patient and a health provider for the purpose of treatment, payment and/or healthcare operations consistent with the requirements set forth in HIPAA; (d) a relationship with a health provider asserted by a consumer and approved by the health provider; or (e) any person or TDSO authorized to receive message content under an exhibit which specifies that an ACR may be generated by sending or receiving message content under that exhibit. ACR records are stored by MiHIN in the ACRS.

Active Care Relationship Service® (ACRS®). The MiHIN infrastructure service that contains records for those TDSOs, their participating organizations participants or any health providers who have an active care relationship with a patient.

Admission, Discharge, Transfer (ADT). An event that occurs when a patient is admitted to, discharged from, or transferred from one care setting to another care setting or to the patient's home. For example, an ADT event occurs when a patient is discharged from a hospital. An ADT event also occurs when a patient arrives in care setting such as a health clinic or hospital.

Applicable Laws and Standards. In addition to the definition set forth in the Data Sharing Agreement, the federal Confidentiality of Alcohol and Drug Abuse Patient Records statute, section 543 of the Public Health Service Act, 42 U.S.C. 290dd-2, and its implementing regulation, 42 CFR Part 2; the Michigan Mental Health Code, at MCLA §§ 333.1748 and 333.1748a; and the Michigan Public Health Code, at MCL § 333.5131, 5114a.

Attribution. The connection between a consumer and their health care providers. One definition of attribution is "assigning a provider or providers, who will be held accountable for a member based on an analysis of that member's claim data." The attributed provider is deemed responsible for the patient's cost and quality of care, regardless of which providers deliver the service.

Conforming Message. A message that is in a standard format that strictly adheres to the implementation guide for its applicable use case.

Critical Congenital Heart Disease (CCHD). A group of serious heart defects that are present from birth. These abnormalities result from problems with the formation of one or more parts of the heart during the early stages of embryonic development.

Data Sharing Agreement. Any data sharing organization agreement signed by both MiHIN and a participating organization. Data sharing organization agreements include but are not limited to: Qualified Data Sharing Organization Agreement, Virtual Qualified Data Sharing Organization Agreement, Consumer Qualified Data Sharing Agreement, Sponsored Shared Organization Agreement, State Sponsored Sharing Organization Agreement, Direct Data Sharing Organization Agreement, Simple Data Sharing Organization Agreement, or other data sharing organization agreements developed by MiHIN.

Electronic Address. A string that identifies the transport protocol and end point address for communicating electronically with a recipient. A recipient may be a person, organization or other entity that has designated the electronic address as the point at which it will receive electronic messages. Examples of an electronic address include a secure email address (Direct via secure SMTP) or secure URL (SOAP / XDR / REST / FHIR). Communication with an electronic address may require a digital certificate or participation in a trust bundle.

Electronic Medical Record or Electronic Health Record (EMR/EHR). A digital version of a patient's paper medical chart.

Electronic Service Information (ESI). All information reasonably necessary to define an electronic destination's ability to receive and use a specific type of information (e.g, discharge summary, patient summary, laboratory report, query for patient/provider/healthcare data). ESI may include the type of information (e.g. patient summary or query), the destination's electronic address, the messaging framework supported (e.g., SMTP, HTTP/SOAP, XDR, REST, FHIR), security information supported or required (e.g., digital certificate) and specific payload definitions (e.g., CCD C32 V2.5). In addition, ESI may include labels that help identify the type of recipient (e.g., medical records department).

End Point. An instance of an electronic address or ESI.

Exhibit. Collectively, a use case exhibit or a pilot activity exhibit.

FedSim. Simulators that are utilized in a testing environment to simulate testing with a federal partner e.g. SSA or VA

Health Directory. The statewide shared service established by MiHIN that contains contact information on health providers, electronic addresses, end points, and ESI, as a resource for authorized users to obtain contact information and to securely exchange health information.

Health Level 7 (HL7). An interface standard and specifications for clinical and administrative healthcare data developed by the Health Level Seven organization and approved by the American National Standards Institute (ANSI). HL7 provides a method for disparate systems to communicate clinical and administrative information in a normalized format with acknowledgement of receipt

Health Information. Any information, including genetic information, whether oral or recorded in any form or medium, that (a) is created or received by a health provider, public health authority, employer, life insurer, school or university, or healthcare clearinghouse; and (b) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Health Information Network (HIN). An organization or group of organizations responsible for coordinating the exchange of protected health information (PHI) in a region, state, or nationally.

Health Plan. An individual or group plan that provides, or pays the cost of medical care (as "group health plan" and "medical care" are defined in section 2791(a)(2) of the Public Health Service Act, 42 U.S.C. 300gg-91(a)(2)). Health plan further includes those entities defined as a health plan under HIPAA, 45 C.F.R 160.103.

Health Professional means (a) any individual licensed, registered, or certified under applicable Federal or State laws or regulations to provide healthcare services; (b) any person holding a nonclinical position within or associated with an organization that provides or coordinates healthcare or healthcare related services; and (c) people who contribute to the gathering, recording, processing, analysis or communication of health information. Examples include, but are not limited to, physicians, physician assistants, nurse practitioners, nurses, medical assistants, home health professionals, administrative assistants, care managers, care coordinators, receptionists and clerks.

Health Provider means facilities/hospitals, health professionals, health plans, caregivers, pharmacists/other qualified professionals, or any other person or organization involved in providing healthcare.

Information Source. Any organization that provides information that is added to a MiHIN infrastructure service.

Master Use Case Agreement (MUCA). Legal document covering expected rules of engagement across all use cases. Trusted data sharing organizations sign master use case agreement one time, then sign use case exhibits for participation in specific use cases.

Message. A mechanism for exchanging message content between the participating organization to MiHIN services, including query and retrieve.

Message Content. Information, as further defined in an Exhibit, which is sent, received, found or used by a participating organization to or from MiHIN services. Message content includes the message content header.

Message Header ("MSH") or Message Content Header. The MSH segment present in every HL7 message type that defines the Message's source, purpose, destination, and certain syntax specifics such as delimiters (separator characters) and character sets. It is always the first segment in the HL7 message, with the only exception being HL7 batch messages.

Michigan Health Information Network Shared Services. The MiHIN for the State of Michigan.

MiHIN Infrastructure Service. Certain services that are shared by numerous use cases. MiHIN infrastructure services include, but are not limited to, Active Care Relationship Service (ACRS), Health Directory, Statewide Consumer Directory (SCD), and the Medical Information DIrect GATEway (MIDIGATE®).

MiHIN Services. The MiHIN infrastructure services and additional services and functionality provided by MiHIN allowing the participating organizations to send, receive, find, or use information to or from MiHIN as further set forth in an exhibit.

Negative Acknowledgment (NAK or NACK). "Not acknowledged" and is used to negatively acknowledge or to reject previously received message content or to indicate an error.

Newborn Screening. Screening to detect conditions such as critical congenital heart disease (CCHD) in newborns. The newborn screening is not limited to this test.

Notice. A message transmission that is not message content and which may include an acknowledgement of receipt or error response, such as an ACK or NACK.

Patient Data. Any data about a patient or a consumer that is electronically filed in a participating organization or participating organization participant's systems or repositories. The data may contain protected health information (PHI), personal credit information (PCI), and/or personally identifiable information (PII).

Person Record. Any record in a MiHIN infrastructure service that primarily relates to a person.

Pilot Activity. The activities set forth in the applicable exhibit and typically includes sharing message content through early trials of a new use case that is still being defined and is still under development and which may include participating organization feedback to MiHIN to assist in finalizing a use case and use case and use case exhibit upon conclusion of the pilot activity.

Principal. A person or a system utilizing a federated identity through a federated organization.

Promoting Interoperability. Using certified EHR technology to improve quality, safety and efficiency of healthcare, and to reduce health disparities as further contemplated by title XIII of the American Recovery and Reinvestment Act of 2009.

Provider Community. A healthcare provider with an active care relationship with the applicable patient.

Send / Receive / Find / Use (SRFU). Means sending, receiving, finding, or using message content. Sending involves the transport of message content. Receiving involves accepting and possibly consuming or storing message content. Finding means querying to locate message content. Using means any use of the message content other than sending, receiving and finding. Examples of use include consuming into workflow, reporting, storing, or analysis. Send/Receive/Find/Use (SRFU) activities must comply with Applicable Laws & Standards or State Administrative Code as that term is defined in this agreement and the data sharing agreement.

Service Interruption. A party is unable to send, receive or find message content for any reason, including the failure of network equipment or software, scheduled or unscheduled maintenance, general Internet outages, and events of force majeure.

Source System. A computer system, such as an electronic health record system, at the participating organization, that sends, receives, finds or uses message content or notices.

Statewide Consumer Directory (SCD). A MiHIN infrastructure service that helps organizations provide tools to consumers, which allow the consumers to manage how their personal Health Information can be shared and used. The Statewide Consumer Directory is essentially a Software Development Kit (SDK) with a robust set of APIs that can be used by consumer-facing applications that enable consumers to take an active role in viewing and editing their preferences for how their health information is shared.

Transactional Basis. The transmission of message content or a notice within a period of time of receiving message content or notice from a sending or receiving party as may be further set forth in a specific exhibit.

Transitions of Care. The movement of a patient from one setting of care (e.g. hospital, ambulatory primary care practice, ambulatory specialty care practice, long-term care, rehabilitation facility) to another setting of care and can include transfers within a healthcare organization.

Trusted Data Sharing Organization (TDSO). An organization that has signed any form of agreement with MiHIN for data sharing.

Use Case. (a) A use case agreement previously executed by a participating organization; or (b) the use case summary, use case exhibit and a use case implementation guide that participating organization or TDSO must follow to share specific message content with the MiHIN.

Use Case Exhibit. The legal agreement attached as an exhibit to the master use case agreement that governs participation in any specific use case.

Use Case Implementation Guide (UCIG). The document providing technical specifications related to message content and transport of message content between participating organization, MiHIN, and other TDSOs. use case implementation guides are made available via URLs in exhibits.

Use Case Summary. The document providing the executive summary, business justification and value proposition of a use case. Use case summaries are provided by MiHIN upon request and via the MiHIN website at www.mihin.org.

View Download Transmit (VDT). A requirement for Meaningful Use with the objective to provide patients with the ability to view online, download and

transmit their health information within a certain period of the information being available to an eligible professional.

XCA. The IHE (Integrating the Healthcare Enterprise®) standard for Cross-Community Access which provides specifications to query and retrieve patient relevant health information held by other communities.

XDS.b. The IHE (Integrating the Healthcare Enterprise®) standard for Cross-Enterprise Document Sharing revision b, which provides specifications to query and retrieve patient relevant healthcare data held within a community.