USE CASE #	New Patient Registration Identity Assurance, in Person *(FUTURE PROCESS)*
Goal in Context	To confirm the identity of a new patient during the registration process. This process may be performed in-person at the healthcare facility or remotely via self-service app
Scope & Level	Patient Access: Registration & Appointment Scheduling
Preconditions	The patient is an individual who is competent and can participate in the process of providing personal identifiable information. The patient is willing to provide information Patient has some form of identity evidence (driver's license, passport) HCO has contracted with an Identity Service (IDAAS) that is integrated with the EMR or the EMR is imbedded with patient identity assurance functionality.
Success End Condition	The patient's identity has been confirmed and a unique, not-duplicated record is established within the health care organization's medical record and/or billing system. Patient's identity has been assured to IAL2.
Failed End Condition	The identity of the patient is not confidently known resulting in possible duplicate record, overlaid record or "skeleton" record that contains a thin amount of PII. The PII contained within the new record is not reliable and may result in downstream adverse events: • improper billing/insurance claim filing, • patient safety issues (death or harm), • breach of patient privacy, • liability because of poor business practices around patient identity assurance
Primary, Secondary Actors	Registrar and Patient Registered Health Information Technicians and Administrations, Clinicians, Payers
Trigger	A New Patient (an individual who has not previously had services provided by the healthcare organization and does not have a medical record established) arrives at the HCO for a clinical visit There are 2 types of initial visits: **Scheduled** and **Walk-In**. A scheduled visit is one where the HCO and Patient have arranged for a specific date/time for the visit. Typically, some amount of patient PII has been provided ahead of time by

	the patient or someone on their behalf to hold the time slot on the healthcare provider's schedule. (example, a patient makes an appointment to see a primary care physician for a physical. Patient provides their full name, DOB and cell phone number to hold the appointment)
	A walk-in visit is one where the HCO had no knowledge beforehand that the patient would be arriving for services (example, a patient arrives at the Emergency Department for a broken finger)

DESCRIPTION	Step	Action
Patient supplies PII	1	The Registrar ask the New Patient to provide his/her PII as part of the registration process. This process may involve the patient filling out a form in the waiting room or being interviewed in a private area by the Registrar. In either case, the patient provides a set of PII to establish their record. PII includes: Name, Address, DOB, Sex Recommended: phone number, email address, identity evidence document # (DL #), Insurance name/ID/Group# Sometimes collected: Mother's maiden name, City of birth Excluded: SSN Not in scope for an identity use case but data that may be collected at the same time as the registration: Clinical data, NOK, Acknowledgements, and other healthcare specific forms included in the registration process

Registrar enters PII into Identity Service application	2	The Registrar enters the patient's PII into the HCO's identity service application.
		
		    The IDAAS is a service that is integrated with the HCO's EMR.
		
		    The Registrar can enter the patient's PII data by typing it in or the Registrar might use and OCR process to "scrape" the data from a form of identity evidence

Existing record check by IDAAS	3	The Identity Service will determine if a likely record for this patient already exists within the EMR and/or within the Healthcare Enterprise
		
		    An existing record check is typically performed by searching for records with same or nearly the same set of PII as the patient
		
		    John Smith, 05/11/1985, 123 Main Street

		Jon Smith, 05/11/1958, 87 Elm Street *Johnny Smith, 04/11/1972, 3489 Main Street*
Confirmed new patient	4	If no plausible existing record is present in the EMR, the identity service application prompts the Registrar to perform a set of identity assurance steps: A) **Collect, Check and Copy** the patient's identity evidence. Is the document expired? Does it appear fake? B) **Compare** the image on the documents to the card bearer, are they the same person? C) **Confirm** identity details (legal name, address, contact details) from a trusted, authoritative source
Patient identity evidence confirmation	4A	The patient gives the Registrar a copy of his/her driver's license (or other identity document) and the Registrar inspects it This process may be performed *manually* by the Registrar visually inspecting and handling the document, or May be performed *electronically* by taking an image of the document and sending that to a 3rd party service that authenticates the document as being valid (not fake) nor expired
Photo of Patient captured and biometrically compared to the image on the identity evidence	4B	The identity service application prompts the registrar to confirm the document bearer is the same as the patient. This may involve taking a picture of the patient Registrar can *manually* compare the photo on the document to the person standing before them, or A photo of the patient, taken at the point of registration, is electronically biometrically compared to the photo on the identity document confirming the images are of the same person
PII confirmed	4C	The PII contained on the document is electronically verified by authoritative sources as being current and belonging to this individual Legal Name Address of residence DOB Contact details (email, phone number(s))

Determination of IAL	5	The identity service determines if the assurance process is complete and if all steps are "passed" then the identity assurance level for this patient is recorded (IAL1 or IAL2) and associated with this individual in the IDAAS cloud
		Use of a Registration Authority may be appropriate to record the individual's IAL
Patient Insurance confirmation	6	The patient electronically exchanges their digital insurance card with their provider.
		PUSH: The patient's health insurance payer provides a mobile app that the patient has placed on his/her smart phone
		The patient selects "share insurance card" from this app and is prompted to enter or select the name of their healthcare provider
		The patient's insurance information is electronically shared with the HCO's EMR
		PULL: The patient has indicated through their payer's application that they consent to share their insurance coverage details with their care providers
		The Registrar sends a query through the EMR to the patient's healthcare payer to retrieve this individual's coverage details
		Because this workflow requires the patient to login to the payer's site to use the app or consent to share, there is some degree of confidence that the insurance details belong to this individual and are not stolen/fraudulent
Identity record added into the EMR	7	The IDAAS determines the patient's IAL. Regardless of IAL determination or Insurance coverage, the new record is established within the identity and is simultaneously added into the HCO's EMR. The resulting new MRN# created in the EMR is shared between the EMR and the Service

Definitions:

New Patient – an individual who has not previously had services provided by the health care organization, does not have a record established at the HCO

Existing Patient – an individual who has previously received services from the HCO and has a record established

Health Care Organization (HCO) – an organization that provides healthcare goods or services in any one of several environments (hospital, clinic, lab, imaging center, pharmacy, durable medical equipment provider, long term care facility, home health care provider, telehealth provider, etc.)

Visit – an episode where the patient engages with a care professional to acquire healthcare goods or services

IDAAS – Identity as a Service, a cloud-based service, in this case integrated with the HCO's EMR, that provides functionality to confirm and authenticate a person's identity. This add on service enhances the patient identity verification process and supports a compliant NIST 800-63A workflow.