Accurate Patient Identity

A Complete and Trusted Patient Identity is the Basis for Health Information Exchange, Continuity of Care and Patient
Providing an accurate, timely and complete set of demographic details are hallmarks of a strong identity.

A complete and trusted patient identity is the basis for health information exchange, continuity of care and patient safety. Without it, the healthcare industry struggles to ensure that each party is sharing information about the same individual. Current patient registration processes are set up to capture patient demographics and generate a reliable record for that patient. However, this process stops short of establishing a highly reliable identity, making it difficult for that patient’s record to be confidently known and shared across the care continuum.

This paper explores the role of Identity Proofing within a health care organization and describes how – and with minimal effort – the process can be enabled at healthcare facilities.

Identity Proofing

Establishing a strong identity foundation begins with identity proofing. The National Institute of Standards and Technology (NIST) defines Identity Proofing as:

The process by which a Credential Service Provider (CSP) collects and verifies information about a person for the purpose of issuing credentials to that person.

The objective of Identity Proofing is to:

• Resolve a claimed identity to a single, unique identity within the context of the population of users the CSP serves.
• Validate that all evidence that is supplied is valid (correct) and genuine (not counterfeit or misappropriated).
• Validate that the claimed identity exists in the real world.
• Verify that the claimed identity is associated with the real person supplying the identity evidence.

There is no federal requirement that strong identity proofing, or any identity proofing-like processes, be performed on patients today. However, the importance of identity proofing has been outlined by the National eHealth Collaborative in conjunction with the Office of the National Coordinator for Health Information Technology (ONC):

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. All manner of access stems from the application of a user’s credentials, if identity proofing and authentication are not implemented effectively, there is a negative downstream effect on exchange organizations and providers make numerous decisions based on identity within several security controls including access, encryption, auditing, and non-repudiation (digital signatures and authentication). As electronic health information exchange between different organizations and providers grows, it is essential to focus on these key building blocks of security and how trust with respect to identity controls can be improved.1

NIST has published an official guideline entitled “Electronic Authentication Guideline”, or most commonly known as NIST Special Publication 800-63-2.2

It is from this source document that the foundation for identity proofing, and authentication standards and regulations begin. This guidance continues to mature and the updated version 800-63-3 is anticipated to be released in 2017.3

Levels of Assurance (LOA) describe a scale outlined by NIST, from 1 to 4, that conveys the extent to which the individual’s identity has been proofed (the patient is who they say they are) and the degree of confidence that the individual who uses the identity authenticator (aka “token”) is the individual to whom the authenticator was issued. Within the 800-63-2 guideline, NIST defines 4 Levels of Assurance:

- LOA1 – Little to no confidence in the asserted identity
- LOA2 – Some confidence in the asserted identity
- LOA3 – Strong confidence in the asserted identity
- LOA4 – Very High confidence in the asserted identity

At the time of this paper’s publication the proposed NIST scheme (800-63-3) for separating Level of Assurance (LOA) into Identity Assurance Levels (IAL) and Authenticator Assurance Levels (AAL) has not yet been finalized.4

Today, most patient identities are proofed at LOA1 or LOA2. While the patient is asked to provide a copy of their driver’s license or government issued identity document during the registration or check-in process, these artifacts are seldom verified externally to confirm to a high degree of authenticity. It is recommended that for the purposes of accurate, reliable health information exchange and patient safety that LOA3 be adopted for patient and caregiver identities.
The Patient Identity Proofing Process

How it works:

1. The patient completes the health care organization’s (HCO) registration form, and provides supportive, verifiable identity documentation in the form of their driver’s license, state issued ID card, passport, etc.
2. The properly trained registration specialist inspects the identity document(s) along with the registration information supplied by the patient applicant.
3. The clerk, using a Federated Identity, Credential and Access Management (FICAM) approved identity proofing service, verifies the patient’s identity and address. These FICAM approved services are supplied by companies like Equifax, TransUnion and others, and reference authoritative sources to substantiate the data provided.
4. Once the individual’s identity has been properly verified, the registration specialist can electronically request via Kantara or SAFE BioPharma approved CSPs an identity credential.³
5. The issued credential is bound to the identity token that is issued to the patient. The token, in turn, is affiliated with the patient’s medical record at that facility.
6. Every time the patient uses their identity token (also known as an “authenticator”) the CSP reconfirms the individual’s credential.
7. The token also invokes the patient’s medical record preventing the creation of duplicate or overlaid records.
8. All participants within the CSP’s ecosystem can now take advantage of this trusted identity and can be confident that the individual presenting this token is who they say they are. All share in a single understanding of the patient’s identity.

Identity Proofing vs. Patient Record

Matching

While the process of identity proofing concerns collecting and verifying personal data, patient matching, or patient record matching, is the process by which two or more records are compared to determine if they belong to the same individual.

Both processes are necessary to resolve an individual’s identity within the HCO.

How it works:

Patient record matching typically involves a combination of deterministic and probabilistic logic (found in enterprise master patient index [EMPI]) and master data management (MDM) offerings) that electronically compares files to determine the likelihood that two or more records are a match and belong to the same individual, or are not a match and belong to different individuals.

A Federated Identity Ecosystem

An absolute identifier that can belong to only one person establishes the foundation upon which data sharing can be built. In order for this to work, the identifier must be able to be shared across all systems and facilities.

Today, every healthcare organization and their respective Health Information Technology (HIT) systems have a specific set of identifiers for their patients and, while these identifiers may be reconciled within that enterprise via EMPI, they also need to be accurately recognized and accepted across the entire care community in order to be truly useful. The concept of a federated identity ecosystem allows an individual’s trusted identity to be shared nationwide. The Identity Ecosystem Steering Group (IDESG) built around National Identities in Cyberspace (NSTIC) principals, envisions an overarching set of interoperable standards, risk models, policies and requirements that structure an identity ecosystem.⁶ It is within this ecosystem that a trust framework specific to the needs of the healthcare community can be established. It is this design that holds the most promise for a reliable, federated patient identity system.
For more information on this topic stay tuned for the upcoming HIMSS white paper to be published by the Identity Management Task Force.

**About this Brief**

This brief was developed by Catherine Schulten, VP of product at LifeMed ID to inform the audience (HCOs, Providers, CIOs, etc.) that reliable patient identity is essential for so many processes that the health care industry relies on.

Patient identity is the first, and most important, step in a successful care model. The industry must ensure the collection and verification of reliable data at every point of care. If the industry is not successful with this concept, all subsequent processes fail; including record retrieval, revenue cycle, analytics, population health and others.

LifeMed ID enables accurate patient identification by providing AIMe™, a patent pending comprehensive ID platform. AIMe provides confirmation that patients are accurately known as they travel throughout the various stages of care, allowing facilities to confidently welcome patients and successfully manage their identities. Patients simply present their ID which is already linked to their unique records at check-in. This process provided by AIMe allows physicians to reference the right information for treatment.

Additional information can be found on the LifeMed ID website, www.lifemedid.com.

**About the Author**

Catherine Schulten is V.P. of Product Management at LifeMed ID. Catherine has over 25 years of health information technology experience addressing industry challenges from revenue cycle, HIPAA transactions, fraud, waste and abuse, and patient identity management. She has served as a WEDI board member and has co-chaired several WEDI workgroups. Catherine currently serves on the IDESG health care workgroups and the HIMSS identity task force. She has also served as a Task Force Member for the HIMSS National Health Information Infrastructure team and earned a Spirit of HIMSS award. She has been an active participant in key standards development organizations including X12 and HL7. Catherine earned a B.S. in Marketing Management at Virginia Tech.