The Future of Patient Identification

Executive summary

Are you concerned about the negative impact misidentification has on patient care? Does the compromise of 145 million records at Equifax raise alarms? Are you worried about increased healthcare interoperability without accurate patient identification? Do you think that healthcare will ever achieve its identification goals using probabilistic matching?

We think not. Healthcare requires entirely accurate patient identification at each clinical encounter. Most importantly, a compromised identity must be able to be completely restored. This will only be possible if the industry implements a simple, but profound, patient identification paradigm shift to an "identity first" approach.

Introduction

It is universally acknowledged that accurate patient identification is an essential prerequisite to providing medical care that is safe, efficient, and effective. Despite this consensus, and despite more than 20 years of effort, achieving this goal has remained elusive. Recent events have in many ways made this situation worse. Increasing automation of healthcare delivery and the consequent requirements for interoperability have placed increased demands on patient identification mechanisms. The recent Equifax data breach which compromised the Personally Identifiable Information (PII) of over 145 million people has placed the PII of roughly 40% of the adult population in the US at risk. Breaches within healthcare are occurring at a rate exceeding one a day and impact an average of more than 475,000 individuals per month.

The solution

Analyses of these trends and their root causes have made it clear that the only reasonable hope to achieve healthcare's stated goal of 100% accurate patient identification for every medical encounter is to **implement a fundamental patient identification paradigm shift.** We must move away from relying on PII as the basis for patient *identification* and use it instead for patient *authentication*. The foundations for this shift have been laid in a series of analyses by various healthcare organizations. We have chosen to present our work as an expansion of the requirements expressed by the National Institute of Standards and Technology (NIST) National Strategy for Trusted Identities in Cyberspace (NSTIC) Identity Ecosystem Steering Group (IDESG)[1], one of the many organizations dedicated to addressing problems in the patient identification space.

As part of its Identity Ecosystem Framework (IDEF) the NIST IDESG has identified seven requirements that must be met by all identity solutions: 1) privacy enhancing, 2) voluntary, 3) secure, 4) resilient, 5) interoperable, 6) cost-effective, and 7) easy to use. We have added to these requirements below. We believe compliance with the expanded list is crucial if

[1] https://www.idesg.org/About/Overview.

healthcare is going to achieve an effective and lasting solution to the patient identification challenge. Note that the recent Equifax breach incident dramatically illustrates that the current, PII-based approach to patient identification fails at least requirements three and four.

Healthcare's current patient identity paradigm is based on probabilistic matching of PII. At each medical encounter the patient is expected to provide a set of PII data elements - name, date of birth, Social Security Number (SSN), insurance identifiers, etc. This set of data is then statistically matched against various records in the healthcare organization's database to see if an optimum match exists. If the likelihood of a match is high enough, the patient's identity is considered to have been established and the care process proceeds.

There are many problems with this approach but here we will confine our analysis to the fact that this method does not provide guaranteed accuracy. PII matches are made on a statistical basis, meaning that there is always the possibility of a false positive or a false negative match[2]. It is universally agreed that the goal for accurate identification for healthcare must be 100% accuracy. PII matching can get close to this 100% goal (within 5% in some cases), but can never achieve it. To get to completely accurate identification we must implement a new paradigm.

The new paradigm, 'identity first'

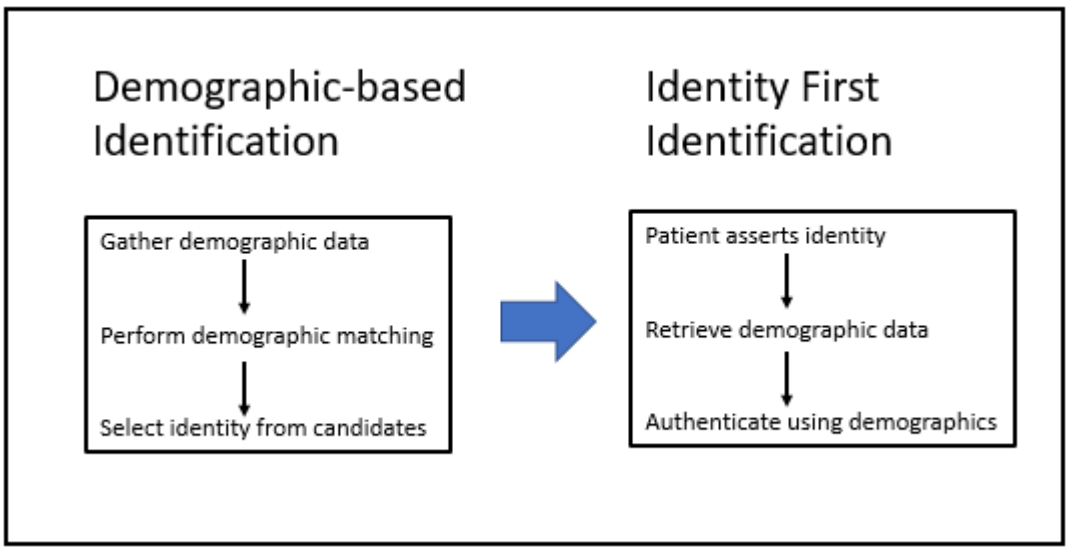

Figure 1

The new paradigm we propose is one that enables a patient to unambiguously *identify* themselves first and then use PII information to *authenticate* that identity. Figure 1 illustrates this paradigm shift. Upon enrollment in the patient identification system, the patient is given a method to unambiguously identify themselves at the start of each subsequent medical

[2] False positive match = two people are improperly matched as being the same person, false negative match = a person is not matched when their data is actually in the system.

encounter. This identification does not depend on PII but instead uses a token that is issued to the patient when they enroll in the system. Once the patient has identified herself (or himself) for an encounter, the healthcare organization can use whatever PII data elements it has established in its own policies to authenticate the patient identity that has just been asserted. This approach means that the patient can use one consistent technique to identify themselves for all encounters. Each healthcare organization can then use whatever set of PII information - name, SSN, birth date, biometric, etc. - it chooses to achieve appropriate authentication of that individual.

Specific identification requirements

The initial seven requirements listed below come from the principles listed on the IDESG website.

1) Privacy enhancing

Healthcare is one of the most sensitive personal information domains. Patients will be unwilling to use any identification system that threatens their privacy. Conversely, patients will want to participate in an identification system that they believe will protect and enhance their privacy. The ability to improve privacy thus becomes a crucial enabler for a patient identification system.

2) Voluntary

In the United States patients have difficulty trusting identification systems that are mandatory, especially those that are mandated by the government. To maximize patient trust – and therefore patient participation – in an identification system, it should be offered in a voluntary manner. However, there will also be specific applications (for example, membership in an insurance plan) where accurate patient identification will be mandatory. Any patient identification strategy must be able to support both voluntary and mandatory approaches concurrently.

3) Secure

The private nature of healthcare information, coupled with increasingly frequent healthcare data breaches – and dramatically underscored by the recent Equifax data loss – make heightened security a critical requirement for the patient identification system. Not only should the system avoid being an increased threat for the loss of PII, it should actively assist in the prevention of PII loss.

4) Resilient

One of the most damaging aspects of healthcare data breaches is that in the current environment it is not feasible to restore a compromised identity to wholeness. Once PII is stolen, that information cannot be retrieved. Any system that relies on PII to determine identity is therefore compromised. The new patient identification paradigm must make it possible to completely restore an identity to its original validity, whether that involves a single

patient or millions of patients. Perhaps more than any other identity requirement, this need for resilience has been underscored by the Equifax data breach.

5) Interoperable

Patient identification is required in virtually every clinical healthcare encounter. Any patient identification paradigm must operate correctly and seamlessly across the entire spectrum of healthcare information processing environments. While accurate identification does not guarantee interoperability of clinical data, it does represent the bedrock precondition that enables such interoperability to occur.

6) Cost-effective

The number of patient identification episodes occurring each month in the US healthcare system is enormous (millions). Because of this huge activity volume, it is essential that the cost of each patient identification episode be kept to a minimum. Not only does this mean that the financial impact must be minimal, but also the time and effort involved by both patients and healthcare workers must be minimized.

7) Easy to use

A patient identification system must be deployed across a wide variety of healthcare IT environments. The registration staff will have a variable amount of training on the system. Patients being processed will have limited knowledge about the system and some of them (for example a person who is comatose or critically ill) may not be able to actively participate in the registration process. These and other factors strongly argue for a patient identification approach that is both as simple and foolproof as possible.

Additional patient identification requirements

The list of requirements provided by the IDESG forms an excellent starting point, but it is far from complete. The additional requirements listed below are essential if a nationwide identification solution is going to withstand the test of time as a nation-wide capability.

8) Accurate

An effective national patient identification solution must – at least in theory – be able to achieve 100% accuracy in patient identification for every person across all of their medical encounters. We all know that humans create errors, both unintentionally and otherwise, but any new approach, if used properly, should avoid errors. This need to eliminate patient identification errors is a compelling reason healthcare must adopt a new patient identification paradigm.

9) Universal

Any new patient identification approach must be applicable to <u>any</u> person (including the unborn) who requires medical care. There can be no condition which prevents an individual

from being processed by the identification system. Thus; language, citizenship, ability to pay, mental status, insurance, legislation – none of these should represent a barrier that prevents patient identification for the delivery of appropriate clinical care. It must also be possible to deploy the patient identification system across all healthcare information technology (IT) platforms.

10) Simple

A patient identification system must be as simple as possible. Simplicity helps ensure accurate operation of the system. It also carries a host of other benefits including reduced user training needs, improved usability, lower system costs, easier incorporation into existing IT systems, wider acceptance by provider organizations, and increased patient acceptance and usage.

11) Identity-proofing and authentication

Recently the ONC has issued proposed guidelines for identity-proofing and authentication associated with a patient identification system[3]. Patients must be identity proofed before they are enrolled in an identification system. At all subsequent encounters they must be authenticated to confirm their identity. Both of these activities must occur in compliance with the NIST requirements for IAL2, AAL2, and FAL2 levels of assurance. These requirements ensure that the identity of each individual contained in the system can be trusted at a level sufficient to enable the exchange of medical information.

12) Patient controlled

To ensure that the system meets the specific needs of each individual, the patient must be able to exercise control over the identification activities it provides. We believe this implies that the patient must be equipped with some artifact (ID card, cell phone app, etc.) that they can use to participate in the identification system. This artifact is issued at the time the patient is identity-proofed as part of system enrollment. It enables patients to assert their identity at each subsequent medical encounter, makes this assertion as convenient as possible, and eliminates the possibility of an erroneous identity assertion. We believe the artifact also can play a critical role in enabling patients to manage the privacy of their clinical information.

13) Counterfeit resistance

The creation of a national patient identification capability will involve the deployment of millions of patient-controlled identity artifacts. In a project of this scale it will be essential to have the ability to detect and reject attempts to create forged identity artifacts. This ability to avoid fraud and abuse will, over time, become one of the major factors ensuring the long-term viability of the identification system.

[3] https://www.healthit.gov/sites/default/files/draft-trusted-exchange-framework.pdf

14) Data location enabled

Healthcare maintains information on any given patient in a wide variety of healthcare organizations and IT automation systems. An identification system must enable patients and their caregivers to access all of this distributed information in order to facilitate the creation of a lifetime longitudinal medical record. Accurate patient identification, combined with the knowledge of where information on that individual resides, is the key to making this possible. It follows that accurate data location capability will become an essential aspect of the new patient identification paradigm.

15) Dedicated solely to healthcare

The breadth, depth, and unique characteristics of healthcare argue that patient identification must be dedicated exclusively to that domain. Other disciplines such as finance and national security may wish to use analogous functions, but will inevitably have fundamental requirements that conflict with those of the healthcare industry. For example, national security identification will need to be restricted to US citizens, while healthcare must be available to every person who needs it, regardless of citizenship.

16) Anonymity

There are many healthcare situations that need anonymity. Research, public health reporting, and patient privacy are three examples. Regardless of the need for anonymity, it is still essential to be able to maintain accurate patient identification. Furthermore, this anonymity must be under the control of the associated patient. Any identification system must provide accurate identification of patients even in situations where that person chooses to remain anonymous.

17) Permanence

Once an individual has been identity-proofed and enrolled in the patient identification system, the identity they have established should be valid for that individual's lifetime. There are only two exceptions to this permanence: (1) the individual chooses to terminate their participation in the system, or, (2) some sort of "error" such as identity theft or a data breach requires that the individual's identity be reconstituted. In the absence of those exceptions a patient should be able to use their healthcare identifier for a lifetime.

18) Language and alphabet independent

Patient identification must be available to every individual regardless of their ethnicity and choice of language. Furthermore, that identification needs to endure even if that person enters an environment with linguistic requirements that differ from their initial choice. It follows that the core healthcare identification artifact that is issued to each individual should be as independent as possible from any linguistic and alphabetic constraints. We believe that only a purely numeric identifier can be used to achieve this goal.

19) System longevity

Implementing a new patient identification paradigm represents a massive effort that will take years to achieve success. This amount of time, effort, and resources can only be justified if the resulting system can provide service indefinitely. Nothing in the design, implementation, management, support, technology, infrastructure or any other aspect of the identification system should place an inappropriate limitation on the time duration that the system can serve its healthcare users.

20) Scalability

The initial primary focus of the healthcare patient identification system will be the United States. However, if successful, it will certainly be of value to significantly larger populations. Therefore, the system must be designed with sufficient scalability to enable it to eventually serve the population of the entire world.

21) Real-time operation

Many patient identification system processes are complex and involve sites that may be geographically widely distributed. Despite these challenges, the system will often be called upon to serve situations that are extremely time critical. As a result, it must be designed to support execution of its functions at electronic speed whenever possible. It must include appropriate shortcuts for potentially lengthy manual processes, such as identity-proofing, to ensure that time-critical medical care is not delayed.

22) System management

Choosing the organization that should manage the patient identification system is a challenge worthy of careful consideration. The need to avoid political entanglements and the potential to extend functions far beyond the boundaries of the United States argue strongly that the system should not be tied directly to the federal government. We also believe that a for-profit motive will not provide the necessary long-term incentive for the system to remain dedicated to its healthcare mandate. For-profit companies can provide services that will substantially enhance the viability of the system but they cannot serve as the primary steward of the system. This may suggest an organization like ICANN (Internet Corporation for Assigned Names and Numbers) should manage the top-level architecture of the identification system just as ICANN does for the internet domain names space.

23) Future-proof design

None of us can foresee what challenges the future may bring. The design of a “new paradigm” patient identification system must, therefore, be able to readily adapt to new approaches and technologies while still maintaining the integrity and value of the identification capabilities that have gone before. This “future-proof” design must be well-planned and carefully implemented to serve a healthcare industry that will continue to change in ways that we cannot currently foresee.

24) Coexistence

A patient identification system must permanently coexist with the current PII-matching methodologies. This is important for several reasons:

- Deployment of a new system will take time, but healthcare activities will continue unabated during this rollout period.
- Even when patients are enrolled in the new system, addition of retroactive historical information to patient records will almost certainly require PII-matching against information stored in legacy IT systems.
- If implemented as a voluntary system, there will always be some patients who choose not to participate in the new system. These patients will continue to require PII-matching support.

Extended discussion: Resilience

Of all the requirements listed above, it appears that perhaps the most difficult one to achieve is resilience. Using the current PII-based identification approach, it is simply not possible to restore the integrity of an identity that has been compromised. The 145 million individuals whose information was lost in the Equifax breach have no way to restore the privacy of their names, addresses, SSNs, credit histories and the like. In 2017 alone, they were joined by roughly 5 ½ million people whose PII was compromised as part of over 445 healthcare data breaches.

One inexpensive way to rectify this situation is to implement the new "identity first" paradigm described in this article. Each person, after identity proofing, is issued an abstract, globally-unique identifier. From that point on, they use that identifier to assert their identity at the start of each medical encounter. The identity system's data location function maintains an accurate and comprehensive record of all locations where that identifier has been used.

If a patient's identifier becomes compromised, the system is notified to deactivate that identifier and the patient destroys their identity artifact. The system generates a new replacement identifier which is supplied to the patient in the form of a new artifact. The data location information is then used to notify each site containing data linked to the old identifier that the old identifier is no longer valid and needs to be replaced with the new one. Once this process is completed, the patient's identity has been restored to wholeness and resiliency has been accomplished.

Conclusion

Current healthcare patient identification mechanisms do a reasonable job for many of today's situations requiring patient identification. However, they fall far short of achieving the requirements listed here. The current system is not resilient. It cannot provide the level of accuracy that is needed. It does not effectively support patient-specific privacy. There is no uniform and effective mechanism to provide anonymity. Data location capability is spotty.

Accuracy and efficiency decline as the system attempts to deal with larger and larger patient populations.

It is not trivial to move to a new patient identification paradigm. Along with the time, effort, and resources required, difficult implementation decisions will need to be made. Undoubtedly there will be some mistakes along the way. However, the benefits that will result are substantial. Registrations will be accurate and faster. Patients will be able to easily manage their own privacy as they see fit. Healthcare organizations will realize substantial financial benefits. The incidence of medical errors and other complications due to misidentification will be lessened. Most importantly of all, there will be an opportunity to dramatically reduce the estimated 300 patients per day that are inadvertently killed because of medical errors that arise as a result of misidentification.

It is time to begin this transition.

Barry Hieb, M.D.
Chief Scientist, Global Patient Identifiers, Inc.