Achieving Identity Resiliency
A white paper for the healthcare identity ecosystem steering group

Executive summary

The recent massive Equifax breach has exposed a fundamental flaw in the methodology used to identify individuals including all healthcare providers and consumers. Once an individual's identity has been compromised there is no mechanism in place to restore that person's identity to wholeness. This document discusses why that strategic deficiency is no longer acceptable. It describes what is necessary to rectify this omission and provides an example of how this can be accomplished.

Introduction

For at least the past 15 years the healthcare industry in the United States has been debating how to solve the patient identification problem. It is universally acknowledged that being 100% certain about the identity of a patient and the information linked to that identity is a prerequisite to providing appropriate care for that individual and avoid potentially very serious error and harm. It is also universally acknowledged that, despite years of effort, healthcare has been unable to achieve that critical goal. Patient identification, especially across disparate healthcare sites, continues to encounter error rates from 10% to as much as 40% or more. These errors lead to an incredible burden in the healthcare system. As many as 300 avoidable deaths each day, unnecessary complications, delayed recovery, excessive costs, unnecessary malpractice litigation, patient and physician dissatisfaction, . . . the list goes on and on.

On September 7 of this year a new twist was added to this sad story when Equifax publicly announced that its database had been hacked and that the Personally Identifiable Information (PII) of 143 million Americans (representing roughly 40% of the adult population) had been stolen. The size of this incident is breathtaking but equally breathtaking is its scope. As one of the three primary US credit bureaus, the data stored by Equifax covers an incredible spectrum of information from personal data to financial transactions to history of residence all the way down to personal 'secrets' like the name of your first girlfriend.

There are two crucially important observations about this Equifax data breach.

1. It is inexcusable that apparently none of this information was encrypted. That means that this episode represents a virtually irretrievable breach of identifying information for roughly 40% of the US population.
2. Despite years of struggling with the United States identification challenge **there is no effective mechanism in place to enable a compromised identity to be restored to wholeness.** In other words, it is not clear whether the affected individuals will ever be able to resume 'normal' activities with respect to identification.

Resiliency proposal

This is not acceptable. One of the IDESG's four founding principles is that identity solutions must be "secure and resilient." We propose that healthcare must begin immediately to take steps towards establishing an error-resilient method for patient identification. It is the purpose of this white paper to propose strategies and options that might be used to mitigate and eventually eliminate the inability of healthcare to restore compromised identities to wholeness.

Definition: identity resiliency

Within healthcare, 'identity resiliency' means that the overall system which manages identification functions can restore the integrity of an individual's identity even though that person's information has experienced events that 'break the rules'. Identity theft, data breaches, ransomware, insider malfeasance, and hacking all represent examples of such incidents. Note that there already are a wide variety of procedures, technologies, regulations, etc. aimed at making sure that identity-compromising incidents do not occur. Those efforts are laudable and must continue. However, despite that work, violations of identity integrity continue to be experienced. It is the goal of this document to discuss how to upgrade the healthcare identification system so that it can readily recover, even when one of these unfortunate events occurs.

The current healthcare identification paradigm

The bedrock of healthcare's current identification strategy is demographic matching. Multiple pieces of Personable Identifiable Information (PII) concerning an individual are assembled into a query that is submitted to an Enterprise Master Person Index (EMPI). Searching through the records in its database the EMPI finds the record with the data elements that provide the best match to the query parameters by using its internal matching algorithm. Inside a single healthcare organization, experience indicates that this process is accurate approximately 95% of the time. When the matching occurs across independent organizations the accuracy drops substantially. Neither of these accuracy rates is sufficient for healthcare where an accuracy of 100% is required to achieve patient safety and efficient operation.

In addition to the fact that demographic matching cannot achieve the required accuracy, there is a deficiency from an identity resilience perspective which is equally troubling. It is usually not possible for a patient to change their demographic information. Items such as name, birthdate, current address, etc. are reasonably static. Therefore, if the patient's identity is based on this set of data, it cannot be replaced should an episode such as identity theft occur. And yet that is exactly what is required if healthcare is going to achieve identity resilience. It must be possible to give the patient a new identifier that corresponds to the true person if the old identifier(s) have been compromised.

Identity resiliency

We use the term **identity resiliency** to describe this critical improvement in the country's approach to identification. The essence of identity resiliency is that **if an individual experiences**

some event that compromises the integrity of their identity, there is a mechanism available that allows them to restore their identity to wholeness. This is the core property of an identity resilient system. In this document, we focus on how to accomplish this within the healthcare domain but believe that these remedies are applicable to the entire US identification domain.

A truly resilient identification system will also exhibit many other properties and capabilities. Some of them are listed here.

- Simplicity – it must be simple and straightforward to restore the integrity of an identity.
- Patient empowerment – each individual patient (or their surrogate) must be able to restore their identity integrity at any point in time.
- Complete – the identity integrity restoration process must result in the patient's identity being restored to the same integrity and functionality it had prior to the compromising incident.
- Rapid – correction of identity integrity errors should occur at "electronic" speeds to enable real-time remediation once an error has been detected.
- Network-based – due to the dispersed nature of modern healthcare, a patient's identity will typically be distributed across a wide array of geographically distinct locations. Any mechanism to restore identity integrity must operate across all those disparate locations.
- Secure – all the components and processes involved in identity integrity restoration must be protected from electronic malfeasance. To the extent possible the system must resist attempts at counterfeiting, ransomware, hacking, and well-intentioned but erroneous patient and provider actions.
- Synergistic – the system responsible for maintaining identity integrity must be able to work synergistically with existing and planned identity capabilities such as EMPIs, biometrics, interoperability capabilities and other emerging technologies.

It is also important to note features and capabilities that are <u>not</u> part of a resilient identity system.

- Retroactive repair – even a resilient system cannot retroactively correct the effect of a compromising incident. It is not possible to go back in time and "undo" the damage caused by the incident. Those repairs will depend on manual efforts outside the scope of the identification system.
- Compromising incident detection – the identification system cannot itself determine that an identity-compromising event has occurred. This will remain the domain of fraud and error detection capabilities external to the identification system including informed patients, alert providers and staff, and highly trained identity professionals.

A new paradigm

In the words of the Chinese proverb "If we don't change direction, we might end up where we are headed." Healthcare needs to migrate to a new identification paradigm that does not use demographic information as the primary attributes. At the same time, in light of the enormous size and substantial complexity of the existing healthcare computing environment, we must take extreme care to ensure that any changes needed to implement the new system are as minimal as possible while still ensuring effective resilience. We believe that this set of constraints leads to the conclusion that any attempt to achieve identity resiliency must focus on additive approaches rather than trying to repair existing techniques.

It is easier to add something new than ‘fix’ something already in place. A simple example shows why. Up until the present time the Social Security number (SSN) has been the closest thing to a unique healthcare identifier. As a data element, it is incorporated into literally tens of thousands of healthcare applications using dozens and dozens of different software languages. If healthcare attempted to achieve resilience by making a modification to the SSN – for example by adding some additional check digits – that change would need to be propagated across the entire installed base of applications that currently process SSNs. This would represent a gigantic software development project accompanied by phenomenal expense. Instead, we propose an additive approach to achieving resiliency. This strategy is much simpler, offers operational consistency across different environments, can be implemented relatively rapidly, and is orders of magnitude less expensive.

Identity proposal

The simplest, and perhaps only, way to achieve effective identity resilience in today’s environment is to assign each participating patient an identifier and then use that identifier as the mechanism to link to all that person’s clinical information. In addition, it must be possible for the patient or their surrogate to request that the identifier be deactivated and replaced with a new, independent identifier in case an identity compromising event occurs.

Identity paradigm properties

Any proposed healthcare identifier must be supported by an infrastructure that makes the system operational and effective. Here’s a look at some of the properties that are required for such a system to succeed. These properties are shown in alphabetical order rather than any attempt to assign relative importance.

1. **Abstract**
   The new approach must be abstract with respect to PII. The identification mechanism must not incorporate any information – name, birthdate, sex, address… – that represents patient data.
2. **Accurate**
   The identification paradigm must enable 100% accurate patient identification across all healthcare encounters for every individual.
3. **Anonymizable**
   In light of the numerous situations where healthcare demands privacy (e.g. treating a VIP), the resilient identification paradigm must provide full support for data sets that are anonymous as well as those that are fully identifiable.
4. **Application- (and vendor-) independent**

It must be feasible to incorporate the new identification paradigm into all known healthcare applications.

5. **Atomic**
   It should not be necessary to assemble a set of identification data elements to achieve accurate identification. Doing so would add complexity and ensure that the system could not achieve 100% identity accuracy due to errors in set membership.
6. **Automatable**
   The mechanisms to assign, query, terminate, replace and merge identities must be accessible to fully automated as well as manually initiated processes.
7. **Compact**
   The strategies and technologies used for resilient identification must be compact to permit ready incorporation into both manual and automated healthcare artifacts.
8. **Compatible with existing IT systems**
   It must be as simple as possible to incorporate resilient identification into virtually every existing healthcare information technology application.
9. **Consistent**
   The characteristics of the identification strategy (syntax, semantics, format) must be consistent across all healthcare environments to ensure reliable performance.
10. **Counterfeit resistant**
    The identification mechanism must include features that make it difficult or impossible for a hacker to create counterfeit identities that the system sees as valid.
11. **Durable**
    An identifier assigned to a patient should be valid for the lifetime of that individual unless they experience an identity compromising event.
12. **Fungible**
    It must be straightforward to replace an individual's identifier if that is needed to restore the integrity of their identity.
13. **Future-proof**
    The identification mechanism must incorporate the ability to adapt to currently unforeseen future requirements to avoid obsolescence.
14. **Globally unique**
    To provide 100% accuracy, the identification mechanism must be able to ensure that no two individuals participating in the system will ever be confused.
15. **Inexpensive**
    Considering the wide distribution of healthcare identification, the chosen implementation strategy must be as cost-effective as possible.
16. **Interoperable**
    A resilient patient identification strategy represents the core capability needed to make implementation of a truly interoperable healthcare system feasible.
17. **Longevity**
    The identification system must be designed to function indefinitely. There must not be built-in limits or restrictions that might cause the system to cease being valid.
18. **Multilingual**

The implementation strategy for a resilient healthcare identification system should support a wide variety of languages.

19. **Privacy enhancing**
    Implementation of a resilient patient identification mechanism should provably enhance, rather than diminish, the privacy of its associated medical information.
20. **Scalable**
    There should be no effective limits on the number of patients that can be supported by a resilient patient identification system.
21. **Secure**
    Users must have assurance that the system is well protected and does not represent a threat of identifier compromise.
22. **Simple**
    To maximize the accuracy and efficiency of the patient identification system, it must be designed to function as simply as is feasible.
23. **Standardized**
    A resilient patient identification strategy that is standardized maximizes the ability for a wide variety of vendors and care delivery organizations to benefit from its capabilities.
24. **Tokenizeable/Authenticator friendly**
    Whatever mechanism is chosen to implement a resilient identification system, it must be feasible to provide individual patients with tokens/authenticators that enable them to use the system, including tokens implemented on smart phones.
25. **Trust**
    It must be feasible for the majority of the population to trust the integrity and proper operation of the identity system. This will ensure that it is used and effective.
26. **Unambiguous**
    There should be no opportunity to misinterpret a resilient identifier, for example by confusing the letter 'o' with the number zero.
27. **Universal (no exclusions)**
    No individual should ever be excluded from participation in the identification system due to any personal characteristic.
28. **Verifiable**
    It must be feasible to verify the authenticity of an identifier electronically.

Identity system workflow

Patient participation in the resilient identification system would begin when the patient enrolls. The IDESG recommends (requires?) that enrollment include identity proofing to a minimum of IAL and AAL level 2. Once this has been achieved at a client organization the client can incorporate this patient into its local identification system and issue the client an appropriate identity token.

Once enrolled, a patient uses their identity token/authenticator to register for each medical encounter. They present the token which is read automatically. The system confirms the patient's identity using some form of authentication – a biometric, a comparison of PII or some other form of Knowledge Based Authentication (KBA). This entire process should require less than one minute and involves no typing on behalf of the registration staff.

If an event occurs which compromises a patient's identity the patient can request a replacement of their existing identifier. Patient's token is read automatically and the patient authenticates themselves in the standard manner. The clerk then requests to have the identifier replaced. The identifier system generates a new identifier and delivers it to the registration clerk who creates a replacement token and hands it to the patient. At the same time, the identification system notifies all locations where the old identifier has been used that it is no longer valid and that all information should be transferred to the new identifier. Once this process has been completed the patient's identity integrity has been restored and they can use their new identity token in exactly the same way as their previous one.

Patient empowerment

Any attempt to achieve identification resiliency must be based on patient empowerment. The patient must be able to control the various functions and activities that are used to maintain the integrity of their identity. This control forms the essential foundation needed to build patient trust, and trust will be essential if a resilient patient identification system is going to be effective. Physicians, healthcare administrators, and other ancillary personnel will play important roles in accomplishing this but the core driving force to maintain accurate patient identification must come from the individual patient.

Summary

In today's healthcare patient identification environment, the occurrence of a data breach such as the recent Equifax incident represents a potentially crippling event. The number of individuals involved – 143 million - is staggering. The breadth of information compromised is equally intimidating. The coup de grace is that there is no systematic capability to restore the integrity of the identities that have been compromised. We must move to a healthcare identification system that offers true identity resiliency. It is not at all pleasant to contemplate the task of trying to restore 143 million identities. But in a resilient environment that would at least be feasible, and would hold out the prospect of effectively restoring wholeness to the affected individuals' identities once the process was completed. None of that is feasible in today's environment and as a result the healthcare identification system has been dealt a major blow from which it may not recover for decades. The time to take action is now to ensure that such a mistake is never repeated.

For more information on achieving identity resiliency see www.gpii.info.