PATIENT IDENTITY PROOFING

ABSTRACT

Knowing with confidence who your patient is improves patient safety, deters fraud and promotes a better registration experience

Creating Access to Real-time Information Now through Consumer-Directed Exchange

Document Abstract

This document will provide the patient access professional a background on the concept of identity proofing and the steps needed to resolve, verify and validate a patient when they are registered at the Healthcare Organization (HCO).

Organizations will learn the concept of Identity Assurance and the documentation needed to verify a patient and the resulting outcomes of the identity proofing process.

Aims and Objectives

This document aims to provide patient access professionals the knowledge and skills to accurately and reliably perform patient identity proofing within their HCO.

The objectives of this document are as follows:

- Explain why patient identity proofing is important in a healthcare environment and the possible outcomes resulting in poor identity data capture
- Describe the differences between Resolve, Verify and Validate
- Understand the data elements needed to resolve a patient's identity
- Explain the overlap between identity assurance and risk
- Describe the two most common methods to verify an individual
- Give examples of Knowledge Based Authentication (KBA) questions and identity proofing documents
- Know the steps to perform when physically inspecting an identity document
- Describe the results an Identity Management (IM) Service may provide
- Understand how to identity proof a minor, or a person without physical/mental capacity, and the identity documents these individuals may possess
- Explain the correlation between identity proofing and HIPAA Privacy
- Understand the outcomes of a strong identity proofing process

The Expanding Role of Patient Access

Patient access professionals play a vital role in in the healthcare ecosystem. These professionals, who are often the first point of contact a patient has with the health system, are tasked with an enormous number of responsibilities that must be performed consistently and accurately at each patient encounter. From registration to scheduling to cash collection, the patient access professional must be proficient in a variety of jobs, all the while providing exemplary customer service. The patient access department, like many departments within the health system, is also under increasing pressure to do more with less. Registering more patients with higher expectations of data accuracy but with fewer staff to perform the operations is not uncommon.

Over the years, technical advances have helped to improve the patient access workflow. Technical solutions that allow real time insurance eligibility checking, automated methods that enable collecting and posting patient payments at the time of service, appointment scheduling optimization software and other technical advancements all serve to assist the patient access professional in quickly and correctly performing their duties.

One task that has always been at the top of the registrar's list is accurately collecting and entering patient data to establish a new record or to update an existing record. This activity is foundational to all subsequent interactions with the patient and his or her record. Patient access professionals are diligent in their efforts to obtain accurate data, from collecting and copying the patient's driver's license and insurance cards to double checking demographic details on file at each patient visit. Fortunately, technical solutions are available to assist the registrar in these tasks. These technical solutions support a concept known as *Identity Proofing*.

Identity Proofing is not a new idea. It is also an activity that is encountered when one applies for a credit card, establishes a checking account or secures new employment. **Identity proofing is simply the process of verifying that a person is who he or she claims to be**.

Patient Identity Proofing

Patient identity proofing is the process whereby a patient access professional gathers, inspects and verifies via 3rd party the claimed identity documents and details of a patient who is being registered.

The workflow for strong identity proofing need not be onerous for the registration staff nor the patient and adheres to existing best practices for patient onboarding.

The following material explains why identity proofing is important, the national guidelines and best practices that currently exist and outlines the identity confirmation steps that should be performed when registering a new patient or confirming the identity of an existing patient.

Why Patient Identity Proofing is Important

"Trust but Verify" is sage advice. While a source of information provided by patients might be considered reliable, one should perform additional research to verify that such information is accurate. While most patients checking in for service are who they claim to be and will provide accurate information during their registration, there will be some individuals who will provide, intentionally or sometimes unintentionally, bad information about their demographics or insurance coverage. It's up to Patient Access to ensure this doesn't happen.

Reasons for a patient to unintentionally supply bad information:

- Forgetfulness, confusion
- Physical or mental inability to provide sufficient or correct details at the time of service
- A mistake made by a patient when writing down information on a registration form
- Registration data that is supplied inaccurately by a family member or friend

Reasons for intentionally providing bad information:

- An attempt to ensure privacy
- Registration fatigue or unwillingness to provide details because it was provided at previous visits
- Mistrust in the healthcare organization's ability to keep their personal information secure
- Attempt to use a fraudulent or stolen identity as their own.

Patient access professionals are the individuals on the front line who deter inaccurate identification and confirm the inclusion of accurate identity details into the patient's record.

When incorrect personally identifiable information (PII) is included in a patient's record the following are potential outcomes:

- Inability to locate a record
    - When staff cannot identify an existing record, a new record may be established creating a duplicate record situation
- Wrong record selection
    - When incorrect PII is provided at registration the result may be the wrong record is selected and a duplicate overlay situation occurs
- Revenue cycle disruption
    - When incorrect PII is gathered, insurance claims can be sent to the wrong payer, statements may be mailed to the wrong address and the wrong patient may be billed for services they did not receive
- Time spent on patient record correction
    - Requires staff time spent researching and unwinding the resulting downstream errors
    - Requires staff time to research and correct duplicate and overlaid records
- Data exchange errors
    - Originates from incorrect data points, such as Patient Name, DOB, Address, etc. that are used to establish record matching
- Mistrust in the records and waste of resources
    - When staff experience first-hand the results of bad data, they are more likely to doubt the data contained in the records and may spend unnecessary time re-confirming details from other sources.
- Patient distrust
    - When a patient has their identity credentials misappropriated or they experience the result of their clinical record being duplicated or overlaid, they are left with the impression that the HCO is not well managed and may believe that their clinical care is sub-par
- Incorrect data analysis
    - When duplicate and overlaid records are created, over or under counting unique patient records occurs. In addition, the inclusion of bad addresses will skew reports that rely on ZIP codes segmentation

An approach to patient registration that includes strong identity proofing techniques helps to eliminate the inclusion of unreliable PII and promotes accurate identification.

Background

In January 2018, Health and Human Services (HHS) published a draft specification known as the "Trusted Exchange Framework and Common Agreement" (TEFCA). This specification – once final – will define standards for interoperability as required by the 21st Century Cures Act. TEFCA, among other things, calls for individuals to be identity proofed to a level known as NIST Identity Assurance Level 2 (IAL2).

NIST, founded in 1901 and a part of the U.S. Department of Commerce, is one of the nation's oldest scientific laboratories. Within their purview they research and publish guidelines on identification and authentication for all entity types that need to establish confidence in their user and consumer communities.

Other groups such as NSTIC (National Strategy for Trusted Identities in Cyberspace) and the IDESG (Identity Ecosystem Steering Group) also point to the NIST guidelines in their efforts to establish a common model for strong identity and authentication across the nation.

In 2013, NIST published a recommendation entitled "*Electronic Authentication Guideline*", most commonly known as NIST Special Publication 800-63-2.

This guidance has matured over the years and version 800-63-3 was published in June 2017 and is the current specification to be applied in the U.S. for digital identity. It is from this source document that the foundation for identity proofing and authentication standards and regulations begins.

Identity Assurance

NIST defines 3 levels of identity assurance: IAL1, IAL2 and IAL3. Each level provides increasing assurance as to the strength of the individual's identity.

When a subject is identity proofed, the expected outcomes are:

- *Resolve a claimed identity to a single, unique identity within the context of the population of users the Credential Service Providers (CSP) serves.*
- *Validate that all supplied evidence is correct and genuine (e.g., 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.*

Identity Assurance Level 2 (IAL2) is defined within NIST 800-63-3:

> *IAL2 allows for **remote** or **in-person** identity proofing. IAL2 supports a wide range of acceptable identity proofing techniques in order to increase user adoption, decrease false negatives (legitimate applicants that cannot successfully complete identity proofing), and detect to the best extent possible the presentation of fraudulent identities by a malicious applicant.*

NIST further describes the requirements for IAL2 in the following diagram:

Table 4-1 IAL Requirements Summary

Requirement	IAL1	IAL2	IAL3
Presence	No requirements	In-person and unsupervised remote.	In-person and supervised remote.
Resolution	No requirements	The minimum attributes necessary to accomplish identity resolution. KBV may be used for added confidence.	Same as IAL2.
Evidence	No identity evidence is collected	One piece of SUPERIOR or STRONG evidence depending on strength of original proof and validation occurs with issuing source, or Two pieces of STRONG evidence, or One piece of STRONG evidence plus two (2) pieces of FAIR evidence.	Two pieces of SUPERIOR evidence, or One piece of SUPERIOR evidence and one piece of STRONG evidence depending on strength of original proof and validation occurs with issuing source, or Two pieces of STRONG evidence plus one piece of FAIR evidence.
Validation	No validation	Each piece of evidence must be validated with a process that is able to achieve the same strength as the evidence presented.	Same as IAL2.
Verification	No verification	Verified by a process that is able to achieve a strength of STRONG.	Verified by a process that is able to achieve a strength of SUPERIOR.
Address Confirmation	No requirements for address confirmation	Required. Enrollment code sent to any address of record. Notification sent by means different from enrollment code.	Required. Notification of proofing to postal address.
Biometric Collection	No	Optional	Mandatory
Security Controls	N/A	SP 800-53 Moderate Baseline (or equivalent federal or industry standard).	SP 800-53 High Baseline (or equivalent federal or industry standard).

It is the intention of this document to educate the public and provide healthcare organizations with clarity around how to achieve identity assurance level 2 for their patients.

Identity Proofing and Risk

Different business types have different tolerances to risk.

Identity information is classified along the dimensions of Risk and Assurance. Risk means how bad would it be if the identity information was wrong or if it was exposed and Assurance meaning how confident are you that the identity information is accurate. The higher the risk, the more important it is that the identity information about the individual be accurate. Because healthcare deals with patient safety the tolerance for risk is very low and the need for identity assurance is high.

Low Assurance Identity Proofing: no requirement for an individual's identity to be proven. Ex: creating an online email address through Gmail there is no requirement that your identity be known.

High Assurance Identity Proofing: in-person identity proofing is required; identity attributes must be verified by an authorized and trained representative. Ex: registering to access an online patient portal or setting up a PayPal account there is a requirement that your identity be known.

The sensitive nature of healthcare data and HIPAA Privacy and Security regulations suggest that a strong level of identity proofing is the most appropriate level to which patient should be known.

Today there is no HIPAA or federal requirement that strong or any identity proofing be performed on patients. However, the National eHealth Collaborative in conjunction with the ONC have noted the importance of identity proofing:

"*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 as 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.*"

https://www.healthit.gov/sites/default/files/identitymanagementfinal.pdf

Foundations of Identity

NIST explains that Identity Proofing is the process used to *verify an individual's association with a name*. The basics of identity proofing are to Resolve, Verify and Validate.

- Resolve: capture and disambiguate the data to identify one unique identity
- Verify: Establish that the identity exists
- Validate: confirm that the identity is correctly associated with the individual over time

Resolve

The first step in identity proofing is confirmation that no other individual has the same set of attributes. This requires that a set of demographic details that can belong to only one person are gathered and documented. The attributes selected for patients have qualities that contribute to identity resolution including completeness, validity, distinctiveness, comparability and stability.

- **Completeness**: the likelihood that this attribute is captured and available
- **Validity**: Probability that this attribute is known to be true and is seldom a default value. An example of a default value is all 9's for a phone number or a ZIP code of 12345
- **Distinctiveness**: The trait is highly unique such that no other person is likely to have the same value. Gender, M or F, is not distinct while a 10-digit phone number is very distinct.
- **Comparability**: The trait is structured or in a reliable, consistent format. An example of a distinct format is how a phone number is captured in the format "(nnn) nnn-nnnn" and can be easily compared to other phone numbers in a table
- **Stability**: The likelihood of the trait staying the same. For example, a DOB doesn't change over time while a home address is likely to change.

With these qualities in mind, identity resolution for a patient consists of gathering the following specific set of details:

- **Patient First and Last Name**: The legal name by which this person is known is required. A Middle Name or Middle Initial is helpful for identity resolution and is encouraged as an additional

component of the name. Nicknames, abbreviations, etc. are not appropriate and Name Prefix or Suffix do not contribute to identity resolution.

- **Date of Birth**: The month, day and year of the individual's date of birth is required
- **Administrative Gender**: The distinction of Male, Female or Unknown is required
- **Current Address**: 1st and 2nd line as appropriate along with City and State
- **ZIP Code**: The 5-digit postal code associated with the patient's primary or home address is required
- **Phone Number**: The 10-digit primary phone number for a patient is required

SSN is not included in this set of attributes. The collection and use of that unique identifier is discouraged because of the potential for it to be used in identity theft schemes. Many HCOs are no longer collecting the full SSN, or maybe only collecting the last 4 digits. Also, the MARCA regulation requires that CMS remove the use of the patient's SSN from Medicare cards by April 2019.

With this set of demographic details, a patient's identity can be resolved to a high degree of certainty at or above 98%

Source: Sequoia Project: http://sequoiaproject.org/framework-for-cross-organizational-patient-identity-matching/

Verify

There are two common methods used to verify a person's identity. One is a dynamic, knowledge-based authentication (KBA) process that supplies a set of questions that only the true individual can correctly answer. The other method for identity verification is for an authorized person to gather and inspect certain forms of documentation that help to proof the individual presenting them.

Identity Documents

"In the United States, there is no national method for verifying a person's identity. Each government credential issuing authority specifies a minimum set of documentary evidence that must be produced and in some cases, they conduct face-to-face meetings in a discovery process aimed at verifying claims made. But the procedures are not uniform."

-ANSI, Identity Theft Prevention and Identity Management Standards Panel IDSP, 10/2009

Identity documents created by state and federal agencies, along with some private institutions, are most often used to support an individual's identity claims. While these documents are created for other purposes, they are issued by trusted, authoritative sources which makes them reliable and capable of being validated.

Examples of Superior Identity Documents:

Document	Issued by	Purpose
Driver's License	State Department of Motor Vehicles	Convey driving privileges
State ID Card	State Department of Motor Vehicles	Provide a way for a state resident to reveal identity to law enforcement and/or to obtain state services
Passports	US State Department	Support for international travel

Military ID Card	Dept. of Defense	For military base or secure building access, to ID the individual for access purposes

Reliable identity documents contain a photo of the individual, the name of the entity that establishes the document, an expiration date, the individual's full, legal name.

The most common form of verifiable documentation available for adult patient identity proofing is the state issued driver's license (DL) or ID card which has a picture of the card bearer on it.

The following are qualities of a Driver's License:

- **Ubiquitous**: Held by over 245 million people, or around 90% of the United States population. A passport on the other hand is held only by 46% of the United States population
- **Known standards**: The REAL ID Act passed by Congress in 2005 recommended that the Federal Government "set standards for the issuance of sources of identification, such as driver's licenses". Only a few states are not yet in compliance, including American Samoa, Minnesota, Missouri and Washington.
- **Requirements to obtain one**: Individuals must first present a set of identity proofing documents that are in turn verified
- **Human readable details**: Display's the individual's:
    1. Full legal name
    2. Signature
    3. Date of birth
    4. Gender
    5. Unique ID Number
    6. Principal residence address
    7. Front facing photograph
- **Machine readable details**: Has a barcode, magnetic stripe or smart chip that allows encoded data to be read and parsed by a machine
- **Anti-spoofing features**: Contains a variety of design elements that deter fraudsters from creating a counterfeit document, such as holograms and watermarks

While the driver's license and state issued ID card are the most useful identity document to verify the identity of an adult patient, they don't apply to every person. Verification of a minor, an individual not from the United States or other identity exceptions will be addressed in an upcoming section.

Validate

It is necessary to confirm that the evidence presented applies to the individual presenting it. This process is called *validation.*

Validation is aimed at deterring and detecting identity fraud, reducing identity uncertainty and binding that identity to the person who legitimately claims it.

Like confirming the details listed on a job applicant's resume, it's important not to take the document and asserted details at face value but to analyze and confirm that what has been presented is true.

In-person identity validation is performed by an individual who is specifically trained to thoroughly and accurately perform the validation steps. Within the healthcare ecosystem, the Patient Access professional

is the individual who is best positioned to interface with the patient, to collect identity documents and to perform the validation steps.

Identity Management (IM) services also play a key role in validation. These services can ensure the uniqueness of the person and either have direct, first-hand knowledge of the identity details or can corroborate the accuracy of the asserted details. In healthcare, the use of 3rd party IM services are most common.

An Identity Management service could be a vital records agency, a data broker, a credit bureau or any other similar group that maintains trusted identity details about a person.

The IM Service will receive the patient's demographic information from a known source (the healthcare organization) and will conduct a set of confirmation checks to ensure that the data presented aligns correctly with the person claiming those details. The service will also check for outliers or warnings that may raise suspicions about the individual's claimed identity.

Example Identity Validation Checks:

- **FTC Red Flag Rules:** Checks to see if this person's identity has been involved in identity theft, has unusual or suspicious activity related to their identity
- **Office of Foreign Assets Control (OFAC) Alerts:** Checks to see if this person's identity is contained on the sanctions list, individuals who are listed as being involved in money laundering, who have financed terrorism or other types of financial dealings related to organized crime
- **Social Security Death Index:** Checks to see if this person's SSN is contained on the Master Death Registry. This includes the SSN of all United States individuals whose death has been reported

Example Address Validation Checks:

- **Unlikely or Suspicious Address**: Checks determines if a location is a Post Office Box or if this is another location where people do not live, such as a shopping mall or a truck stop
- **Impossible Address:** Checks determines if a location that is not known by the United States Postal Service
- **Address Warning:** Checks determines if a location is known but has additional address parts that are needed to be fully complete and correct. As an example, a street name should have been recorded with a direction like "North" or "NE", an address is in a multi-unit building and the unit # is required or if the address is not a place where a person would like (the address is for a campground or shopping mall)
- **Individual is not known to live at that location:** Checks residential utility usage and other sources to determine if the individual resides at that location

Resolve, Verify and Validate the Patient

Step 1 – RESOLVE

Patient Identity Proofing begins with the capture of the following identity details. Typically, these pieces of data are collected during the patient registration process:

- Full Legal Name
- Date of Birth
- Administrative Gender
- Address including ZIP code

- Phone Number (home or cell)

The following demographic details are often requested during patient registration but are not considered highly useful for the purposes of identity proofing:

- Insurance coverage,
- Guarantor
- Employer
- Occupation
- Email
- SSN (full or partial)
- Marital status
- Mother's maiden name

Step 2 – VERIFY

At this point in the process the Patient Access professional requests the patient's state issued driver's license or ID card. State issued photo IDs are preferable since they help to confirm that the identification document belongs to the individual presenting it. The first step in verification is **physical card inspection**. The registrar should physically hold and inspect the document presented to confirm that it appears to be a true document. The registrar should determine if the photo on the card matches the individual standing before them.

F-L-A-G is a simple way to remember how to properly manually check an ID.

F – Feel

Feel for raised edges, glue lines or bumpy surfaces, feel for cut-out and pasted information and check the thickness of the ID. *Does it seem flimsy or too thick?*

L – Look

Check the photograph. Check the expiration date. Expired IDs are not acceptable. *Does it look like the same person who presented the card*? *Is the State seal and holographic information located on the card and in the correct place? Are the corners and edges of the card straight or crooked?*

A – Ask

If the look and feel of the card seem suspicious, ask questions. For example, ask the patient to state their birth month. If they state a number instead of a month they may be lying (the person says "8" instead of "August"). Ask how old they will be on their next birthday. A person who is lying will struggle to quickly answer this question.

G – Give back

Even if you think the identity document is fake you must give it back. Ask for a different identity document since the one provided appears to have issues. Document the incident since this may be an indicator of a person attempting to commit insurance fraud, identity theft or drug seeking behavior.

The next step in verification involves **documenting the information** contained on the card to provide evidence that the artifact was inspected.

Ways to document inspection information

1) The registration clerk can transcribe the Driver's License Number, Expiration Date and Driver's Name/Patient's Name into a log along with the registration clerk's signature and the current date to indicate the card was inspected
2) The front and back image of the card can be scanned into a document imaging system with an associated date/time and end user stamp. The registrar indicates they have inspected the identity document
3) The card can be verified by a 3rd party service by scanning or electronically reading the ID document and electronically submitting the details on the card to an ID verification service. The service will run a set of forensics on the data presented on the card and the card image and will confirm if the card is correctly formatted or if it is false.

Step 3 – VALIDATE

The 3rd and one of the most crucial steps in strong patient identity proofing requires that a 3rd party service independently validates or confirms this individual's claimed identity.

If an IM service is used, then the registrar receives confirmation from a 3rd party related to the patient's claimed identity and address. The IM service provides more details than the KBA by providing human readable alerts and warnings. This allows the registrar to correct and re-submit some of the details if a suspected false-positive is produced.

A common example of real-time alerting occurs when a patient has recently moved and the identity service does not have the new address on file for this person. To correct this situation, the patient will need to update one of their accounts or records (update the mailing address for one of their credit cards or update their address with the DMV) to provoke the change within the credit bureau services. It can take several days for the updated information to make its way to the IM service and for them to update their records.

Trusted Referee Process

Since not every patient can produce the material required to be strongly identity proofed, NIST has included a Trusted Referee Process by which an individual may be identity proofed through other measures. Trusted Referees are described as "*notaries, legal guardians, medical professionals, conservators, persons with power of attorney, or some other form of trained and approved or certified individuals — that can vouch for or act on behalf of the applicant in accordance with applicable laws, regulations, or agency policy*".

A health care organization that wishes to employ a trusted referee process will need to document their policies and procedures to perform this method as well as the lifecycle by which the referee receives and retains their status.

The inability to proof a patient's identity is not a reason to withhold necessary healthcare services.

Following are common situations that require alternate methods of identity proofing:

Identity Proofing Minors

Minors are a prime example of individuals who may not have the document evidence or identity history needed to sufficiently proof themselves to a high degree of confidence. Minors have varying degrees to which they can be identity proofed.

The legal definition of a minor in the U.S. is someone under the age of 18. Minors are under the control of their parents or legal guardians until they attain the age of majority, at which point they become legal adults. In most states this is upon turning 18 years of age. However, in special circumstances, minors can be freed from control by their guardian before they reach the age of majority either through a process called emancipation or through marriage.

Minors between the ages of 16 and 18 may have a driver's license or a state issued ID card. Some may have already have begun to establish records with the credit bureaus from jobs that have tax withholdings or through the purchase and/or registration of a car. Patients such as these who have identity documents are usually able to be identity proofed in much the same manner as an adult patient.

Children under the age of 16 however, will not have a driver's license although some may have a state issued ID card or other forms of documentation.

Identity Proofing Documents for Young Children

Proof of identity for a child typically requires a certified copy of a birth certificate or other reliable proof of the child's identity and age.

The following documents may also be acceptable forms of reliable proof. *Keep in mind that state laws may vary*:

- Certified copy of a birth certificate
- Birth registration card
- Notification of birth (hospital, physician, or midwife record)
- Passport
- Copy of placement agreement or entrustment agreement from a child placing agency including foster care and adoption agencies
- Record from a public school
- Certification by a principal, or his designee, of a public school in the United States that a certified copy of the child's birth record was previously presented
- Copy of the conferring temporary legal custody or entrustment agreement of a child to an independent foster parent
- Child identification card issued by the Department of Motor Vehicles (DMV)

In some cases, minors will not have these documents available and may not be able to be strongly identity proofed. The child's parent or guardian should be identity proofed to serve as their delegate. The minor will need to be accompanied by and should have their identity record linked to the adult parent's or guardian's identity record who can be proofed.

Identity Proofing Individuals without Physical or Mental Capacity

Some patients, due to lack of physical or mental capacity (either permanent or temporary), will not be able to provide sufficient documentation to be identity proofed. These patients will need a person who can serve as their delegate, such as a spouse, an adult child, a caregiver, etc., to identity proof both themselves and the patient. The delegate's proven identity should be associated with patient who cannot be proofed.

Identity Proofing Individuals who are Unable to Provide Appropriate Documents

Some patients will not have access to the appropriate documents to support their identity.

Common examples of individuals who cannot support their own identity include:

- A patient who forgets to bring their wallet with their driver's license in it
- A patient visiting the United States from another country who has a foreign passport but doesn't possess a United States form of identity
- A patient who may be in the country illegally and doesn't carry proof of identity
- A patient with an expired driver's license

The registrar is advised to attempt to collect appropriate documents upon the patient's next visit to the facility and to make a note within their registration system that this individual has not been identity proofed.

Since some attempt at identity proofing is better than none, the registrar should still attempt to collect demographic details needed to resolve their identity and to collect some form of identity documentation.

Fair or Weak identity documents that do not strongly identify the patient include

- Expired driver's license
- Insurance card
- School ID card with a photo
- Employer issued ID card with a photo

These identity documents may be used to support identity assurance to a lower level or may be used in combination to support a stronger level of identity.

Identity Proofing a Patient Delegate or Individual who is Not a Patient

Some registration scenarios involve the collection of identity details for a person who is not the patient.

Examples of these individuals include

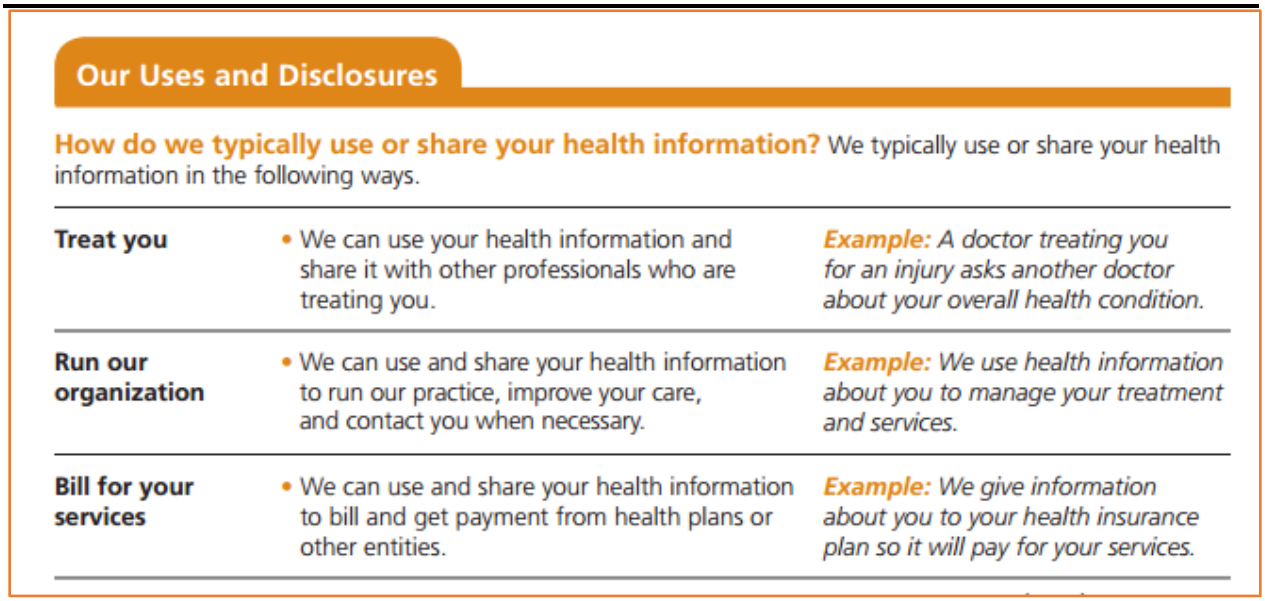
- Parent of a minor child
- Adult family member or caregiver of a patient without physical or mental capacity
- Spouse or other family member who shares in the care of a patient

In some cases, the delegate is not and may not ever be a patient at that healthcare organization. However, it is necessary to identity proof the delegate as they will be the individual who will serve as a proxy for the patient. A patient delegate is a person who is assigned the duties of asserting the patient's identity and may also be granted access rights to the patient's portal. Keep in mind that a patient's delegate is not necessarily the same as the patient's guarantor or even their legal guardian/power of attorney.

Identity Proofing and Consent

While written consent is not legally required to perform identity proofing steps, many organizations obtain it. Every healthcare organization today obtains all manner of consents when registering a new patient. Identity proofing services fall under the requirement related to gathering and sharing information for purposes of treatment, payment and healthcare operations (TPO).

The standard *HIPAA Notice of Privacy Practice* explicitly gives the healthcare organization the right to use or share the patient's health information for operational purposes. In other words, the hospital or practice can use and share the patient's information to effectively run their organization, to improve the patient's care and to contact the patient when necessary.



Our Uses and Disclosures

How do we typically use or share your health information? We typically use or share your health information in the following ways.

Treat you	• We can use your health information and share it with other professionals who are treating you.	*Example: A doctor treating you for an injury asks another doctor about your overall health condition.*
Run our organization	• We can use and share your health information to run our practice, improve your care, and contact you when necessary.	*Example: We use health information about you to manage your treatment and services.*
Bill for your services	• We can use and share your health information to bill and get payment from health plans or other entities.	*Example: We give information about you to your health insurance plan so it will pay for your services.*

Each HCO is different, so it will be up to the Patient Access professional to understand their organization's consent requirements for identity proofing.

Identity Proofing and its Impact on the Patient's Credit Bureau Consumer Report

When an IM service is provided to the healthcare organization by one of the credit bureaus (Experian, TransUnion, etc.), there is no resulting impact to a person's credit score. Neither the query nor the resulting pass or fail of the identity proofing transaction impacts the patient's credit score.

The Benefits of Knowing your Patient's Identity:

- Promotes patient safety
- Duplicate and overlaid records that arise from misidentification are avoided
- Strongly deters fraud and identity theft
- Establishes a foundation for the issuance of identity tokens
- Confirms identity before the issuance of patient portal access credentials
- Promotes more accurate record matching across disparate entities since a reliable set of demographic details have been established
- Other "byproducts" of identity proofing include
    - Enhanced revenue cycle experience (billing and correspondence go to the correct address)
    - The true age of patient is known
    - Capture of the photo from the driver's license can be used for other identity purposes
    - Patients attempting to be seen anonymously can be spotted and an alternate process that supports their need for anonymity can be accommodated
    - Patient satisfaction in the onboarding experience
    - Staff satisfaction on the reliance on the patient identity data

REFERENCES

National HIE Governance Forum Identity and Access Management for Health Information Exchange

https://www.healthit.gov/sites/default/files/identitymanagementfinal.pdf

NIST Special Publication 800-63-2

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf

NIST Special Publication 800-63-3 (Draft)

https://pages.nist.gov/800-63-3/sp800-63-3.html

Workshop Report, Identity Verification, Identity Theft Prevention and Identity Management Standards Panel October 2009:

http://fileopen.ansi.org/encservice/FileStreamer.ashx?TaskID=8fc8119be274476bb3eeb4985e3413a7

National Identity Proofing Guidelines (Commonwealth of Australia, 2016)

https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/NationalIdentityProofingGuidelines.pdf

Design Principles and Guidelines for Secure DL/ID Cards (SCDP)

http://www.aamva.org/WorkArea/DownloadAsset.aspx?id=5523

HIMSS Patient Portal Identity Proofing and Authentication

http://www.himss.org/sites/himssorg/files/Patient_Portal_Identity_Proofing_and_Authentication_Final.pdf

i9 Acceptable Documents

https://www.uscis.gov/i-9-central/acceptable-documents/list-documents/form-i-9-acceptable-documents

Sequoia: A Framework for Cross-Organizational Patient Identity Matching

http://sequoiaproject.org/framework-for-cross-organizational-patient-identity-matching/