The Office of the National Coordinator for Health Information Technology

Identity Management

STATE HEALTH IT MODULAR FUNCTIONS FOR VALUE-BASED PAYMENT STRATEGIC IMPLEMENTATION GUIDE

ONC-SIM Health IT Resource Center

Version 1.1

December 6, 2017

Acknowledgements

This report was created by the Office of National Coordinator for Health Information Technology (ONC) State Innovation Model (SIM) Resource Center staff and contractors.

ONC Office of Care Transformation Health IT Resource Center Contributors:

- Robert Cothren, PhD – Contractor, ONC Resource Center (Lead Contributor)
- Kelly Cronin – Director, ONC Office of Care Transformation
- John Rancourt – Deputy Director, ONC Office of Care Transformation
- Terry Bequette – Contractor, ONC Resource Center
- David Kendrick, MD, MPH, FACP, ABPM-CI[1] – Contractor, ONC Resource Center

Office of the National Coordinator for Health Information Technology
U.S. Department of Health and Human Services
300 C Street SW
Washington, DC 20201

[1] University of Oklahoma School of Community Medicine

Executive Summary

Identity management includes all activities related to establishing and verifying the identity of providers, patients, caregivers, and other stakeholders in order to:

1. Control access to health-related information and meet regulatory requirements
2. Link health information with the correct individual
3. Link health outcomes with providers, organizations, and care teams

A learning health system depends on robust identities and linkages, not just security and access control. When coordinated across participating organizations, such as payers and providers in a State Innovation Model, identity management also enables proper care coordination, service delivery, value-based payment, and performance measurement. This guide discusses these critical healthcare use cases in the section on *Use Cases*, and outlines the business and technical requirements that are derived from these use cases in *Business Requirements* and *Technical Requirements*.

Unfortunately, significant challenges exist with meeting identity management needs within healthcare. Issues include defining unique identifiers for both providers and consumers, accurate representation and maintenance of the data fields that define an identity and enable person matching, and a collaborative governance process to implement identity management as a shared service across participating organizations. This guide discusses these challenges in the section on *Challenges in Identity Management in Healthcare*. Many of these issues were the focus of ONC's call-to-action in A Shared Nationwide Interoperability Roadmap,[2] and they continue to be barriers today.

Provider identities are usually managed through provider or healthcare directories, provider registries, credentialing systems, and provider enrollment systems. Patient identities, in turn, are usually managed by a master patient/person index, which maintains consistent, accurate, and current demographic information on individuals seen within an organization. However, an increasingly mobile society requires consistent identities across organizations, and most use cases that support value-based care rely on consistent identities beyond an organization's boundaries. A number of technical standards and initiatives are being explored to allow interoperability among provider directories, enable reliable patient matching across enterprises, and create statewide master patient/person indexes. This guide discusses today's most common technical approaches as partial solutions to identity management and the standards used to implement them in the section on *Technical Approaches* and *Appendix 3: Business Process* and Technical Standards in the appendices.

States may use this guide in developing and implementing an identity management strategy and potential funding opportunities at the state level in *Implementation Guidance*. Critical steps in developing and implementing a strategy might include:

1. Identifying priority use cases from among those listed in the guide
2. Identifying requirements, using those in the guide as a starting point
3. Determining the most appropriate home for the solution
4. Evaluating the maturity of processes across all collaborating organizations

[2] ONC's A Shared Nationwide Interoperability Roadmap identifies actions and roles that stakeholders should perform to make immediate progress and impacts with respect to interoperability.

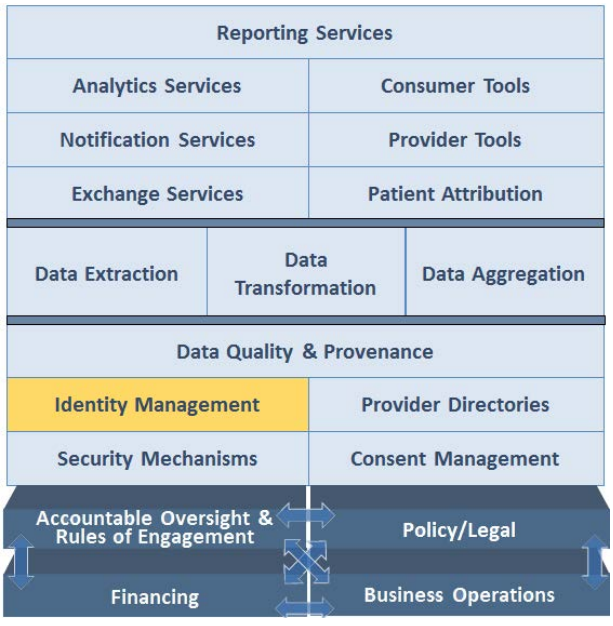
5. Establishing implementation goals
6. Implementing policy levers to promote adoption
7. Continuously adjusting as necessary

What is ultimately required is not simply a technical system for patient or provider identity management supported by technical standards but a master data management approach that includes processes, governance, policies, and operational standards. The guide introduces important data and information governance tools to be used as a model. There is significant value in implementing identity/master data management as a shared service to reduce individual organizational burden as value-based payment is implemented across payers and providers. This guide also briefly discusses funding options for identity management initiatives.

Finally, the guide includes specific case studies in the appendix on *Appendix 2*: Case Studies that illustrate some key approaches, successes, and lessons learned in implementing an identity management strategy.

About the Implementation Guide

The following diagram illustrates the core functionalities and foundational operational elements needed to support value-based payment models. Multi-payer alignment and shared use of the appropriate health IT functionalities can result in cost savings, enhanced efficiency through standardization, and an opportunity for shared governance for participating state agencies, payers, providers, and other healthcare stakeholders.



The ONC Health IT Resource Center provides technical assistance to CMS, State Innovation Model[3] (SIM) states, All-Payer Model States[4], and Medicaid Innovation Accelerator Program[5] (IAP) states. The Resource Center has undertaken a series of Learning Events and Affinity Groups on specific health IT topics, including provider directories and identity management. Informed by the discussions, this guide has collected and distilled available information into strategic and tactical guidance that can assist states in planning, procurement, and implementation of an identity management strategy. ONC has also published strategic implementation guides for Provider Directories[6] and Health IT-Enabled Quality Measurement.[7] Additional state guides are forthcoming.

3 See the State Innovation Models Initiative for general information on the SIM program.
4 Summaries of the All-Payer Models are available for in Maryland, Pennsylvania, and Vermont.
5 See the Medicaid Innovation Accelerator Program for an overview of the IAP program.
6 State Health IT Modular Functions for Value-Based Payment Strategic Implementation Guide Provider Directories
7 ONC SIM Health IT Resource Center Health IT-Enabled Quality Measurement Strategic Implementation Guide

Version History

Version	Date	Description
1	May 23, 2017	Initial release to State Innovation Model states
1.1	December 6, 2017	Full public release

TABLE OF CONTENTS

Purpose of the Identity Management State Guide

As value-based payment models expand, the success and progress of delivery system and payment reforms will depend on many factors, including enhanced care models, improved patient engagement, properly designed financial incentives, and the ability to share and access data. These activities all rely on access to reliable information on the identity of individuals, the association of health information with the correct individual, the association of providers with the consumers they serve, and the organizational affiliations of individual providers – all components of successful identity management.

This guide offers an overview of identity management within the healthcare domain, and provides helpful information to support achieving an operational and sustainable management strategy that enables value-based payment models. The guide is intentionally short, covering key topics at a high level. Links to other, more detailed information are included in footnotes and appendices. The ONC Resource Center has established a resource repository on HealthIT.gov where many of these documents are available.

The 21st Century Cures Act (Cures Act), which became law on December 13, 2016, identified patient identity management as a priority to "ensure appropriate patient matching to protect patient privacy and security with respect to electronic health records and the exchange of electronic health information."[8] It calls on the U.S. Government Accountability Office (GAO) to conduct a study on the topic.

The Cures Act also calls for ONC to "convene appropriate public and private stakeholders to develop or support a trusted exchange framework for trust policies and practices and for a common agreement for exchange between health information networks" that includes "a common method for authenticating trusted health information network participants."[9]

States should apply the advice in this guide to make progress on identity management, while planning for and aligning with the national efforts whenever possible. ONC will continue to communicate to states and other stakeholders the identity management requirements that will support nationwide alignment as they are identified.

Definition of Identity Management

Within the Information Technology Industry

Identity management can be defined as a broad discipline that establishes the identity of individuals within a system (an enterprise, a network, a device, or a software application) in order to control access to resources based on the rights and restrictions associated with that identity. "Identity management systems store attributes associated with users and employ these attributes to facilitate authorization."[10]

8 21st Century Cures Act, Section 4007

9 21st Century Cures Act, Section 4003

10 Birrell, Eleanor, and Fred B. Schneider. Federated Identity Management Systems: A Privacy-Based Characterization. IEEE Security and Privacy. September/October 2013

It addresses the need to ensure appropriate access to resources across increasingly heterogeneous technology environments and to meet increasingly rigorous compliance requirements.

Within the Healthcare Ecosystem

Within the health IT industry, identity management:

1. Establishes the identity of providers, patients, caregivers, and other stakeholders in order to control access to health-related information and meet regulatory requirements
2. Attempts to link health information associated with an encounter or other health-related event with the correct individual identity to create a longitudinal view of the individual's health record or enable care coordination, including notification of health events across and among healthcare delivery enterprises
3. Attempts to link health information, in this case including health outcomes, with provider identities and care team definitions in order to enable performance measurement and value-based payment models

Identity management addresses issues such as how users gain a verifiable identity (e.g., identity proofing, provisioning of access credentials), the protection of that identity (e.g., passwords and other authentication mechanisms, protecting passwords or other security tokens), and the technologies supporting that protection (e.g., network protocols, digital certificates, other access tokens). Authorization, which is often tied explicitly to identity management, addresses permissions granted to access systems and the information they hold based on verifiable identity.

Identity management is also closely linked to a number of other considerations critical to healthcare: processes and technologies for provisioning access to information systems, processes for de-provisioning or revoking access, protection of information privacy, security and privacy of information on mobile devices, and security and privacy of information stored in cloud-based systems. These topics are beyond the scope of this guide, but the considerations and guidance here should be part of the larger privacy and security analysis that encompasses these topics. [11] [12] [13]

Requirements for Effective Identity Management

Identity management should be a fundamental part of every information security program. Good identity management reduces the risk of inappropriate access to resources and information, inappropriate association of information to consumers, and inappropriate attribution of information, relationships, or activities to providers. Enterprises that develop mature identity management capabilities can reduce identity management costs while at the same time reducing security risk. They

[11] A Shared Nationwide Interoperability Roadmap version 1.0 provides a comprehensive discussion of verifiable identity and authentication, security, and privacy.

[12] NIST Special Publication 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

[13] ONC developed three fact sheets with the Office for Civil Rights giving examples of when electronic health information can be exchanged, including Exchange for Treatment, Exchange for Public Health Activities, and Exchange for Health Care Operations.

can also become significantly more agile in supporting new business initiatives. This may be especially true for healthcare organizations wishing to be more effective in care coordination and participating in value-based payment models. However, to be successful, enterprises undertaking identity management must understand the underlying business requirements and processes, as well as the technical approaches and solutions for identity management.

Use Cases

The following is an exploration of the characteristics of identity management associated with some of the major use cases in healthcare and value-based payment models. They provide some insight into major business and technical requirements.

Use cases for identity management within the healthcare ecosystem can perhaps be separated into two overarching categories:

1. Those associated with identity management and access management, more closely identified with a traditional IT definition of identity management
2. Those associated with linking health information to the appropriate individual that is a specific concern of healthcare

The following discussion is separated into these two distinct, but related, categories.

Health Information Access Management

Strong identity proofing and authentication controls increase confidence and assurance in the validity of the identity of an individual or organization, and provide greater protection from unauthorized access to system resources, including health-related information. Identity proofing and authentication are the first line of security defense at both the provider and organizational level and have the potential to be the weakest link in the security chain, as they are the primary control which opens the door to access management on which many aspects of security rely.

Strong identity proofing and authentication are the first line of security defense and have the potential to be the weakest link in the security chain.

Health Information Access by Providers

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule requires that an individual or entity accessing protected health information (PHI) electronically be authenticated before such access is granted. Although the Rule does not mandate a specific framework or specify how to implement the standard, it does require that each covered entity "conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate"[14] and to then "implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level."[15] NIST publications are a source of commonly accepted standards across the federal government for security and technical specifications guidance. With specific reference to the Security

[14] 45 C.F.R. §164.308 (a)(1)(ii)(A)
[15] 45 C.F.R. §164.308 (a)(1)(ii)(B)

Rule, the NIST Cybersecurity Framework,[16] is widely adopted guidance by organizations seeking to establish a risk management program.[17]

Rather than granting access based on identity, many systems, including healthcare systems, provide access to system resources and information based on the role of the individual requesting access and the purpose for which the information is being retrieved. The same individual may fill different roles at different times, on different systems, or for different patients. Therefore, it is necessary to unambiguously establish and maintain the roles appropriate to individuals, and a means for individuals to assert a role and purpose-for-use as a right to access resources such as health information.

Health Information Access by Individuals, Family Members, and Caregivers

The need for identity proofing and strong authentication does not end with individual providers or provider organizations. It is likewise necessary to identity-proof consumers to allow them to access their own health information electronically. There is likewise a growing desire by consumers to grant their family members and caregivers access to their health information, extending the scope for identity proofing and the need to establish and easily maintain relationships among consumers, their family members that should be granted access, and their caregivers.

Non-Repudiation

Broadly, non-repudiation is the assurance that someone cannot deny the authorship or validity of information. Non-repudiation requires strong identity proofing and strong authentication that can be used to assert the genuine origin of information with high assurance. It also requires a strong and irrefutable means to associate information with an individual or organization. This is often accomplished through digital signatures.

Associating Health Information or Care Delivery with an Individual or Provider

Care Coordination Management

According to the Agency for Healthcare Research and Quality (AHRQ), "care coordination involves deliberately organizing patient care activities and sharing information among all of the participants concerned with a patient's care to achieve safer and more effective care."[18] This process is essential for providers operating under value-based payment models as they are seeking to achieve more effective care through improved quality and reduced cost.

Care coordination activities require identity management[19] of both providers and health consumers for a number of reasons:

1. An individual's health information must be associated with the correct individual identity across the care continuum: within an enterprise and across enterprise boundaries

---

16 See the NIST Cybersecurity Framework for more information.

17 See Cyber Security Guidance Material on the HHS.gov web site for more information.

18 For more information, see Care Coordination on the web site of the Agency of Healthcare Research and Quality.

19 The case study of the *Utah Community Solution for Identity Management* in *Appendix 2: Case Studies* describes a coordinated approach to consumer identity for the primary purpose of care coordination.

2. Consent or consumer preferences to share information with providers electronically must allow systems to associate an individual's information and identity with the consent or preferences asserted by the individual and the provider identities involved in their care and named in consent documents and assertions
3. Providers and healthcare systems must be able to identify providers that are members of the individual's care team in order to alert them of important care events and provide them with access to the associated encounter information, as well as to allow aggregation of individual consumer health information from these different sources into a shared care plan

While many enterprises – hospital systems, integrated delivery networks, state health and non-health programs, and even some health information exchanges (HIEs) – create and may share an enterprise-wide individual identifier, they are not universally unique and often not shared outside of the enterprise. The lack of a shared nationwide patient identity results in a requirement for robust algorithms to perform individual identity matching based on demographics.

Attribution Management for Service Delivery and Payment

It is critical to link providers to the individuals for which they are providing care in order to provide appropriate access to health information for service delivery and payment. However, there often exist gaps in accurate and verified association of providers to patients; the association may not be identified and recorded, for example, during registration. Instead, many systems allow the provider to assert a patient relationship and through that assertion grant access to the patient's health information.

All value-based payment models incorporate financial incentives for positive outcomes for populations associated with provider entities participating in the model. A key element of operating a value-based payment model is accurately attributing patients to providers. Attribution is important to payment operations, as well as to ensuring that providers understand cost and quality results for patient populations. Examples include shared savings in a total cost of care model or achievement of quality milestones over the course of a performance period. Attribution is the process of associating individuals with the defined provider entities participating in the value-based payment model. This is usually performed by applying a sequence of decision-making rules to information about individuals, either prospectively or retrospectively.

Since multiple data sources may be accessed to complete attribution, processes must be in place to ensure that claims, financial, clinical, and other data are accurately associated with the correct individual, while avoiding errors of omission or of erroneous inclusion. Identity must be resolved across these multiple sources. Complications arise when multiple patient and/or provider identities are involved due to enterprise boundaries or when value-based payment models overlap to contend for the same patient encounters to be assigned to different models. A secondary concern is confirming the identity of the provider entity across the various data sources used for attribution. Identity management and a provider directory are usually used together to accomplish attribution.

A variety of models may be used to establish attribution, including frequency of visits, specific events or procedures, or specific assignments. Attribution models may need to be customized in order to address the needs of primary versus specialty care, and multiple models may be needed for different initiatives and performance metrics. The Health Care Payment Learning & Action Network (LAN), which was

created to drive alignment in payment approaches across the public and private sectors, provides a white paper with general recommendations guiding the patient attribution process.[20]

Both the *Michigan Health Information Network Shared Services* (MiHIN) and the *MyHealth Access Network* solutions for identity management described in *Appendix 2: Case Studies* concentrate on attribution for service delivery as well as for performance measurement. The MiHIN model for attribution utilizes what it terms "physician-centric attribution" that focuses on self-reported relationships between providers and consumers, obtained either from physicians who indicate active patients or from individuals who indicate their healthcare providers. MyHealth Access Network, on the other hand, uses information obtained through patient encounters with providers, the relationship of individual providers to their organization, the location of the encounter, and the reason for the encounter as most relevant in making decisions to attribute an individual to a provider.

While not called out in this analysis as a separate use case, the processes put in place for health information access management, non-repudiation, care coordination management, and attribution management all require information that is also valuable for the detection and investigation of healthcare payment fraud and abuse. For example, these processes define robust provider identities across multiple care settings, appropriate provider-consumer relationships, provider-organization affiliations, and appropriate service delivery.

Performance Measurement

Performance measurements calculated for purposes of value-based payment must be determined based on data attributed to a provider or provider organization. This is complicated in multi-payer models, since the necessary data may reside in multiple clinical systems as well as multiple claims and other databases. Patient identities must therefore be resolved across all organizations in any attribution model that relies on more than self-reported information.

> Identity must be resolved across all organizations in any attribution model.

Consider for example a consumer seeing several providers, all of whom are reporting blood pressure. A single payer assessing performance on blood pressure control may receive values from providers both within and outside of the plan. Some measurements may show good control of hypertension while others indicate unsatisfactorily-elevated blood pressure. Some values may be for the patient in question and others for a different patient with similar demographics. An effective identity management process can confirm the measurements belonging to a single individual, and the appropriate credit for that individual can be given to all of the providers that the individual sees.

Business Requirements

Based on the use cases above, the following business requirements can be developed.

Requirements for access management

1. Identity proofing for individual providers
2. Identification and management of individual provider roles
3. Identity validation for organizations

[20] Accelerating and Aligning Population-Based Payment Models: Patient Attribution published by the Health Care Payment Learning & Action Network

4. Identity proofing for consumers
5. Identification and management of consumer relationships to family members and caregivers
6. Processes for issuing and managing digital credentials for providers and provider organizations
7. Processes for issuing and managing digital credentials for consumers

In addition to these requirements for access management, there are additional requirements that apply to other categories: non-repudiation, care coordination, provider-patient attribution, and quality measurement.

Additional requirements for non-repudiation

8. Processes for issuing and managing digital signatures for providers and provider organizations

Additional requirements for care coordination management

9. Identification and management of patient/provider relationships
10. Processes for collecting, validating, and storing provider information

Additional requirements for attribution management

11. Processes for allocating patient encounters to the appropriate value-based payment model

Additional requirements for performance measurement

12. Processes to associate performance (processes and outcomes) with providers and provider organizations

Technical Requirements

The above discussion might suggest the following technical requirements for identity management.

Requirements for access management

1. Digital credentials for providers
2. Digital credentials for provider organizations
3. Digital credentials for consumers
4. Strong access, authentication, and authorization mechanisms for providers
5. Communication of access rights, including identity, role, and purpose

Likewise, there are additional technical requirements for non-repudiation, care coordination, provider-patient attribution, and quality measurement.

Additional requirements for non-repudiation

6. Mechanisms for validating digital signatures
7. Mechanisms for tracking information provenance

Additional requirements for care coordination management

8. Mechanisms for representing and communicating patient/provider relationships
9. Robust algorithms to match patients
10. Directories of provider information

Additional requirements for attribution management

11. Mechanisms for representing and communicating the members of care teams

Additional requirements for performance measurement

12. Mechanisms for communicating information provenance

What becomes clear from the above brief analysis is that the business and technical requirements for identity management in the healthcare setting are complex, and the requirements to support a value-based payment model go far beyond the requirements of identity management in the traditional IT setting. Fortunately, requirements to support value-based payment models and performance measurement build upon the requirements of other use cases, allowing organizations seeking to use value-based payment models to build upon the work already set in motion to support robust access management and care coordination.

Requirements to support a value-based payment model go far beyond those of access management in the traditional IT setting.

Any procurement for an identity management solution will require a more extensive requirements analysis.[21]

Challenges in Identity Management in Healthcare

There are a number of challenges associated with meeting the needs of identity management in the healthcare setting. These challenges present barriers to the implementation of value-based payment models or can compromise the underlying attribution and performance measurements needed to support the models.

Issues with Unique Identifiers

Identifiers for Providers

The Administrative Simplification provisions of HIPAA[22] mandated the adoption of standard, unique identifiers for healthcare providers. The Centers for Medicare & Medicaid Services (CMS) developed the National Plan and Provider Enumeration System (NPPES) to assign these unique identifiers, and established the National Provider Identifier (NPI) as a unique identifier number issued to healthcare providers in the United States. Individual providers may have only a single NPI, and therefore the number can function as a universal provider identifier.

However, many individuals associated with care may not have applied for and been issued NPIs.[23] Furthermore, healthcare organizations often have multiple NPIs,[24] making the use of the NPI as a unique

---

21 As described in *Proposed Solutions* below, identity management solutions often include a master patient/person index or MPI. An example of more detailed requirements for an MPI is included in the case study for *MyHealth Access Network* described in *Appendix 2: Case Studies*.

22 45 C.F.R. Part 162 HIPAA Administrative Simplification: Standard Unique Health Identifier for Health Care Providers; Final Rule

23 Under the National Provider Identifier Regulation, only healthcare providers who are covered entities as defined in 45 C.F.R. § 160.103 and who transmit health information electronically using HIPAA standard transactions are required to obtain an NPI.

24 Under the National Provider Identifier Regulation, organizational providers are allowed multiple NPI numbers for subparts.

organizational identifier difficult or impossible. Also, providers often use their organization's NPI instead of their individual NPI, resulting in multiple providers using a single organizational NPI.

Identifiers for Consumers

In the United States, every healthcare setting establishes its own identifier for consumers, often referred to as a medical record number or MRN. Multiple MRNs, that is an individual's multiple identities across multiple healthcare settings, are linked by deterministic or probabilistic algorithms for matching demographic information. Manual processes are typically also used for identities that cannot be matched via algorithms, or as a means to supplement algorithms. The lack of standardized data capture processes, and the lack of adherence to standardized data elements, data encoding, and data formats associated with demographic information make algorithmic matching very difficult.

This issue has long been described as a difficulty in HIE and care coordination. For value-based payment model purposes, the clinical and claims data about an individual that is needed to calculate performance measures and incentive payments likewise may reside in multiple repositories, and is subject to the same identity matching challenges as HIE and care coordination.

Information Inaccuracy

Provider Information

Even if the NPI serves as a unique identifier for individual providers, other information about the provider is of primary importance for care coordination management, attribution, or performance measurement. This includes organizational affiliations, services, locations, roles, and plan participation, and electronic endpoints (e.g., Direct address or web service addresses to query for health information). Current directories of provider information, including but not limited to NPPES, suffer greatly from inaccuracies or incompleteness in these data elements that make their use unreliable.

Even if information is entered correctly, addresses and telephone numbers change, care teams change, and providers change their association with provider organizations and care delivery locations. There are few reliable business processes that *continually* update provider information to ensure its accuracy. Credentialing, for example, provides an accurate recording of provider information at a single snapshot in time. Existing business processes generally result in infrequent checks that may not accurately reflect changes in provider information. Anecdotal reports from health plans suggest that changes to provider information is reported on average at least twice a year, and "secret-shopper" studies suggest that many changes go undiscovered because no business process exists to capture those changes.[25]

Consumer Information

Local patient identities assigned by different healthcare entities in different care settings are usually consolidated through matching based on demographic information. However, such demographic information is often incomplete or inaccurate. Information is usually entered manually and is not validated within the care setting.

---

[25] Simon Haeder, David Weimer, Dana Mukamel, Secret Shoppers Find Access To Providers And Network Accuracy Lacking For Those In Marketplace And Commercial Plans published in Health Affairs 35:7 (not free) and summarized in a posting on Affordable Health California.

As with provider information, there are few reliable business processes that *continually* update consumer information to ensure its accuracy. Information entered during registration – the most common process for entering or confirming patient demographics – is too often inaccurate.[26] Many systems that record demographic information for consumers fail to record and take into account historical information that may be useful in matching identities across enterprise boundaries or even modest spans of time to measure performance, establish appropriate service delivery, or detect and investigate fraud or abuse. Consumers seeking care from multiple providers may report a change to demographics at one location, but there often exists no process to propagate that change to other providers, resulting in demographic differences that may thwart even the best matching algorithms.

As a result, even the best matching algorithms will at times fail,[27] requiring the manual reconciliation of match failures and inappropriate matches resulting from failed automatic algorithms. Both Type I and Type II errors[28] in these systems present a safety risk, as health information electronically available during care delivery is not retrievable, or incorrect health information is associated with the individual and used erroneously. They also contribute to missed opportunities in provider alerting and care coordination, resulting in poorer outcomes and lower overall care quality. Medical identity theft – the theft of personal information to obtain medical care, buy drugs, or submit fake billings – can further cause incorrect health information to be associated with the consumer whose identity was stolen.

The description of the *Utah Community Solution for Identity Management* in *Appendix 2: Case Studies* describes an approach to coordinated improvement of data quality and the impact it had on successful consumer identity management. Likewise, the approach to consumer identity management at *MyHealth Access Network* in *Appendix 2: Case Studies* describes a master data management approach that incorporates processes and governance and emphasizes transparency in matching solutions, all to address data quality.

Lack of Adoption of Uniform Information Standards

The representation of demographic information and the use of controlled terminologies is inconsistent in both provider and consumer information. The 2017 Interoperability Standards Advisory (ISA)[29] identifies HL7 v2.5.1 ADT (Admit, Discharge, Transfer) messages as a mature, widely adopted standard that includes a significant amount of information on individual consumer identity through demographics and other information. However, it also points out that Integrating the Healthcare Enterprise[30] (IHE) profiles, such as the Patient Identifier Cross-Reference and Patient Demographic Query (PIX/PDQ) and

---

26 Incorrect registration data is a significant patient safety worry: Multiple patients have been harmed, according to recent report

27 Managing the Integrity of Patient Identity in Health Information Exchange updated in 2014

28 Type I errors, or false negatives, are failures to link records that actually belong to the same individual. Type II errors, or false positives, are inappropriate linkages of records that appear to belong to the same individual, but do not.

29 ONC's Interoperability Standards Advisory is a process to coordinate identification, assessment, and public awareness of best-available interoperability standards and implementation specifications that can be used to address specific interoperability needs.

30 IHE is an industry initiative to improve the way systems in healthcare share information by constraining how standards are used through "profiles" that address specific use cases.

Cross-Community Patient Discovery (XCPD),[31] are used to support patient matching in queries for health information, not ADTs. These standards contain much less information than an ADT with fewer constraints on data element representation or terminology. Additionally, the ISA lists the IHE Healthcare Provider Directory (HPD)[32] profile for provider directories. However, few have adopted it.

The representation of demographic information is inconsistent in both provider and consumer information due to a lack of uniform data standards for items as simple as family name or complex as a practice address, and terminologies as simple as gender or complex as specialty and sub-specialty. When organizations must establish a shared understanding of a single consumer or provider identity based on communication of demographic information, standards for how that information is encoded and communicated must be established and applied uniformly. Fast Healthcare Interoperability Resources (FHIR)[33] may address some of these limitations, but the ISA notes that FHIR remains an emerging standard in many areas and is not yet widely adopted.

Interoperability Roadmap Call-to-Action

The Interoperability Roadmap[34] has much to say about several aspects of identity management. It identifies identity management "as a privacy and security issue," and calls for the following to improve identity management:

- Ensure that data elements for individual identity matching are standardized, consistently captured, and shared
- Document evidence-based best practices for individual identity matching processes, data quality, and matching technology
- Advance the use of industry-recognized data definition and data normalization standards
- Adopt uniform standards and best practices for capturing and matching health-related data
- Consistently include the data elements for individual identity matching in exchange transactions
- Implement a uniform approach to individual identity matching and performance measurement that is informed by the best practices
- Advance standards for primary, secondary, and voluntary data elements, including the use of unique identifiers and biometrics

The Interoperability Roadmap notes that "as a learning health system evolves, more than individual/patient-specific information from health records will be matched and linked, including provider identities, system identities, device identities and others to support public health and clinical research,"[34] greatly expanding the IT focus of identity management on access control.

> The needs of a learning health system for robust identities and linkages greatly expand upon the IT focus of identity management on access control.

---

31 See *Standards for Matching Patient Identities* in *Appendix 3: Business Process and Technical Standards* for a description of the PIX/PDQ and XCPD profile.

32 See *Standards for Managing Provider Identities* in *Appendix 3: Business Process and Technical Standards* for a description of the HPD profile.

33 See *Standards for Managing Provider Identities* and in *Appendix 3: Business Process and Technical Standards* for a description of the FHIR standard.

34 A Shared Nationwide Interoperability Roadmap version 1.0

The Interoperability Roadmap also states that "there is a significant near-term need to focus on identity matching for clinical care, so that patients can receive safe and effective care at every point of care. However, there is a long-term need to consistently and accurately match individual data for public health purposes to support investigation and to also support research and administrative claims processing and payment." [34]

Proposed Solutions

The vision for identity management is that of a healthcare ecosystem characterized by accurate and attributable identities wherever they are reflected in systems, indexes, and repositories. Mechanisms supported by governance, accountable oversight, and rules of engagement resolve identity questions as they arise.

A master data management approach to identity management is required – considering more than just technical systems, but also processes, governance, policies and standards.

What is ultimately required is a master data management approach to identity management – that is, not only a technical system, but the processes, governance, policies, and standards to establish a consistent reference identity for individuals, the data attributed to them, the identity of providers, provider membership in organizations, and patients attributed to them. Both the *Utah Community Solution for Identity Management* and *MyHealth Access Network* approach to the master patient/person index (MPI) described in *Appendix 2: Case Studies* emphasize the need for processes, governance, and data standards as part of the identity management solution.

While the healthcare industry is still working to achieve this vision, approaches to partial solutions to the challenges above do exist. The following partial solutions for identity management follow recommended standards and best practices.

Technical Approaches

Registries and Indexes

The primary approach to a common representation of provider or patient identity given multiple identifiers within an enterprise, and sometimes even across enterprises, is through the use of registries and indexes.

Provider Registries

Provider identities are usually managed through provider or healthcare directories or provider registries.[35] Provider directories allow information on individual providers, including identifying information, address and telephone numbers, credentials, practice specialty and other details, organizational affiliations, and available communication means, including HIE, to be collected, managed,

[35] Within this guide, a directory and registry are differentiated only in that a directory catalogs information about individuals or organizations without specifying the source, and a registry is created through the positive attestation of individuals or organizations, often in response to business or regulatory requirements.

and even made searchable electronically. Provider directories are also beginning to include information on provider organizations and even plans and plan participation. A number of standards are available that describe potential data models and interfaces to provider directories, most notably including X12 274,[36] HPD,[37] and FHIR[38] described briefly in *Appendix 3: Business Process and Technical Standards*.

Different models have been explored for exchanging information in provider directories. Directories may be created as statewide resources, sometimes extracting some information from NPPES as the authority for NPIs. A few examples of statewide provider directories are in operation or under development today, including those in Michigan,[39] New York, Oregon, and Rhode Island. Some directories follow a federated architecture, allowing regional or specialty organizations to take responsibility for subsets of providers and distributing the responsibility for data integrity. Until recently, California operated a federated solution, and New York currently operates one. Some directories are exchanged as flat files between or among cooperating organizations that may have reached consensus on a "standardized" format to the file, with DirectTrust[40] operating the most extensive coordinated directory exchange of this type.

ONC has established a HealthCare Directory Technology Learning Community (TLC)[41] to leverage stakeholder expertise to drive the development and interoperability of healthcare directories, a superset of "traditional" provider registries. The TLC is one outlet for the work products of four "Tiger Teams" convened by ONC to explore a potential national resource of validated provider information. The Tiger Teams have the following goals:

1. Use Cases Tiger Team: Define a key set of use cases for healthcare directories and prioritize those uses cases in a suggested order of implementation
2. Data Elements Tiger Team: Define the data elements required to meet the needs of the healthcare directories
3. Architecture Tiger Team: Define a proposed national architecture for the exchange of core and use case-specific data between a national resource of validated information and local environments
4. Interoperability Standards Tiger Team: Develop a national standard and implementation guide for the exchange of core and use case-specific data elements between a national resource and local environments using FHIR

---

36 Accredited Standards Committee X12 274 Healthcare Provider Directory (004050X109)

37 IHE IT Infrastructure Technical Framework Supplement on Healthcare Provider Directory (HPD) Trial Implementation version 1.5

38 FHIR (Fast Health Interoperability Resources) Release 3 (STU)

39 *Michigan Health Information Network Shared Services* described in *Appendix 2: Case Studies* has implemented a solution for a provider directory that, when coupled to its patient index, provides solutions for care coordination, alerts, and provider-patient attribution.

40 DirectTrust is a non-profit association of organizations supporting secure health information exchange via Direct messaging, and coordinates the exchange of individual provider names and Direct addresses via standardized file format.

41 See the ONC Healthcare Directory Technology Learning Community (HcDir TLC) for information on its virtual meetings.

If successful, this initiative will help address some of the key issues surrounding provider directories, most notably information accuracy and volatility, by establishing a validated resource of core provider information, processes to validate that information, and standards to access it.

Provider directories or registries are often included in master data management solutions offered by a number of companies. In addition, there are vendors that offer specific provider directory solutions.

Related to provider registries, some states including Oregon and Washington have legislation to implement common credentialing systems that associate provider identities with their credentials. Additionally, 12 states and the District of Columbia have adopted a specific collection instrument developed by the Council for Affordable Quality Healthcare[42] (CAQH) to collect professional and practice information for state credentialing.[43]

Patient Indexes

The primary tool for managing patient identities is a master patient/person index (MPI) or enterprise master patient/person index (eMPI). The MPI is used across a healthcare organization to maintain consistent, accurate, and current demographic information on the individuals seen within the organization and managed within its various, perhaps disparate, information systems. Most MPIs assign each individual a unique identifier that is used to refer to the individual across the enterprise, together with local identifiers (MRNs) that may be issued by the various systems within the enterprise. The objective is to ensure that each individual is represented only once across all software systems. Patient information usually includes name, gender, date of birth, race and ethnicity, and current address and contact information. It may also include social security number, license number, and insurance information.[44]

An MPI is designed to create a single, authoritative, and consistent location for individual patient identity within an enterprise. Patient identities are usually created during admission or registration, and then communicated to other systems through HL7 ADT messages. Most MPIs obtain the information they use from these ADT messages emitted by electronic health records (EHRs) and other healthcare systems, and manage a single identity across a hospital system, integrated delivery system, or community.

When MPIs are created to facilitate care coordination, consistent identity within an enterprise or community may be sufficient. However, our increasingly mobile society is demonstrating the need to exchange health information consistently and securely beyond organizational boundaries. Creating a consistent identity across organizations is more problematic, as patient matching must be accomplished without the rich source of information provided by the ADT message. For this reason, several states have chosen to organize a statewide MPI to coordinate identities across multiple communities rather

---

42 CAQH is a non-profit alliance of health plans and trade associations that, in its ProView provider data source product, provides a resource for self-reporting professional and practice information to health plans and other healthcare organizations.

43 Testimony Provided to the Subcommittee on Standards, National Committee on Vital and Health Statistics by CAQH, November 19,2011

44 Patient Identification and Matching: Final Report

than relying on a patchwork of MPIs of regional HIEs.[45] Further, most use cases that support value-based care (for example, population health management) rely on consistent identity of patients beyond enterprise boundaries. Cross-organizational identity is therefore a pre-requisite to scaling health IT services for value-based care.

There is no consistent data model for MPIs, and several proprietary solutions exist. MPIs establish individual identities and return information on individuals using deterministic or probabilistic algorithms that match demographic information. Such algorithms are imperfect, requiring enterprises and HIEs to expend significant effort merging identities not matched automatically by the MPI and unmerging identities that were matched automatically in error. Appropriate MPI strategies and solutions must include two critical components:

1. Initial effort during implementation to appropriately set matching algorithm parameters for the demographics present in the population for which the MPI is being developed
2. Ongoing effort during operation to manually merge failures to associate matching identities automatically, and manually unmerge inappropriate associations of different identities

A cross-reference manager is a specific type of MPI that collects local identifiers, such as the MRNs assigned by EHRs, and associates them with a single individual's identity. In this case, the master identifier for the individual is usually not discoverable publicly. Instead, a successful query for a patient identity returns the various local identifiers along with the systems that use them. The PIX/PDQ standard described in *Appendix 3: Business Process and Technical Standards* is an example of a cross-reference manager solution relatively common among EHR implementations.

Most EHR and HIE technology vendors offer MPI solutions as part of their product. Many can also include third-party solutions from vendors.

Peer-to-Peer Based Approaches

Some networks manage patient identities through peer-to-peer matching schemes rather than any centralized MPI or other index or registry. In the peer-to-peer approach, a requesting organization sends demographic information for an individual to a responding organization, requesting potential matches based on that information. The responding organization searches for matches, probably through its own MPI, and returns zero, one, or perhaps more potential matches along with the demographic information it has for each match and a unique identifier within its system (e.g., within its MPI). The requesting system can then investigate the results to determine if it agrees on a match, probably using the algorithms in its own MPI.

XCPD described in *Appendix 3: Business Process and Technical Standards* is the most common technical standard that implements a peer-to-peer based approach to patient matching, which is in turn used by the eHealth Exchange and Carequality national exchange initiatives.[46]

---

[45] See the case study on the *New York eHealth Collaborative* in *Appendix 2: Case Studies* for a discussion of a federated example of a statewide MPI.

[46] See The Sequoia Project for more information on eHealth Exchange and Carequality.

Big-Data Solutions

MPI solutions are plagued by incomplete or outdated information that results in missed opportunities for patient matches. For example, two systems may have slightly different versions of an individual's name, gender, and date of birth that lead to an ambiguous match. One may also have an address but no telephone number, while the other has a telephone number but no address. Or one may have a current address and the other a previous address. In many cases, opportunities for appropriate patient matches will be missed.

Significant increases in successful matches have been observed using big-data approaches to identity matching.

An alternative approach is to use a larger set of publicly available information that includes names, aliases or common alternative names the person may have used, current and previous addresses, current and previous telephone numbers, and perhaps even other less common information. Each of the systems above would then match against this larger data set, enabling a match.

A few vendors make big-data solutions like this available today, and a few organizations have employed them with good results. For example, San Diego Health Connect[47] has observed and documented significant increases in successful individual identity matches using a big-data approach to identity matching.

Policy and Practice Guidance

There are several policy and practice guidance areas that should be considered when addressing identity management.

NIST Guidance

NIST has published guidance for the level of assurance[48] both when identity proofing providers for issuing credentials as well as for authenticating providers using health information systems and consumers accessing their health information. This guidance should be reviewed and, as appropriate, referenced or incorporated into the policies and procedures for identity management for access control in healthcare systems.

Guidance for Provider Directories

Most state regulations do not consider the information contained in provider directories to fall under protections for personally identifiable information if it is limited to publicly-available information provided for business purposes. Despite this fact, many providers consider information in a provider directory "sensitive" and are reluctant to have it shared broadly. Care should be taken in publishing provider directory information for anonymous access.

Some states have initiated policies that only allow controlled and authorized access to provider directories,[49] perhaps limited to organizations of a particular type or with a limited and specified

---

47 See San Diego Health Connect Community News or the CAHIE Knowledge Network presentation for more information about San Diego Health Connect's use of Verado technology in patient matching.

48 See NIST Special Publication 800-63-2 Electronic Authentication Guideline, and NIST Special Publication 800-63-3 Digital Identity Guidelines which superseded 800-63-2.

49 For example, contact MiHIN for its policies (not published on the Internet).

purpose for using the provider information. They may also have policies associated with disclosure of provider information obtained from a directory and auditing individual access to allow for the investigation of inappropriate behavior or policy violation. The Western States Consortium published a paper[50] outlining some of the considerations for policies for sharing provider information which California used in establishing policies for its federated provider directory.

State Policies and Guidance

Some states have used policy, regulation, or legislation to address issues concerning identity management. For example, California State Bill SB-137 "Health care coverage: provider directories," enacted into law in 2015,[51] addresses in part the challenge of accurate provider information by requiring health plans in California and their contracted providers to keep up to date, accurate provider directories online and in printed form. The statute defines information that must be included in the provider directories and sets strict timelines to update information as well as correct misinformation. The law places pressure on health plans by making them reimburse an enrollee who ends up paying for out-of-network service because of inaccurate information, and suggests there may be penalties if there is a lack of communication between health plans and providers. The law also allows health plans to withhold payments to providers that do not comply with the update process. The California Department of Managed Health Care and the Department of Insurance must develop uniform provider directory standards for plans to follow.

States should consider policy levers related to identity management to establish authority or pursue public policy objectives. The ONC Resource Center has developed a State Health IT Policy Lever Compendium[52] that is a useful reference tool for states to consider (specifically policies related to purchasing, credentialing, provider licensure, and other applicable policies).

States should also consider implementing data governance processes to ensure that (1) data associated with identity management are formally managed, (2) data can be trusted, and (3) accountability exists for poor data quality. The resources managed and made accessible by health IT systems should all fall under data governance processes. Likewise, provider and patient identities, which are in turn data assets that allow for information access and control change management, should have defined data governance policies associated with them. Provider directories, provider registry and credentialing systems, MPIs, attribution systems, and other key components of any identity management strategy should be accompanied by a defined data governance structure.

Business Process and Technical Standards

Standard business processes and technologies for identity management fall roughly into those that:

1. Establish or communicate an identity
2. Store and/or communicate information about individuals
3. Match records to a single individual identity

---

50 Western States Consortium ONC State Health Policy Consortium Project Final Report

51 California State Bill SB-137 "Health care coverage: provider directories"

52 State Health IT Policy Lever Compendium

Public key infrastructure (PKI), Security Assertion Markup Language (SAML), and OAuth and OpenID Connect are among the most common standards for establishing or communicating identity. They are used most commonly for establishing provider identities and communicating authentication and/or authorization information, but can be applied to consumers, as well.[53]

The X12 274 Healthcare Provider Information transaction set and the IHE Healthcare Provider Directory (HPD) standards are among the most common for storing and communicating information about either organizational or individual providers, their relationships, and the services they offer. Neither are widely implemented.

HL7 version 2.x ADT messages are the most common standards for communicating information about patients. ADT messages are usually used as input into MPIs, but ADT messages may be inconsistent in the information they transmit and there is no uniform standard for how information in an MPI is stored.

Patient Identifier Cross-Reference (PIX), Patient Demographic Query (PDQ), and Cross-Community Patient Discovery (XCPD) are the most common standards for communicating patient demographic information for the purposes of seeking patient matches. PIX/PDQ is relatively mature and commonly implemented by EHR and HIE solutions within an enterprise setting. XCPD is relatively mature and used by eHealth Exchange and Carequality to seek matches across enterprise boundaries.

HL7 FHIR is an emerging standard that has capabilities for communicating provider and patient information, as well as relationships among providers and consumers, individual provider affiliations, memberships in care teams, and consumer relationships to family members and caregivers. FHIR is not yet widely implemented, but many vendors have expressed a commitment to FHIR as a more granular alternative HL7 v3 for many use cases.

Appendix 3: Business Process and Technical Standards contains a brief overview of technical standards and standard business processes for identity management.

Implementation Guidance

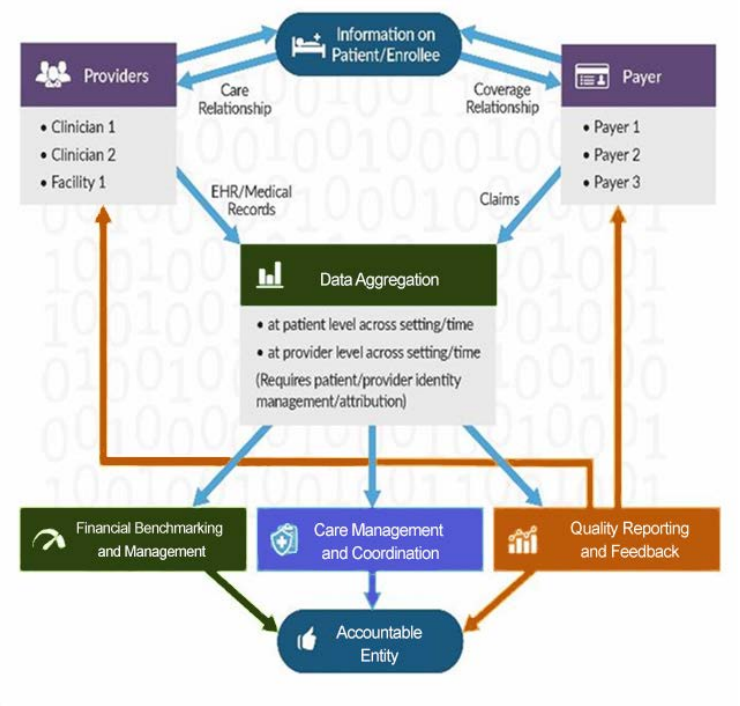
The diagram on the next page from the Data Sharing Requirements Initiative (DSRI) toolkit[54] shows a typical set of partners within a value-based payment model and the associated data flow. It illustrates how data aggregation is a critical component of value-based payment models, as well as data aggregation's dependency upon identity management, both for providers and for the consumers they serve.

It is important to work across organizations, both regionally and nationally, to identify and build data sharing capacity, and build the capability for identity management. It is neither feasible nor efficient to build such tools from scratch, organization by organization. Tools are complex, resource intensive, and

[53] Health Relationship Trust (HEART), for example, applies OAuth and OpenID Connect when authenticating and authorizing consumers to control access to their health information.

[54] Data Sharing Requirements Initiative: Collaborative Approaches to Advanced Data Sharing toolkit published by the Health Care Payment Learning & Action Network, which was created to drive alignment in payment reform approaches across the U.S. healthcare system.

require common definitions (that is, common data governance). External resources may be especially helpful in establishing identity management of providers and consumers, for attributing patients to providers, and understanding provider relationships within health systems.



This guide attempts to lay out, at a high level, the background and information necessary to develop an effective identity management solution. The following illustrates a potential process a state might use to assess its current solution or implement a more robust solution.

Identify priority use cases that the identity management solution needs to address. Many identity management solutions were established to facilitate care coordination. While critical, other use cases, as illustrated in the section on *Use Cases*, are important for value-based payment models. Use cases must be selected to address organizations' or states' real needs. While this guide concentrates on identity management to support value-based payment models, it is important to ensure that the effort meets the overall strategic needs beyond value-based payment models to ensure full stakeholder engagement. Be sure to include not only use cases for health information access management for providers and consumers and mechanisms such as MPIs to associate consumers with their health information – use cases that support care coordination – but also association of providers to health information and care delivery through attribution that can facilitate appropriate payment and performance measurement.

Identify requirements associated with priority use cases. This guide outlines some of the high-level requirements for identity management associated with the various use cases in the sections on *Business Requirements* and *Technical Requirements*. States should look for opportunities to plan for a more extensive solution over time, recognizing that requirements to support value-based payment models and performance measurement build upon the requirements of other use cases, such as care coordination. A roadmap for a comprehensive identity management solution will allow states to build upon the work already set in motion to support robust access management and care coordination through HIE efforts.

Chief among the business requirements are the analytic and technical capacity to:

- De-duplicate patients
- De-duplicate providers
- Link/distinguish across clinicians, practices, and systems
- Distinguish between billing and rendering provider

- Maintain and update relationships as they evolve

Use cases should be used to create a very specific definition of the patient, provider, and relationship between patients and providers, as well as the relationships among providers and between individual providers and their organizational affiliations.

Requirements, as well as the use cases that drove their development, should go far beyond any individual provider organization or provider system. States should identify all of the providers and disparate systems and data sources required to realize value-based payment models, and ensure that the solution meets all of their needs. Such collaboration will require joint governance and joint funding of the solution.

A more extensive requirements analysis beyond what is included in this guide will be necessary, especially to meet the needs of a specific application. Contact other states with similar projects for procurement advice, requirements analysis, sample request for proposal (RFP) language, and/or vendor experiences. If the solution includes an MPI, consider the description of lessons learned and requirements for a large scale MPI described in the case study for *MyHealth Access Network* in *Appendix 2: Case Studies*.

Determine the appropriate home for the solution. Since identity management must be addressed both within and across organizations, it is important to determine the most efficient and logical place for these services to be organized and delivered in support of a multi-organizational value-based payment model implementation. This determination can in part be based on a survey of what exists, what services are needed, and who needs those services. It is almost certainly beyond a single registry, and extends beyond a health system or regional HIE. The state should assess how existing assets at a local or organizational level can be leveraged in planning and implementing a shared service across payers and providers. Identity management solutions are also complex and resource intensive. Use or expansion of existing systems and collaboration with organizations that may have partial solutions is imperative.

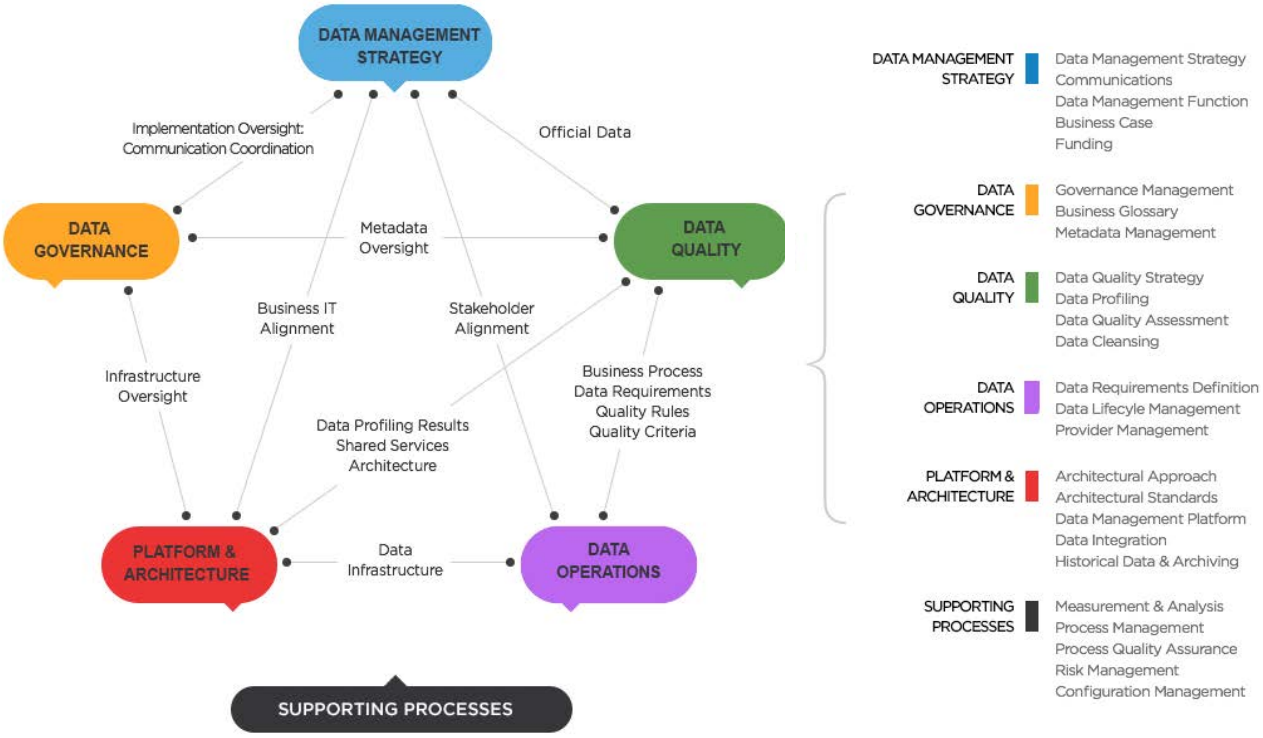
In the current environment, providers and other stakeholders are developing identity management services for their specific populations of focus. These services become more effective and efficient when shared across stakeholders. For an MPI, community or regional HIEs have often chosen MPI technologies that facilitate care coordination. These MPIs may be a good starting point for more extensive identity management approaches that include a broader set of use cases. The *New York eHealth Collaborative* described in *Appendix 2: Case Studies* chose to leverage regional MPIs in a coordinated effort to create a statewide solution for consumer identity management.

States should consider a more comprehensive MPI or master data management approach that includes a broader group of stakeholders, use cases, and geographies. Some states have chosen to base these statewide solutions in state-operated or designated statewide HIEs. However, a more common approach is to govern, develop, and operate a statewide MPI and other critical master data management services through public-private partnerships that leverage the policy levers of state government and the innovation offered by private industry. Shared governance most often leads to better identification and buy-in to priority use cases and solutions. States and stakeholders alike can gain significant efficiencies through shared governance and financing for such services.

Evaluate the maturity of information management business processes within all collaborating organizations and their systems. As described in the case study for the *Utah Community Solution for*

Identity Management in *Appendix 2: Case Studies*, issues associated with poor patient matching performance were not related to poor matching algorithms, but instead to poor data quality within each participating institution. Any successful identity management solution must have robust processes for good data and information management.

The Data Management Maturity (DMM) model is a tool developed by the CMMI Institute (Capability Maturity Model Integration) that can be used for assessing and improving identity management practices. A diagrammatic overview of the model is illustrated below. [55] The DMM provides a common language and framework depicting what progress looks like in all of the fundamental disciplines of data management, including identity management, and can help an organization develop a tailored path to improvement.



The Patient Demographic Data Quality (PDDQ) Framework[56] used the DMM, and is a resource available to states that is intended to support health systems, large practices, HIEs, and payers in improving their patient demographic data quality.

An important component of data management maturity is the development and application of mature data governance and information governance processes. There are other proprietary and fee-based models that can be used as a defined means to address such governance processes.

Data and information governance processes ensure that the data and information that forms the basis for consumer identities, provider identities, attribution, and provider affiliations meet precise technical

55 CMMI Data Management Maturity (DMM)SM

56 Patient Demographic Data Quality (PDDQ) Framework is intended to support health systems, large practices, HIEs, and health plans in improving their patient demographic data quality.

and quality standards. It is important that all organizations collaborating on shared identity management services agree to and support a common master identity management governance approach, data definitions, and data management system, including requirements for frequent updates.

Establish implementation goals. An implementation approach must include a description of how data will be populated. For example, a solution that includes an MPI should set clear goals and expectations for the proportion of the population to be covered in the MPI, a realistic assessment of current data quality, a mechanism and timeline for improving data quality if necessary, a timeline for realizing priority use cases, and a timeline for expanding to additional uses cases if desired.

These goals should include a procurement strategy which borrows successful approaches and language from other states where possible. It should also include instituting data governance and information governance processes, building upon existing business processes where they exist, bolstering immature processes as necessary, and creating new processes to fill gaps.

Finally, it should also include implementing solutions based on national standards where possible to ease interoperability with other, yet to be envisioned, systems and use cases in the future. See *Appendix 3: Business Process and Technical Standards* for a summary of business processes, technical standards that make use of these processes, and the extent to which they are adopted nationally.

Implement policy levers to promote adoption of the strategy. Policy levers related to identity management can be an important component to help establish authority or pursue public policy objectives. As described earlier, the ONC Resource Center has developed a State Health IT Policy Lever Compendium that is a useful reference tool for states to consider.

Adjust as necessary. An important aspect of any implementation plan is to monitor success and adjust as necessary. While identity management is a mature field within the IT industry, there is much activity within healthcare to adopt IT industry best practices, develop new identity matching schemes, and develop and adopt new standards. Best practices will emerge over time, so a flexible approach based on widely-adopted business processes and technical standards can help set up for long-term success.

Monitoring should include periodic assessment of (1) process maturity against the DMM model and/or other existing models, (2) compliance with established business processes, (3) success of policy levers, (4) adoption of the identity management solution, and (5) realizing other established goals.

Funding Opportunities

In the Medicaid enterprise, identity management might be supported directly in the state system as either a shared service, or perhaps a module of the enterprise. In such cases, it might be subject to the funding guidance contained in Medicaid Program; Mechanized Claims: Processing and Information Retrieval Systems (90/10).[57] If criteria are met, not only does this support include a 90 percent federal match for design, development, and installation activities, but operational support might also be available at a 75 percent federal match.

[57] 42 C.F.R. Part 433, Medicaid Program; Mechanized Claims Processing and Information Retrieval Systems (90/10)

Alternatively, identity management might be part of a state's HIE support and could potentially be funded in a cost-allocated manner by the allowances for provider directory or query support described in SMD# 16-003[58] at a 90 percent match subject to the eligibility criteria. Similarly, an MPI might be supported as described in Enclosure A of SMD# 10-016[59] in a cost-allocated manner. Also, as onboarding of Medicaid providers or other kinds of interoperable systems might require consent processes, creating such systems is consistent with the need for thorough oversight of regulatory compliance and verification of identity.

The SIM Grant Funding Opportunity Announcement[60] identifies that SIM grant funding is possible for health IT and HIE and can include infrastructure for collecting and managing model testing initiatives, including identity management. However, SIM funding may not supplant existing federal or state funding.

58 Letter to State Medicaid Directors SMD# 16-003, Availability of HITECH Administrative Matching Funds to Help Professionals and Hospitals Eligible for Medicaid EHR Incentive Payments Connect to Other Medicaid Providers

59 Letter to State Medicaid Directors SMD# 16-0016, Federal Funding for Medicaid HIT Activities

60 Cooperative Agreement Initial Announcement Funding Opportunity Number: CMS-1G1-14-001, State Innovation Models: Round Two of Funding for Design and Test Assistance

Appendix 1: Brief Glossary

The following is a glossary of some key terms and concepts associated with identity management in the healthcare setting as used in this guide. It is not intended as a complete glossary either for the topic of value-based payment models, or as a reference for those seeking a deep technical understanding of identity management.

Attribution – Within healthcare, the process of identifying the provider responsible for an individual's healthcare

Authentication – For IT systems, the process of identifying an individual, organization, or IT system to an IT system using digital credentials, such as user ID, password, digital certificates, etc., issued to the individual or organization

Authorization – For IT systems, authorization is distinct from authentication as a process of giving individuals, organizations, or other IT systems identified through authentication access to system resources such as health information

Data governance – Processes and controls that ensure that the data meets precise technical and quality standards, such as a business rule, a data definition, or data integrity constraints in the data model

Identity and access management - A broad discipline that establishes the identity of individuals within a system (an enterprise, a network, or a software application) in order to control access to resources based on the rights and restrictions associated with that identity

Identity management – Within this guide, the policies and processes that establish the identity of individuals – providers and health consumers – and provider organizations for the purposes of health information access management, attribution of provider and health information to the appropriate patient, care coordination management, performance measurement, and other critical functions that enable quality healthcare and value-based payment models

Identity proofing – The process of verifying that a people are who they claim to be, often associated with issuing digital credentials to be used for authentication, and associated in NIST publications with a "level of assurance" (LOA) procedures best suited to avoid an authentication error[61]

Information governance – An organization-wide framework for managing information throughout its lifecycle and for supporting the organization's strategy, operations, regulatory, legal, risk, and environmental requirements

Master data management – A combination of processes, governance, policies, standards, and tools that are designed to define and manage consistently the critical data of an organization to provide a single authoritative and trusted reference

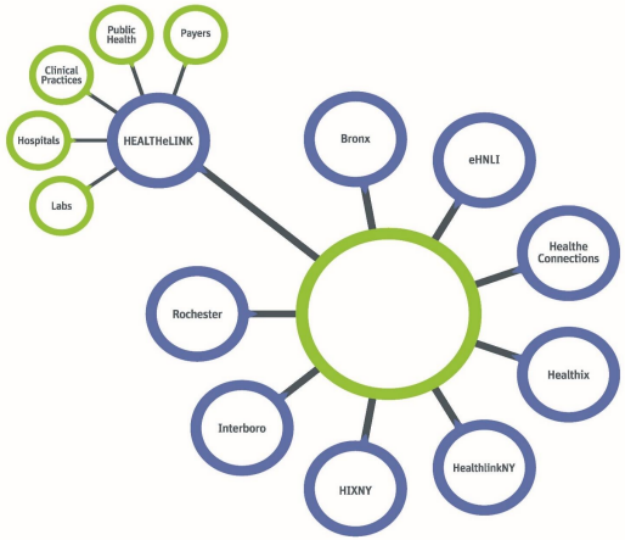
[61] See NIST Special Publication 800-63-3 Digital Identity Guidelines.

Non-repudiation – The assurance that an individual or organization cannot deny the authorship or validity of information, such as through the use of a digital signature of the authoring provider on electronic health information

Appendix 2: Case Studies

New York eHealth Collaborative

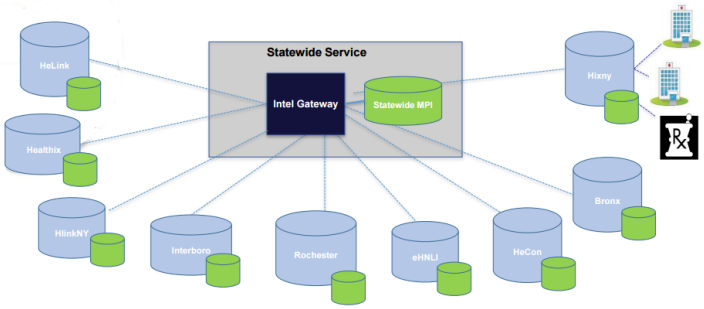
The New York eHealth Collaborative (NYeC) leads the development of the statewide health information strategy in New York, which includes technical capabilities and a statewide HIE framework referred to as the Statewide Health Information Network of New York, or the SHIN-NY (pronounced "shiny"). The SHIN-NY establishes a secure network of regional HIEs for the purpose of sharing electronic clinical records across the state. Stakeholders in New York consider the SHIN-NY an important part of realizing value-based payments. The state's Delivery System Reform Incentive Payment[62] (DSRIP) Program requires providers that are part of the DSRIP Performing Provider Systems (PPSs) to be connected to a regional HIE as a means of improving collaboration and care coordination.



The SHIN-NY comprises nine regional HIEs connected through a "bus" that enables bi-directional exchange among connected HIEs. The SHIN-NY also facilitates statewide lookup of patient records as a statewide service. Part of this service is a federated statewide MPI.

Participants in the SHIN-NY are non-profit regional HIEs originally established by local healthcare stakeholder communities that may offer a number of services based on stakeholder needs. Four services are offered by all HIEs participating in the SHIN-NY: patient record lookup, secure messaging, notifications, and lab results delivery. Each regional HIE is responsible for its own technical infrastructure and governance and the business processes that maintain its individual MPI.

To facilitate statewide patient record lookup, each regional HIE connects to the SHIN-NY through a gateway connected to a statewide MPI. Each HIE shares information from its regional MPI with the statewide MPI. The process for creating statewide identifiers follows these steps:



1. Local MRNs at member facilities flow to the regional HIE
2. Next, the regional identifier is created at the HIE MPI for each patient, joining together the MRNs across member facilities

[62] DSRIP programs are part of Section 1115 Medicaid waiver safety-net care programs which operate a pay-for-performance model and a rewards-based payment structure. Each state implementation of DSRIP may be different.

3. Then, the regional HIE sends its identifier to the statewide MPI where a statewide identifier is created
4. Last, a statewide algorithm works to match individual identities across regional HIEs based on demographic information. Records with low matching scores are entered as separate identities. Records with high matching confidence are evaluated manually to confirm a match, with the highest matching scores merged automatically

Each provider seeking records statewide requests them of the regional HIE, which in turn makes a request to the SHIN-NY which distributes the request to all participating HIEs known to have records for that individual based on the statewide MPI. The SHIN-NY collects responses from HIEs and returns them to the requestor.

CommonWell Health Alliance

The CommonWell Health Alliance is an independent, not-for-profit trade association, the activities of which are largely driven by EHR and health IT vendors serving more than 20 care settings. Its members and participants also include private data sharing networks, systems integrators, federal agencies, state authorities and HIEs, and other non-profit organizations.

CommonWell has created an enabling infrastructure with the goal of providing access to health information regardless of where care occurs at a reasonable cost and for use by a broad range of healthcare providers and patients, within the health IT systems they use. Today, CommonWell services support a query/retrieve model for accessing person-centered health information for the purposes of treatment and direct patient access. The infrastructure includes:

1. An integrated MPI and
2. A record locator service (RLS) supporting
3. A brokered query model

The brokered query simplifies the user experience by fanning out requests to all network participants and bundling the responses. As of July 2017,[63] the CommonWell network included over 5,400 live clinical sites, with over 17 million unique individuals and over 53 million records. Importantly, more than one million individuals have linked identities across different vendors and care settings.

Participating systems send identifiers, demographics, and encounter information on individuals to CommonWell using IHE PIX or FHIR protocols, pre-populating the MPI with patient identities with information collected at each care setting. The users of the participating systems "enroll" an individual with the individual's cooperation and agreement, ideally using a strong identifier (such as a driver's license) to ensure that the individual's identity is correctly represented.

[63] Statistics and figures taken from the 21st Century Cures Act Trusted Exchange Framework and Common Agreement Kick-Off Meeting.

Once a patient identity is established in CommonWell, providers can search for matches across the country, identifying potential patient matches and, via the RLS, pointers to health records within the systems that enrolled the patient.

A critical part of the CommonWell workflow is patient linking. With the patient's participation, a provider uses their system on the CommonWell network to search for records. The provider and patient work together to confirm that the patient identity retrieved from the MPI is correct, and that the linked records retrieved from the RLS belong to the patient. Incorrect matches returned by the search (for example, a record for an encounter at a facility that the patient has never visited) can be marked as incorrect, preventing future searches from returning it again. Once the patient identity on CommonWell is confirmed, the provider can explicitly link the local patient record to records at other remote organizations. This process enables the remote practices to reciprocally retrieve data with assurance that the information is correctly linked to their patient and their local patient identifiers.

Utah Community Solution for Identity Management

Utah is exploring a different approach to consumer identity management based on a vision for automating workflow for care coordination across very different care domains. A priority was to relieve the burden of identity management to allow timely movement of health information. A solution required both solving the identity management problem at the community level and developing a trusted mechanism for automated system-to-system resolution of consumer identity with minimal manual intervention.

The effort was motivated by existing patient matching inaccuracies impacting clinical, financial, and operational performance. For example, Intermountain Healthcare, a 23-hospital health system based in Salt Lake City, spends an estimated $5 million annually on technologies and processes to try to ensure proper patient identification. The system considers the patient safety issues even more alarming than the financial cost.

The approach is not based on a new paradigm for identity matching but leverages existing standards, including the XCPD cross-community identification and authorization standards already in wide use. Like traditional matching mechanisms, it achieves patient matches using demographic information. Each participating organization uses its own methods and algorithms for identity matches. Key to the service is utilizing the state-designated HIE that has matched millions of identities to create a longitudinal record.

What the Utah team discovered was that each organization had its own mechanisms for identity management that functioned within the organization. However, attempts to find matching identities for individuals across organizational boundaries presented issues. The issues didn't appear to be a result of inconsistent matching algorithms, but instead poor data quality within each institution's MPI. One key to success has been a significant focus on data quality. Project participants found that most matching algorithms will perform well if data quality is sufficient, and no algorithm will work well community-wide

with poor data quality. Clearly, the more data that can be used to process identities, the more opportunity to link the disparate identities.

The project created a constrained data template against which all MPIs need to perform. The project team then asked participants to self-report on consumer demographic information they have, consistent with the template, including data sets that may be incomplete for an individual. That information was compared to that contained in the Utah Health Information Network (UHIN) MPI to identify areas of potential data quality improvement.

Important early findings identified that matching performance could be significantly improved by improving data quality through business process improvement, often associated with patient registration.

The proposed solution also leverages a community approach to matching. If one organization is trying to determine whether two records should be merged as a single identity, it can submit the proposed pair to the larger community via UHIN's MPI to determine whether others have linked these records before. In addition, including other data in UHIN's MPI, such as the Utah Population Database, a research database, can contribute important data cleansing information leading to more accurate patient matching. Currently, the pilot relies on a consensus approach to community identity matching. However, over the next two years, the project participants will explore development of a community-wide "golden record" housed in UHIN's MPI.

Development of the pilot solution was dependent upon two key elements:

1. Identification of appropriate grant funding that would provide for development of a constrained template and data quality improvements among participating organizations
2. Legislative protection against liability associated allowed electronic disclosures of health information[64]

Funding for the pilot ended with the SIM Design grant completion. The team plans to continue its activity under expanded HITECH funding. To ensure that the project continues to advance, the community has created a committee with participants from government, public health, health insurance, health systems, clinics, pharmacies, and UHIN.

Michigan Health Information Network Shared Services

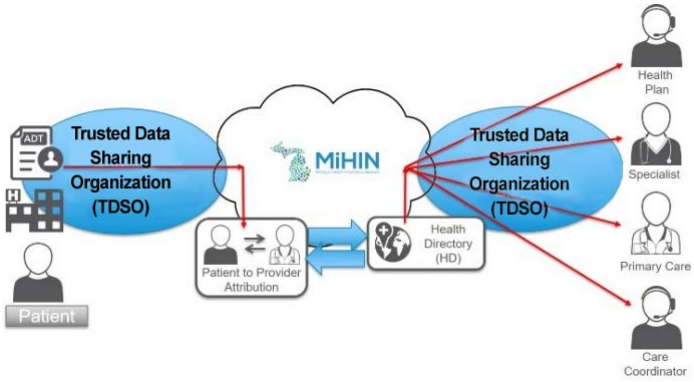
The Michigan Health Information Network Shared Services (MiHIN) is a statewide initiative to promote and support secure, electronic exchange of health information. MiHIN has developed an extensive provider directory that tracks not only provider demographic information but also complex affiliations the provider may have with multiple organizations, as well as the provider's preferred means of electronic communication for health information. The directory pairs with MiHIN's Active Care Relationship Service (ACRS), a patient-provider attribution mechanism to track current, "declared" care relationships to ensure that a patient's full "care team" is known and can be notified in the event of

[64] Utah Code 26-1-37(5) states that a health care provider or a qualified network is not subject to civil liability for disclosure of clinical health information if an electronic exchange that is a permitted disclosure to a local health department or for treatment, payment, or health care operations as defined in 45 C.F.R. Parts 160, 162, and 164.

changes to the patient's status. The two services work together to ensure that health information is sent to the correct providers/care coordinators in an actionable, consumable format.

Key drivers for these paired services included identification of valuable use cases that could leverage provider identity information and a robust attribution mechanism as part of the MiHIN core infrastructure. Those use cases include:

1. Care coordination use cases, such as Admission, Discharge, Transfer Notifications and Medication Reconciliation
2. Quality measurement use cases



The provider directory aggregates data from multiple sources from which it derives variable "trust" based on each source's domain. This allows insurance companies to maintain data for which they are sources of truth (e.g., which providers are in-network), and providers to contribute data for which they are the source of truth (e.g., relationships, affiliations, telephone numbers). The MiHIN model for declared attribution does not need to depend on health-plan-assigned attribution or retrospective claims-based attribution. These attribution methods have been found to include conflicting information, may not track with patients' changes in health plans, does not work for specialists and safety-net providers who are not attributed by health plans, and may not be well-aligned with more advanced payment models. Instead, MiHIN utilizes what it terms "physician-centric attribution" that focuses on declared relationships between providers and consumers, obtained either from physicians who indicate active patients or from individuals who indicate their healthcare providers. Attribution is therefore typically based on a physician's patient roster showing the panel of patients with which the doctor feels there is an active care relationship in place. Leveraging this information to govern transitions of care use cases increases stakeholder desire to keep the information accurate and current. This stakeholder engagement promotes proactive maintenance by the data sources, thereby keeping the overall process cost-effective.

To address care coordination use cases, ACRS and the provider directory identify and track providers who comprise a patient's care team. The services also maintain those providers' Direct addresses[65] or other preferred methods for electronic communication of health information. This means providers on the care team are quickly and efficiently alerted of health events for individuals attributed to them.

MyHealth Access Network

MyHealth Access Network is a statewide HIE in Oklahoma connecting doctors, hospitals, pharmacies, payers, public health and others to facilitate the secure sharing of health information. As one of 17 ONC-supported Beacon Communities,[66] MyHealth Access Network has developed a set of requirements for large scale (such as statewide) MPIs based on its experience and the evolution of its own MPI solution.

---

65 Direct messaging is a technical standard for securely exchanging health information between individuals that uses an address structure similar to email.

66 See Beacon Community Program for more information.

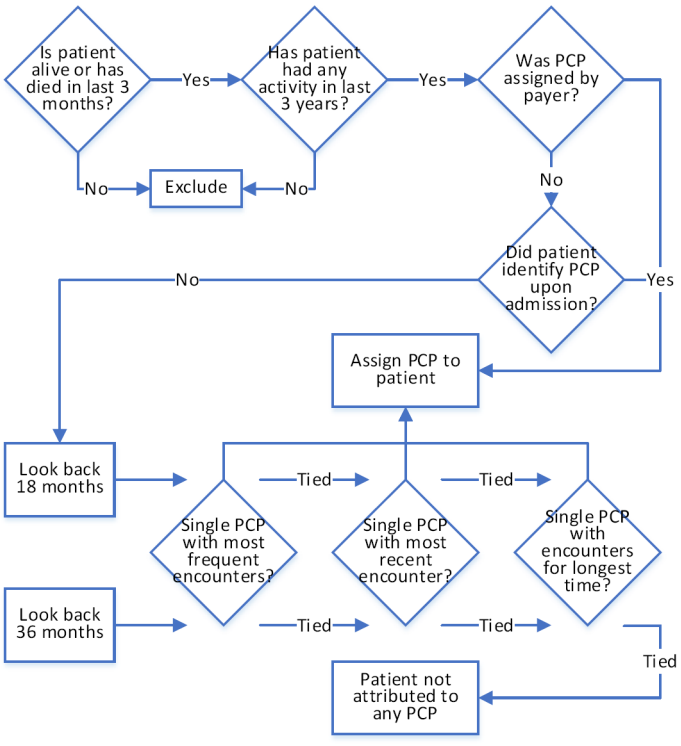
Importantly, MyHealth Access Network now approaches the need to manage provider and consumer identities with the vision to include patient attribution to allow for performance measurement and value-based payment models. Lessons learned through multiple MPI implementations and the requirements for an effective identity management system included:

1. Traditional MPI solutions have proven to be insufficient to meet the full needs of an organization that tracks not only individual identities, but also providers and their organizations, as well as other community resources. The need to attribute patients to providers for primary care, specialty care, surgical, and other reasons increases the need to have accurate provider and resource directory information. It is important to approach identity management using master data management concepts, whether they are bolted onto an existing MPI or are included within a single MPI package. The current iteration of the MPI at MyHealth Access Network uses a true master data management tool rather than a traditional MPI.
2. Too little emphasis is placed on data transparency and too much on matching algorithms. The user interface of many identity management systems is insufficient and too opaque to provide true transparency into the identities, attributes, and attribution of consumer and provider data. MyHealth Access Network has chosen to potentially sacrifice some power in the proprietary matching algorithms in exchange for a user interface and experience that provides better consistency and transparency.[67]
3. It is necessary to not only track and resolve provider identities and patient identities, but also the location of care delivery and of the interaction between providers and patients. Location and type of service provide important context for patient attribution and performance metrics, which together enable support of value-based payment models and performance reporting.
4. It is better to make matching decisions, merging patient identities and attributing health information to the right patient, close to the source of the information, both geographically but more importantly logically. For example, there are hundreds of organizations feeding data to the typical HIE. The peculiarities of each organization's registration and internal identity resolution process are highly relevant to getting patient identities correct when the community-level matching is performed. The labels an organization may use for a John Doe trauma patient or a newborn child must be known and accommodated to ensure that individual identity matching is accurate. This may indicate that there is a theoretical maximum size beyond which MPI management becomes impractical and increasingly inaccurate, as those managing the MPI get further and further removed from the actual sources of the identity information.
5. MyHealth Access Network is exploring the use of clinical information as well as demographic information in making matching decisions, best facilitated by matching decisions made close to the source.
6. MyHealth Access Network is now working with other HIEs to begin exchanging resolved identities to enable cross regional identity management. This is being performed as a part of the Strategic Health Information Exchange Collaborative' s (SHIEC) Patient Centered Data Home™ program and early indicators are that exchanging resolved identities between regional MPIs may obviate the need for a nationwide patient identifier or other nationwide solutions for identity resolution.

[67] The Utah Community Solution for Identity Management noted that data quality was more important than the power of matching algorithms. Transparency should lead to improved data quality.

7. Organizations should instill processes that will detect overlays[68] by ensuring that decisions to match identities and attribute health information to patients are based not only on the MRN, but also on demographic information to confirm the identity of the individual. MyHealth Access Network has found that overlays are not as rare as one might think, especially as more and more small clinics and agencies become data sources for HIEs.
8. Hospitals should create look-up interfaces between registration systems and the MPI so that information from the MPI can (1) populate the registration record and (2) easily be checked and confirmed at the time of registration. Such processes will greatly reduce the errors caused by manual entry of important demographic information at registration.
9. HIEs operating an MPI need to create and analyze variance reports that identify mismatched identities or overlays and communicate the results to their participants with variances. Such reporting can often lead to better data quality at the source of information and solve issues early in the data collection process.
10. Do not underestimate the need for processing performance in selection of an MPI or master data management technology solution. As patient population size grows into the millions and tens of millions, daily identity resolution processing can quickly become a choke point in the overall flow of data, which can be disastrous if ADT alerting or other just-in-time processes need to be supported.

MyHealth Access Network describes the process for identity management as a combination of (1) the identity and information about the person receiving healthcare; (2) the provider involved in the encounter, including the individual provider, the organization to which he/she belongs, and the location of the encounter; (3) the reason for the encounter; and (4) the method(s) used to attribute the patient to the provider. It is important to describe the full organizational structure and identify where the individual provider fits within the structure at the time of the encounter.



The figure describes an example flow chart for making primary care attribution decisions, which includes declaration of relationships as well as historical encounter information. MyHealth Access Network's governing body reviews and approves algorithms for attribution, and currently has approved algorithms for primary care, specialty care, "proceduralists" and oncologic medical home. Others are in consideration.

68 Overlays are situations when the same MRN is assigned to more than one individual, usually through system error, merging health information belonging to two distinct consumers into a single mixed health record. It is often difficult to separate the health information merged as a result of overlays.

Appendix 3: Business Process and Technical Standards

Standards for Managing Identity

The following technical standards and business processes are used to define and manage individual or organizational identities, authenticate them, and authorize access to system resources such as health-related information.

See the 2017 Interoperability Standards Advisory published by ONC[69] for more information on the technical standards for interoperability, including for identity management, along with information on maturity and adoption.

Public Key Infrastructure

Public Key Infrastructure (PKI) is a set of organizational roles, policies, and procedures to create, manage, distribute, and use digital certificates. Its purpose is to facilitate the secure transfer of information on an insecure network, such as the Internet. To do that, it provides a scalable means to perform two critical functions:

1. It enables the sender and/or intended recipient to be unambiguously authenticated, so that messages are only sent by or can only be received by known and established identities (both of individuals or organizations)
2. It enables the information to be encrypted so that it cannot be read except by the intended recipient or altered during transmission without such alteration being detected

PKI is based on public key and private key pairs, and its security is only as strong as the level of effort an individual or organization exercises in issuing and protecting the private key. Information encrypted with or signed by a private key under the control of the sender can be decrypted with the corresponding public key to validate its authenticity. Information encrypted with a sufficiently strong public key can, for all practical purposes, only be decrypted with the corresponding private key under the control of the recipient to ensure disclosure only to the intended recipient. Both processes can ensure that the information was transmitted without corruption or alteration.

PKI establishes two very important business roles and processes:

1. The Certificate Authority (CA) is responsible for issuing and revoking digital certificates
2. The Registration Authority (RA) is responsible for assuring the identity of an individual or organization and the correct registration of a digital certificate with that identity

CA and RA roles may be, and often are, combined into a single organization. Depending on the assurance level that binds the digital certificate to the identity, the RA process can be simple and automated, or detailed, rigorous, and manual.

Digital certificates are issued and managed under a set of policies and procedures that govern the level and process for identity proofing, the process of issuing certificates and publishing the public keys, and the procedures for protecting private keys. If a private key is ever compromised, these policies and

[69] 2017 Interoperability Standards Advisory

procedures also define the methods for revoking a digital certificate as well as for discovering that a certificate has been revoked and its association with an identity is no longer valid or reliable.

Security Assertion Markup Language

Security Assertion Markup Language (SAML) is an XML-based standard for exchanging authentication data and asserting authorization to access system resources between disparate systems. SAML is managed by the OASIS Security Services Technical Committee.[70]

SAML does not establish or manage provider identities, but plays an important role in communicating authentication and authorization to access system resources. Traditionally, SAML has been used most extensively for single sign-on. However, SAML assertions are encapsulated in the SOAP web services[71] described and used in eHealth Exchange specifications.[72] There, SAML describes information about the provider making a request for information, the method used to authenticate the provider, and key information such as the purpose-for-use that the responding system or organization can use to make informed decisions regarding disclosure of health information.

OAuth and OpenID Connect

OAuth is an open standard for authorization, most commonly used as a way for users to authorize one application or system to access information on another system without authenticating to both systems. OAuth is used by Google, Facebook, and other companies to permit users to share information about their accounts with third-party applications or websites. More specifically, this allows a user to access those third-party applications or websites without creating a new user name and password.[73]

OAuth works by providing delegated access to system resources on behalf of the owner of those resources. Importantly, it specifies a process for resource owners to authorize access without sharing their credentials. OAuth is not used extensively between enterprises within healthcare today, but is being explored as a mechanism for single sign-on or other authorization services, including potentially for FHIR.

OAuth is complementary to but distinct from OpenID Connect, which provides an authentication layer built on top of OAuth. Like OAuth, there is little widespread adoption of OpenID Connect.

Like SAML, OAuth and OpenID Connect do not establish provider identities. But the standards do provide a means for a third-party identity manager to provide controlled and secure access to systems without each system having to manage individual or organizational identities and credentials themselves. OAuth and OpenID Connect would be enabling to third-party identity authorities for

---

70 Organization for the Advancement of Structured Information Standards (OASIS) is a global consortium developing and promoting standards for security, the Internet of Things, energy, content technologies, emergency management, and other areas.

71 SOAP (originally Simple Object Access Protocol) is a technical specification for exchanging structured information between systems using eXtensible Markup Language (XML).

72 The eHealth Exchange is a group of federal agencies and non-federal organizations that exchange health information nationwide using a common data use agreement and SOAP web services.

73 OAuth is the underlying standard being used any time an individual is asked to log onto a web site using one's Facebook or Google account.

providers should they emerge, and allow systems to consolidate identity management within heterogeneous networks into one system.

Standards for Managing Provider Identities

The following technical standards and business processes are used to declare or search for individual or organizational provider identities.

X12 274 Healthcare Provider Information

The X12 274 transaction set specifies a data format and establishes the data contents of the Healthcare Provider Information Transaction Set (274) within the Electronic Data Interchange (EDI) environment. X12 EDI standards are managed by the Accredited Standards Committee (ASC) X12, and are most prevalent as administrative functions within the payer community. X12 274 can be used to exchange demographic and educational/professional qualifications about individual or organizational providers. It defines exchanges that include transmitting, querying for, or responding to a query for provider information.

X12 274 is usually used to maintain provider data for claim adjudication provider directories or registries maintained by plans; submitting an application to join a network such as a preferred provider organization (PPO) or health maintenance organization (HMO); or verifying credentials such as educational/professional qualifications, licenses, and malpractice coverage or history. It provides mechanisms to describe individual providers, provider organizations, relationships between individuals and organizations, plan participation, and services and service hours offered by providers at a location.

While many X12 transactions are commonly implemented among payer organizations, including Medicaid and Medicare, X12 274 has not been widely adopted. X12, including the X12 274 transaction, does not specify a transport mechanism or security model for the information it transmits.

Healthcare Provider Directory

Healthcare Provider Directory (HPD) is an IHE profile that defines a data model and interface for registering, managing, and retrieving individual and organizational provider information. The HPD data model is based on Lightweight Directory Access Protocol (LDAP) (later extended to relational database models), and defines optional and required information stored for individual providers, organizational providers, relationships between individuals and organizations, relationships between organizations and their owned sub-organizations, and the means to exchange health-related information with them electronically.

HPD defines an interface for registering or querying for provider information based on Directory Services Markup Language (DSML), a representation of directory information using XML syntax. HPD has not enjoyed broad industry adoption, probably due to its initial specification of a data model based on LDAP and the cumbersome DSML interface model. However, the underlying data requirements and specifications documented in HPD have formed the basis for other provider directory standards and implementations.

HPD does not necessarily establish a unique provider identity, nor does the profile establish or imply business models for storing or retrieving provider identities. Instead, it provides a means to describe provider information and retrieve provider information based on matching demographics.

HPD is based on SOAP web services. The profile does not require that the HPD interface be secured, but implementations often use PKI on public networks to authenticate the server providing the source of provider information.

Standards for Matching Patient Identities

The following technical standards and business processes are used to register and search for individual patient identities, usually for the purpose of matching health or health-related information to a consumer.

Patient Identifier Cross-Reference and Patient Demographic Query

Patient Identifier Cross-Reference (PIX) and Patient Demographic Query (PDQ), or together PIX/PDQ, are profiles developed and managed by IHE for maintaining a registry of identities within an enterprise and for querying that registry for matches.

PIX defines an interface that a healthcare system can use to register an identity with a cross-reference manager. It defines key patient demographic information and associates it with the MRN used by the organization and system as the identity that uniquely identifies that individual. The cross-reference manager, in turn, links the MRNs of other systems to the same individual demographics, effectively associating the identities of these unrelated systems into a single identity within the enterprise.

PDQ defines an interface that a healthcare system can use to locate matching individuals by querying for and retrieving the MRNs from the cross-reference manager based on demographic information. The cross-reference manager uses key demographic information in the query to locate a single unambiguous or multiple potential matches, returning the identities defined by the MRNs it contains.

PIX/PDQ is often associated with a document registry or record locator. PIX registers and associates the identity of an individual with his/her health information. PDQ retrieves pointers to that health information based on demographic information about the individual.

PIX/PDQ are considered mature standards and are relatively well adopted by EHRs and HIE technologies. Like HPD, PIX and PDQ are based on SOAP web services and usually secured and protected by private networks or PKI on public networks.

Cross-Community Patient Discovery

Cross-Community Patient Discovery (XCPD) is another IHE profile for locating individual identity matches, in this case across enterprise boundaries. It defines an interface that two systems can use to "negotiate" a match:

1. The initiating system passes key patient demographic information to a responding system
2. The responding system passes back individual identities that might be a match, along with its version of the demographics it has on file
3. The initiating system examines the returned demographics and, if it agrees they refer to the same individual, declares a match

An important feature of XCPD is that both the initiating and responding systems apply matching algorithms against the demographic information stored by the other system to determine if identities match. They may disagree. For example, one system might allow for transposed month and day in a date

of birth or might allow a variation on the spelling of a last name, while the other is more stringent in its requirements and matches are not declared.

XCPD is considered a mature standard, and is used by eHealth Exchange and Carequality as the primary means for discovering patient identities. XCPD is likewise based on SOAP web services and usually secured and protected by private networks or PKI on public networks, and may use SAML to assert authorization for disclosure of individual consumer identities.

Standards for Attribution

At this time, there is no technical standard available and widely adopted to represent provider-patient attribution. The discussion of *Michigan Health Information Network Shared Services* in *Appendix 2: Case Studies* provides a brief description of an implementation despite the absence of accepted national standards, and the HealthCare Directory Tiger Team efforts described in the section on *Provider Registries* aim to develop a standard based on FHIR.

Emerging Identity Management Standards

Fast Healthcare Interoperability Resources (FHIR) is an emerging standard managed by HL7[74] that defines a set of "resources" that represent granular clinical concepts. The resources can either be managed in isolation, or aggregated into complex concepts or to accomplish more complex use cases. Technically, FHIR is designed for the web using simple XML or JSON data structures, and where possible, open internet standards.

Among other things, FHIR defines the means for transmitting or querying for patients and providers, and therefore a means for discovering patient matches and healthcare information matching individual demographics, or for describing and discovering provider information.

FHIR does not call out a specific transport method or security model. Most FHIR implementations use RESTful web services [75] and PKI or OAuth security models.

FHIR Standards for Provider Identity

Provider identity resources are part of the Administration Module in FHIR. They include:

- Organization, which describes information about formally- or informally-recognized groupings of people or organizations formed for the purpose of achieving some form of collective action (usually care delivery), and may include companies, institutions, departments, community groups, healthcare practice groups, and others
- Location, which describes details and position information for a physical place where services are provided

---

74 Health Level Seven (HL7) is an international standards development organization establishing standards for the transfer of clinical and administrative data between healthcare systems.

75 REST refers to a web standard to create, read, update, and delete data “resources” via a common interface using HTTP standard methods. At the time of this writing, Michigan Health Information Network Shared Services (MiHIN), The Sequoia Project, and the California Association of Health Information Exchanges (CAHIE) have implementations of a provider directory or services registry based on RESTful FHIR services. Other organizations may, as well.

- HealthcareService, which describes a healthcare-related service available at a location
- Practitioner, which describes information about an individual professional person directly or indirectly involved in the provision of healthcare
- PractitionerRole, which specifies the roles, locations, specialties, and services that a practitioner may perform at an organization
- Endpoint, which specifies the means for exchanging health information with an organization, location, or practitioner related to a role or healthcare service

These resources identify data elements and a potential data model for provider information contained in a registry or directory. FHIR does not describe a business process that ensures unique provider identity, but Organization, Location, and Practitioner return unique identifiers for individual providers, provider organizations, and service delivery locations.

In addition, FHIR defines a Group resource which may be suitable for describing the relationship between a provider and a patient, but has not been used that way.

FHIR Standards for Consumer Identity

Likewise, consumer identity resources are part of the Administration Module in FHIR, and include resources that describe Patient and RelatedPerson. The Patient resource contains demographics and other administrative information about an individual receiving care or other health-related services, and can be queried to find individuals that match specific demographic information. The retrieved Patient identity can be linked to FHIR resources that describe clinical information, and therefore used to retrieve health information for that individual. The RelatedPerson resource contains information about a person that is involved in the care for a patient, but who does not have a formal responsibility in the care process, such as a provider. A RelatedPerson may be a family member or other caregiver involved in care, and can be linked to patients.

FHIR does not describe a business process that ensures unique individual consumer identity. However, the Patient resource returns unique identifiers for individuals represented on the server.

Appendix 4: Bibliography

Guidance Documents on Identity Management

- National HIE Governance Forum Identity and Access Management for Health Information Exchange prepared under the auspices of the National eHealth Collaborative through its cooperative agreement with the Office of the National Coordinator for Health Information Technology in 2013
- Federal Health Architecture Patient Identity in Directed Exchange: How Much Assurance? published in 2014 by Federal Health Architecture
- A Shared Nationwide Interoperability Roadmap version 1.0 published by the Office of the National Coordinator for Health Information Technology in 2015, with sections on provider and individual identity management
- State Health IT Modular Functions for Value-Based Payment Strategic Implementation Guide Provider Directories published by the Office of the National Coordinator for Health Information Technology in 2016 with more detail on provider identity management and provider registries
- State Health IT Policy Lever Compendium maintained by the Office of the National Coordinator for Health Information Technology
- Patient Demographic Data Quality (PDDQ) Framework maintained by the Office of the National Coordinator for Health Information Technology
- Patient Demographic Data Quality: Ambulatory Guidance maintained by the Office of the National Coordinator for Health Information Technology
- CMMI Data Management Maturity (DMM)℠ maintained by the CMMI Institute
- Cyber Security Guidance Material on the HHS.gov web site
- Accelerating and Aligning Population-Based Payment Models: Patient Attribution published by the Health Care Payment Learning & Action Network
- Data Sharing Requirements Initiative: Collaborative Approaches to Advanced Data Sharing toolkit, product of the Health Care Payment Learning & Action Network

Papers on Identity Management

- Western States Consortium ONC State Health Policy Consortium Project Final Report prepared for the Office of the National Coordinator for Health Information Technology by RTI International in 2012
- The Most Important Question in Identity Management for Health Care, a whitepaper published in 2012 by LexisNexis
- How Hospitals Should Build a Data Infrastructure published in 2017 in *Hospitals & Health Networks*
- Recommended Identity Assurance for Patient Portals published in 2015 by the HIMSS Identity Management Task Force
- Healthcare has an Identity Problem published in 2015 as guidance from the HIMSS Identity Management Task Force
- Patient Portal Identity Proofing and Authentication published in 2016 as guidance from the HIMSS Identity Management Task Force

Reports on Identity Matching

- XDS Patient Identity Management White Paper published in 2011 by Integrating the Healthcare Enterprise (IHE)
- National Strategy for Trusted Identities in Cyberspace published in 2011 by The White House
- Master Data Management within HIE Infrastructures: A Focus on Master Patient Indexing Approaches prepared for the Office of the National Coordinator for Health Information Technology by Audacious Inquiry in 2012
- Patient Identification and Matching: Final Report prepared for the Office of the National Coordinator for Health Information Technology by Audacious Inquiry in 2014
- Report to HITSC: Virtual Hearing on the National Strategy for Trusted Identities in Cyberspace (NSTIC) presented in 2014
- Managing the Integrity of Patient Identity in Health Information Exchange updated in 2014 and published by AHIMA
- A Framework for Cross-Organizational Patient Identity Management published in 2015 by The Sequoia Project
- San Diego Health Connect Community News on San Diego Health Connect's use of Verado technology in patient matching

NIST Guidelines on Digital Identity Management

- NIST Special Publication 800-63-2 Electronic Authentication Guideline, now archived but published for historical purposes
- NIST Special Publication 800-63-3 Digital Identity Guidelines which will supersede 800-63-2 following public comment and formal release
- NIST Special Publication 800-63A Digital Identity Guidelines: Enrollment and Identity Proofing Requirements
- NIST Special Publication 800-63B Digital Identity Guidelines: Authentication and Lifecycle Management
- NIST Special Publication 800-63C Digital Identity Guidelines: Federation and Assertions
- NIST Special Publication 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
- NIST Cybersecurity Framework

Technical Standards

- Interoperability Standards Advisory (ISA) maintained by the Office of the National Coordinator for Health Information Technology, last updated in 2017
- X12 274 Healthcare Provider Directory (004050X109) published by the Accredited Standards Committee X12
- Healthcare Provider Directory (HPD) Trial Implementation version 1.6 published in 2015 by Integrating the Healthcare Enterprise (IHE) as a supplement to the IT Infrastructure Technical Framework
- Patient Identifier Cross-Reference HL7 V3 (PIXV3) and Patient Demographic Query HL7 V3 (PDQV3) published in 2010 by Integrating the Healthcare Enterprise (IHE) as a supplement to the IT Infrastructure Technical Framework

- Cross-Community Patient Discovery (XCPD) Trial Implementation published in 2011 by Integrating the Healthcare Enterprise (IHE) as a supplement to the IT Infrastructure Technical Framework
- FHIR (Fast Health Interoperability Resources) Release 3 (STU) published in 2017 by HL7
- 2017 Interoperability Standards Advisory published by the Office of the National Coordinator for Health Information Technology