Solving the Patient ID Now Puzzle

Executive summary

Patient matching – the process of accurately linking each individual patient to their medical information – has been an ongoing challenge for healthcare. Despite decades of effort, the process is subject to error, time-consuming, and resource intensive. The recently published patient matching framework by the Patient ID Now coalition[1] states that "Eliminating matching errors is the primary goal of a national strategy around patient identification and matching." The framework document represents the consensus of 27 U.S. healthcare organizations concerning more than 50 properties that are necessary to achieve a successful United States healthcare matching capability. Note that the primary goal is not just to make patient identification and matching incrementally more accurate; it is to eliminate errors in patient identification.

Global Patient Identifiers, Inc. has developed a patient identification solution that meets this critical goal. We strongly support the efforts of the Patient ID Now coalition to repeal the federal unique identifier prohibition but go much further by supporting a specific solution that meets all the requirements in the Patient ID Now framework including privacy, security, and the ability to fully recover from "errors" such as identity theft and data breaches.

Introduction

Global Patient Identifiers Inc. (GPII) is an active member of the Patient ID Now coalition and has spent 10 years developing an innovative solution to the patient identification problem. Our company is not-for-profit and works exclusively in healthcare. Our solution is based on the ASTM/ANSI E 1714 standard first published in 1995.

The Patient ID Now coalition, which includes a variety of organizations with different approaches to patient matching, officially advocates a "solution agnostic" approach to the repeal of the federal prohibition contained in section 510 of the labor – HHS appropriations bill. We fully support that approach, but, with this paper, start to look to the future.

This paper does not address all the GPII solution capabilities here. Instead, we will focus exclusively on how GPII services can eliminate all errors in patient identification. This is the core requirement listed in the framework and it is the key GPII capability that opens the door to achieving all the other benefits that accrue from the use of the GPII solution.

[1] https://catalog.ahima.org/view/251156390/

Accurate patient identification

The GPII solution can generate an exceptionally large number (trillions) of unique identifiers, we call ***<prTags>*** . Each identifier has a consistent format, but each number generated is unique. Healthcare organizations use open-source software supplied by GPII to provide a standard API for GPII services. This software handles all (encrypted) communication between the GPII cloud services and that particular medical site.

When a patient with no identifier arrives at a health care organization, the medical staff must identity proof the patient to at least a NIST level II of assurance. The staff member then requests a new ***<prTag>*** identifier using the GPII solution's secure encrypted communication channel. Note that this request contains no information about the patient. It is simply a request for a new identifier. The GPII solution responds by creating a new unique identifier, placing it in its database and sending it and an associated time stamp to the healthcare organization where they are stored in whatever application the healthcare organization is using (typically an enterprise master person index). The patient is provided with an identifier "token". This token may take the form of an identity card, a smartphone application, a smartcard or some other healthcare organization chosen technology. The patient can then use this token for identification at all subsequent visits to this or any other healthcare organization.

This approach to patient enrollment has several important advantages.

1. First, the enrollment process is *completely anonymous* from the perspective of the GPII cloud service. No patient identification information is sent to the GPII cloud service and the patient's ***<prTag>*** is created without any such input. All such patient specific identification information is retained where it already resides – inside the healthcare organization.
2. Second, the ***<prTag>*** is completely abstract with respect to the individual it identifies. For this reason, the assignment of *every* ***<prTag>*** to an individual is permanent. Nothing that changes about the individual can invalidate the ***<prTag>*** that has been assigned to that individual. There are only two situations that alter this permanence. One is if the patient dies and the other is if the identifier is purposefully invalidated (more about that later).
3. A third significant observation is that the GPII service database *can never represent a data breach risk*. It never contains any information relating to any individual.

Once an individual has received their ***<prTag>*** token they have in effect been given a new, permanent identification capability which, because it is unique, can never be confused with any other individual. Demographic data – name, birthdate, etc. – are no longer needed for identification. Instead, these data elements now represent potential data items for a healthcare organization to use to authenticate identity represented by the ***<prTag>***. When the individual returns for a subsequent visit the healthcare organization reads the ***<prTag>*** token automatically at registration. This asserts the patient's identity. That identity is then authenticated by providing some other type(s) of information known to the healthcare organization - name, address, biometric, . . . - whatever the organization has chosen as its preferred set of authenticators. Registration is fast, automated (no typing) and error-free.

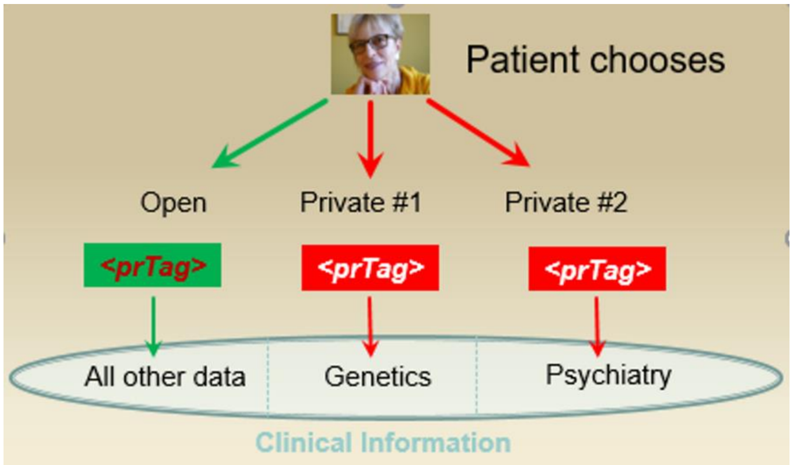
When an individual attends a different healthcare organization they still present their ***<prTag>*** to register. Since the individual has not previously been seen at this site, the attempt to look up the ***<prTag>*** locally fails. This triggers a request to the GPII cloud service – "Is this a valid ***<prTag>*** and if so where is there associated information for this individual?" The GPII service examines its database and verifies that the ***<prTag>*** is valid. It then looks up the healthcare organization where that identifier was issued and returns it to the requestor. Because this organization differs from the one where the patient initially enrolled, the GPII service updates its database to indicate that this is an additional location with information relating to this identifier. In this manner, as the patient over time encounters a series of healthcare organizations, the GPII service builds an accurate and comprehensive list of all the locations where that individual has associated information.

Meanwhile, the staff at this different healthcare organization now have the location where information for this individual can be obtained using clinical interoperability and an error-free way to indicate the involved patient. In other words, GPII services enable accurate, reliable interoperability. Because each ***<prTag>*** is globally unique, there is never any risk that one person's information might be co-mingled with another.

Privacy / Security

Most patients want their complete medical record to be available to all their physicians to ensure they receive the best, safest care possible. However, increasingly, there are reasons why patients may wish to keep some parts of their record private. Currently, these wishes are expressed in consent documents which are then managed in different ways either manually or by diverse healthcare information systems. A far superior approach to privacy, which can be implemented uniformly across the healthcare system, is available - oddly enough - using a properly constructed patient identifier.

The GPII solution introduces the concept of "open" and "private" identifiers. A patient typically receives one open and as many private identifiers as needed. This approach enables a patient's record to be segmented to honor her specific privacy needs.



The patient uses her open ***<prTag>*** to manage all her clinical information that she does not consider to be private. In this case she has acquired a private identifier for her genetics information and a second private identifier for her psychiatric records. She controls access to these sets of information by deciding whether to present the associated private ***<prTag>*** to her physician. If she does, then that physician has access to that information and if she does not, then that information remains concealed.

Since each healthcare IT system treats a ***<prTag>*** as a unique patient, its role in supporting privacy is straight forward; the IT system simply reveals all the information that it has associated with that specific ***<prTag>***. It is the patient who determines what information should be revealed by deciding on whether to present the ***<prTag>*** associated with that data set.

Of course, one objection to this privacy strategy, often raised by physicians, is that they may be presented an incomplete medical record, which could represent a risk to the patient and the physician. The GPII solution resolves this with a “break the glass” procedure. This important topic is addressed in detail elsewhere[2].

Data security must be ensured using obvious methods like encrypting data both in transit and at rest, however, there are other aspects of data security that must also be considered. A nationwide database of Personally Identifiable Information (PII) would represent an irresistible honeypot for hackers, so the GPII solution is architected to prevent the creation of any centralized PII database. There is no risk that the GPII solution could ever be the source of a data breach.

This leads to another important aspect of security which is the ability to recover fully from errors, identity theft and data breaches.

[2] Reference the Balancing Privacy and Safety white paper.

Eliminating errors

Because humans are so intimately involved in the U.S. healthcare system, it is disingenuous to argue that errors will never occur. They will. We use the term "healing" to describe the GPII process of recovering from an identity error. Once an error has been healed it is as if it had not occurred. The GPII solution can enable complete healing and thus fully restoring accurate patient identification.

Identity theft repair

Identity theft[3] is a classic example of an identity error situation. A patient or one of their medical caregivers suspects that an unauthorized person has obtained a copy of the patient's ***<prTag>***. To prevent misuse, the compromised identifier must be replaced. Working with an authorized healthcare organization staff member, the patient submits a request to replace their ***<prTag>***. The GPII service verifies that the current ***<prTag>*** is active and valid, changes its status to "terminated" and issues a new valid ***<prTag>***. It returns this new ***<prTag>*** to the healthcare organization where a new token is generated and handed to the patient. Concurrently, the GPII service consults its data location capability referencing the now invalidated ***<prTag>***. It then sends a replacement message to each of the locations where the invalidated ***<prTag>*** exists notifying the site that it needs to replace the old ***<prTag>*** with the new one. When this process has completed, the patient's compromised identity has been fully restored and they can use their new ***<prTag>*** exactly as they would have used the old one before the identity theft occurred. This "healing" capability is a critical mechanism for enabling completely accurate identification for each participating individual in an ongoing manner.

Data breach repair

Repair of a data breach is analogous to repair of identity theft. However, in this case the repair is initiated by the healthcare organization and may involve hundreds, thousands, or more compromised identifiers. In this case it is the organization which provides a list of the ***<prTags>*** that have been compromised. Each must be replaced. The healthcare organization requests replacements, generates tokens for all new identifiers and supplies them to the patients. At the same time, GPII notifies all relevant locations of the identifier replacement activity so that each individual patient continues to have a correct identity across all the healthcare organizations where they have clinical information stored.

Conclusion

The GPII solution bars no individual who needs medical care from receiving patient identification services. Potential barriers such as language spoken, ability to pay, disabilities, insurance status and nationality do not exist. This ensures that accurate patient identification and record linkage can be offered to <u>every</u> individual who needs medical care.

[3] Note that a person's identity cannot actually be stolen but the term "identity theft" is applied when a person's identification information is obtained/used illegitimately.

We recognize that asserting that any patient identification solution can eliminate matching errors is fraught with peril. Errors will occur in any automated system. The GPII solution is designed to continuously heal. The solution is both simple and resilient. Simplicity makes it much less likely that inadvertent errors will occur. Resiliency ensures that when an error is detected it can be readily and completely corrected. Simplicity and resiliency allow us to assert that the GPII identification solution will finally eliminate person identification errors in the U.S. healthcare system.

We welcome your assistance in testing this hypothesis and helping the healthcare system achieve a new era of error-free patient identification.