[Solution Brief]

SDG's Healthcare Identity Hub: Managing Multiple Personas with Diverse Roles from Various Data Sources

OVERVIEW

Identity governance and administration (IGA) in healthcare cybersecurity is complex due to decentralized, fragmented, and siloed systems. Mergers, acquisitions, partnerships, and separate education and provider departments add to this complexity, along with the expansion of specialized departments funded by grants and donations. Managing access effectively is difficult when individuals have multiple personas, originate from different authoritative sources, and need access across various locations. This challenge extends beyond employees to include students, volunteers, community doctors, residents, travel nurses, and others. The **Identity Hub** framework simplifies identity management by creating a unified identity repository for IGA systems. It consolidates data from multiple sources, such as HR systems, third-party databases, enterprise directories, and external identity platforms, streamlining identity governance in complex healthcare environments.

PROBLEM: MANAGING ACCESS FOR HEALTHCARE PROVIDERS WITH MULTIPLE PERSONAS AND VARIOUS ROLES

Healthcare providers often have multiple personas that require varying degrees of access to enterprise systems. These personas include:

Employees	Non-employees (volunteers, vendors, contractors, community physicians)	Temporary staff (travel nurses, students, residents, fellows)

A single user may belong to multiple categories making it challenging to grant proper access to the correct data at the right time. For example, a healthcare provider might be:

- A resident at Hospital A (Persona 1) – With the "Clinician" role
- A community physician at Clinic B (Persona 2) – With the "Consulting Physician" role

Their system access needs will vary based on **which persona** they are acting under.

Key Challenges:

Different Systems for Different Users:

- Employees, non-employees, and temporary staff identity data often originates from separate authoritative source systems.
- Each source has distinct key attributes, and often the data included lacks critical information required for workflows and assignments.

Gaps in Data Consistency:

- Data quality varies across systems, making it difficult to standardize.
- Missing or inaccurate information can cause delays and errors in access.

Impact from Mergers and Acquisitions:

- Multiple locations and facilities, resulting from mergers or acquisitions, often add additional authoritative sources to an already complex system.

Multiple Personas per Identity:

- A single user may have multiple personas, such as being both a resident and a community physician, each requiring different system access.
- This demands a framework that can handle multiple personas under one identity without compromising security or operational efficiency.

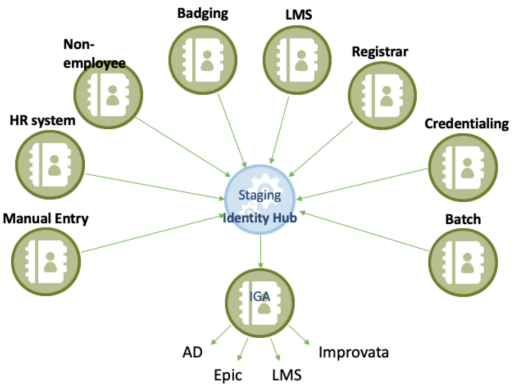
The Core Question:

How can we manage access for individuals with multiple personas and ensure each role has the right permissions while maintaining consistency and preventing duplicate identities?

SOLUTION: CREATE AN IDENTITY HUB

Consolidating identity profiles from multiple trusted sources into a single, centralized **Identity Hub** before pushing to the IGA system solves the healthcare provider's access challenges of managing multiple personas with diverse roles.

The Identity Hub acts as a centralized repository for all identity data. The solution is **technology-agnostic**, meaning it can be implemented using various technical solutions that support the organization's preferences and capabilities.



Implementation Options:

Relational Databases:

Suitable for organizations familiar with managing structured data in a highly customizable format.

Directory Servers:

Ideal for scenarios requiring fast, hierarchical lookups and support for identity-related protocols like LDAP

The specific technology chosen for implementation will depend on:

- The organization's existing technical infrastructure.
- Support capabilities and preferences for ongoing maintenance.

This approach ensures flexibility while achieving the goal of unified identity management.

Identity Hub Provides:

Risk Reduction

- The ability to perform bulk validation of authoritative records (for example, to stop processing and force manual inspection of data if more than 'x' number of changes are detected in a single load cycle).
- Pre-emptive data inspection and cleansing, reducing the likelihood of downstream systems being impacted by unplanned changes to authoritative data.

Performance

- A reduction of the processing burden on the IGA system, leading to faster aggregation/reconciliations. When loading data from connected systems, most IGA products perform data validation and transformation for each individual record, one at a time. This not only impacts performance of the IGA system itself but can result in prolonged load times. Identity Hub normalizes data into a relational database, allowing business rules to be executed against data in a bulk fashion, inspecting and updating multiple records at once.
- A product agnostic approach to data assimilation reduces complex business and data transformation logic in the IGA system by using standard SQL scripts and stored procedures.

Control

- In most organizations, the area responsible for identity management rarely has any control over the systems of record upon which they depend (for example, HRMS systems or contractor repositories). Identity Hub provides a greater level of control over the authoritative data that is foundational to the stability and reliability of the IGA system.
- The creation of custom attributes (for example, action flags or unique identifiers) can be generated based on the evaluation of imported authoritative data.The organization's existing
- A single, unified view of user data simplifies the process of generating meaningful reports and analytics and exposes a single authoritative source that can also be leveraged by other business systems.

Architecture

- In the event that an IGA system needs to consume data from a new authoritative source (for example, a new HRMS system resulting from a merger/acquisition), Identity Hub abstracts the complexity of assimilating data. New authoritative sources can be integrated seamlessly without having to make any major changes to the IGA system, as IGA will still consume the same view of authoritative data.
- Identity Hub is product agnostic. If an organization decides to migrate to a new IGA system, it can use the same authoritative source without having to port legacy business rules.
- Externalizing the aggregation of authoritative data from the IGA system simplifies the process of assimilating new identity attributes and implementing new business processes.

SDG'S APPROACH

Determining if an Identity Hub would be a benefit to your IGA program is the first place to start. SDG would assess the authoritative sources and the identity profiles from each to determine the variations. We would then look for identities where there is no authoritative source, yet they still require access.

Once it has been determined that an Identity Hub would benefit the IGA program, SDG follows a delivery value chain of four stages. This outlines specific use cases where these practices would be beneficial:

- **Returning Identities or Multiple Personas:**

  Situations where users return with prior accounts or require different personas should be carefully managed to avoid creating duplicate accounts.

- **Terminations or Role Changes (Movers):**

  When an account is required for multiple locations or spans multiple domains, we need to ensure that removing one persona does not unintentionally revoke all access.

- **Lack of an Authoritative Source:**

  In cases where no authoritative source exists, a portal or mechanism to add identities is necessary.

- **Correlation Across Systems:**

  If identities cannot be correlated across multiple systems, implementing a globally unique identifier (GUID) is essential to link them effectively.

- **Contractors Without Defined Roles:**

  For contractors who lack specific job roles or titles, additional attributes must be assigned to guide appropriate access permissions.

- **Validate:**

  After the operating model is defined, SDG finalizes user stories, design details are drafted, and plans for construction and deployment are laid out. At this point a technology is chosen.

- **Construct:**

  Implementation of the chosen technology is conducted in this stage. SDG adheres to a disciplined DevOps process. Playbooks are written, staff is trained, systems are tested, and end users are made aware of the changes to come. Construction is agile, and priority follows a line that delivers the target business value quickly and repeatedly.

- **Deployment:**

  As components of the migration program progresses, user acceptance testing (UAT) is conducted, migration plans are exercised, and organizational change management tasks are invoked. Having predefined metrics that align with the organization's business objectives for measuring success, those metrics are now tracked to ensure the value is being realized.

CONCLUSION

Healthcare organizations face significant challenges in managing access for diverse user groups originating from multiple information sources, accessing critical systems across various locations. Issues like duplicate account creation or unintentionally removing access from all locations when it's needed only in one remain persistent problems. SDG, a trusted provider of Identity Governance and Administration (IGA) solutions with extensive healthcare expertise, offers tailored guidance through the assessment, design, and implementation of an Identity Hub solution. This approach helps streamline identity management and resolves complexities introduced by multiple authoritative sources.

ABOUT SDG

SDG is a leading provider of advisory, transformation, and managed services that enable organizations to confidently execute identity, threat, and risk management solutions to identify and mitigate risk, protect assets, and grow securely.

To learn how an Identity Hub can help your organization email us at solutions@sdgc.com or call us at +1 (203) 866.8886.

SDG
75 North Water Street
Norwalk, CT 06854
203.866.8886
sdgc.com