It's Not Another Number: Technical Strategies to Accurately Match Patients with Their Data

Demographic Data Standardization: Patient matching relies on the use of demographic data elements; however, demographic fields vary across electronic health records (EHRs) due to a lack of standardized data attributes and an absence of federal EHR certification requirements. Research indicates that the standardization of some demographic data element used for matching including address, US postal code and date of birth (DOB) could further improve patient matching.[1]

Biometric Information: Involves the use of algorithms that include biometric identifiers such as fingerprints, facial recognition, palm scans, and other biometrics to identify patients. Few institutions in the U.S. currently use biometrics to match patients to their health information and there are few (if any) accepted standards for biometrics.

Algorithmic Patient Matching:

> ***Deterministic matching:*** Involves a unique identifier, sometimes coupled with a limited number of non-unique identifiers (like DOB for additional validation) that are compared to identify exact matches. Considered a basic record matching algorithm. Comparisons are usually made based on name, DOB, social security number (SSN) and sometimes gender.
>
> ***Rules-based matching:*** Each data element receives a "weight" for how essential it is to match a record. Even if every data element does not match exactly, the records are considered "matched" so long as enough data elements are identical. For example, records are considered "matched" if first name, last name, DOB, and gender match or if last name, address, and date of birth match.
>
> ***Probabilistic matching:*** Compares several (non-unique) field values between records, assigning a weight to reflect how closely the two-field values match. The weights are then added across the fields to indicate the probability of an actual match. May be considered an intermediate or advanced algorithm.[2]

Referential Matching: Leverages additional information from multiple sources, including, but not limited to credit bureaus and US Postal Service to accurately identify patient.

Patient-Driven Solutions:

> ***Patient Verify Identity Information:*** Patient verifies existing identity information such as mobile phone number through a one-time passcode sent by their provider.
>
> ***Consumer-Directed Exchange:*** Patient collects health information in one application and can access and share it with providers.

[1] Grannis, et al. Evaluating the Effect of Data Standardization and Validation on Patient Matching Accuracy. JAMIA. 2019; 26(5): 447-456. Published 2019 March.

Health Record Banks: Provider submits health records to a regional data repository that allows patient and provider access.

Manual Patient Verification: Patient verifies record matches or identifies lack of matches through a patient portal or a software application available in provider's office (e.g.—kiosk, tablet, etc.)

Patient Supplies Record Location Information: Patient provides information on previous care locations that provider uses to identify previous records.

Voluntary Universal identifier: A central, trusted organization issues identifiers but does not store protected health information (PHI). A provider manages identifiers using hardware and software supplied by the trusted organization and interfaces with their existing EHR.

Public Key Cryptography: Patient is issued a public key-private key pair, the public key would be used for record matching as a piece of identity information. At each encounter, the patient would use the private key to prove the public key belonged to him or her.

Knowledge-Based Identity Information: Patient answers knowledge-based questions, which are used with demographics for record matching. Knowledge-based data elements may include mother's maiden name, childhood best friend, and birth city.