Bettering Healthcare Through Digital Patient Identification
Table of Contents

Tracing The Patient Identity Illness Back To Its Onset 03

A Treatment Plan That Addresses The Onset And Cures The Ailments Of Patient Identity 06

Piloting Patient Identities in Clinical Trials 10

Curing Patient Identity 12
Tracing The Patient Identity Illness Back To Its Onset

It is a marvel of the modern, interconnected age that all of our medical data is now on one network. However, establishing the means to uniquely and securely identify each person across a lifetime of providers to leverage this medical data continues to elude us.
This lack of ubiquitous and secure patient identity is much like an illness that afflicts every corner of the healthcare industry and worsens as we transcend into an increasingly digital way of life. The cure is a mechanism for confidently identifying a patient in a digital world.

This patient identity illness has been incubating over the past three decades. Its symptoms have been more prevalent in recent years, afflicting our data in numerous ways from ransomware attacks that hold information hostage to the loss of intellectual property, personal information, and payment data due to cyber-breaches. No matter the case, this illness originates in the digital world but impacts our real-world personal and professional lives.

The onset was with those who treat us, cure us, and nourish us, including the companies that manufacture and dispense our medications, medical devices, and vaccines. It began with multinational companies in the health industry whose supply chains extend around the world. Still, when examined closely, it becomes clear that their ailments are not so different from yours and mine.
These companies needed to digitally sign and exchange documents that establish terms of agreement between supply chain vendors and manufacturing companies, much like the HIPAA agreement you sign at the doctor’s office before engaging in treatment.

It was essential for them to exchange sensitive information with their supply chain vendors and ensure that only authorized individuals could read the information, much the same way you expect your medical information to remain private between your physician and yourself.

They needed to allow their supply chain vendors access to their information while denying access to unauthorized individuals, similar to the way you log in to an online patient portal to review medical visits and communicate with your physician.

These companies relied on automated devices and processes for maintaining the health and integrity of their supply chains, similar to the way doctors and patients rely on insulin pumps, pacemakers, and other devices vital to their health.

**Ultimately, there are so many similarities between patients and the companies who treat us, cure us, and nourish us because we are all suffering from the same personal identity illness.** Whether it is a doctor’s visit or an international agreement, it requires a robust and secure mechanism for establishing identity in the virtual world. Nor can we ignore the importance of securing the identity of, and access to, medical devices, as this is equally as important as securing human identity.
A Treatment Plan That Addresses The Onset And Cures The Ailments Of Patient Identity

Given the onset was with the supply chain to the health industry, the cure should start there. We can, in effect, attack this illness at its source and eradicate it from the bottom up.
The end goal of a digital identity is to provide confidence that the person or device with which we are electronically interacting is the person or device it claims to be. Unfortunately, digital identity providers may establish varying criteria for issuing identities and define identities in many ways at different levels of security. This lack of standardization makes trusting digital identities confusing and, therefore, difficult to rely on across all the applications and geographic regions in which they are used.

**Unifying and standardizing how identities are defined is the first step in treating the patient identity illness.**

What better way to standardize how identities are defined in the supply chain of the health industry than to invite the companies relying on these identities to decide the rules for themselves?

Drawing on a 15-year pedigree of defining and operationalizing digital identities for the health community, SAFE-BioPharma is rebranding as SAFE Identity and broadening its horizons beyond biopharma to include healthcare providers, labs, hospitals, device manufacturers, and other health industry organizations. To complete this rebranding, we are inviting members of the health industry to join us in establishing a standard set of policies for defining digital identities for their supply chains.

This SAFE Identity community will define the rules for determining the identity of an individual or device requesting participation in a transaction, regardless of location, before proceeding.
Once the community defines the rules, SAFE Identity will incorporate them in our policies so that the identity provider community can follow the community’s chosen standards for identifying humans and machines in the health industry. These providers will be connected to, monitored by, and audited in a global identity infrastructure that comprises the SAFE Identity community. This consensus-driven infrastructure allows a relying party the confidence that any credential issued from within the SAFE Identity community follows the established rules, freeing the relying party from the burden of individually administering its own trust infrastructure.
We will jumpstart the enablement of digital identities for diverse groups of individuals, by using the knowledge we gain from addressing identity for the health industry’s supply chain. With the ability to connect many issuers to a single Trust Framework already supported by a large portion of the health industry, scaling trust services to a larger, more public audience occurs naturally as the demand increases. Increased demand for digital identities brings increased innovation in ID proofing, onboarding and credential management, and the many ways the public can use their credentials, including signing digital documents, logging into websites without passwords, and even secure email. Thus, the Trust Framework becomes a key component of an overall identity ecosystem.

As we grow this ecosystem for digital identities in the supply chain, the focus will be on those who rely on digital identities. These relying parties are the final arbiters of trust as it pertains to local system access, providing the ultimate treatment for ensuring eradication of the patient identity illness from end to end. Digital identity has long suffered from a lack of technology, policy, and legal interoperability. SAFE Identity represents not only a point of aggregation to achieve technical interoperability, but also a construct to help relying parties understand the total and true implications inherent in relying on SAFE Identity-certified credentials. Just as critically, relying parties must understand the implications of relying on credentials that are not SAFE Identity-certified.

To that end, certifying identities for cross-organizational trust is only half of the SAFE Identity plan. The other half is standardizing how identities are used within applications by relying parties. After all, the best treatments in the world are of limited value if they cannot be delivered effectively. Applications must be able to use and handle these digital identities so they can be employed everywhere. Many relying party applications have come a long way in adopting industry identity standards. Still, we continue to face the challenge of ensuring we assist in effectively carrying out the implementation of these standards.

SAFE Identity meets this challenge through testing adherence of commercial applications to these industry identity standards for the benefit of relying parties. We demonstrate our commitment to these industry standards with a world-class product certification program. Under the SAFE Identity umbrella, we operate an in-house lab staffed with the leading experts in identity and cryptography to test software and hardware for conformance with prevalent digital identity specifications.

We publish products certified in our lab on the SAFE Identity Qualified Products List (QPL). This listing is publicly available to benefit the health community at large and to mitigate the challenges of standardizing digital identity consumption.

Most importantly, the initiatives SAFE Identity is embarking on during this phase in the treatment plan form the bedrock on which we will build the ultimate cure. Each of these initiatives is flexible and incorporates those using and relying on identities into its design. We are taking a community approach to combat this illness because there is strength in wide-scale standardization, which we cannot achieve alone.
Piloting Patient Identities in Clinical Trials

Preparing the cure for the patient identity illness requires perseverance, cooperation, and innovation. We can think of no better place to invite the health industry to stand together and perfect the treatment for this illness than through the clinical trial process. Clinical trials are not only the intersection of patients and the supply chain to the health industry but also of persistent, collaborative, and cutting-edge developments in human well-being.
Clinical trials provide the ideal incubator in which common requirements concerning patient identities can be drafted and nurtured. We will roll the understanding we gain from our work with clinical trials into our efforts to enable digital identities in the health industry supply chain to extend the treatment to the broader health community.

Over time, these requirements will expand to include identities for physicians who travel between hospitals, as well as healthcare staff, medical devices, and new, innovative technologies that depend on digital identities. New products and devices, including wearables, will be evaluated with the goal to improve patient and clinical trial experiences.

The advent of wearable devices carries its own set of challenges for the health industry. Many of these devices can be accessed remotely for diagnostic and calibration reasons and require their own identities to prevent counterfeiting, ensure interoperability, and verify the device-patient association. They must be included in the patient identity cure.

The clinical trial community is well-versed in applying perseverance, cooperation, and innovation to arrive at cutting-edge solutions. The knowledge gained from our experiences with the supply chain and securing medical devices will provide the catalyst within the clinical trial community for achieving the breakthrough necessary to cure the patient identity illness.
Curing Patient Identity

The recovery from the patient identity illness will take time and commitment. Still, the result is a world where doctors can take advantage of in-depth familiarity with a patient’s past and present medical history when providing treatment. As a result, doctors can deliver the best possible treatment to each individual.
We can expect a world where the individual patient’s digital identity provides a link to all that is and has been medically relevant. Just imagine a complete picture of your biology that medical providers can securely and privately access at your discretion. In this world to come, individuals will log in to patient portals, view medical records, sign authorizations, and send doctors secure messages, all without requiring a single password.

Perhaps most importantly, this patient identity and the information it protects will be private and secure, enabling individual identity verification without requiring the release of information that should remain confidential, a core principle of the Hippocratic Oath. Without this protection, an individual’s medical information can be weaponized for blackmail or used by underwriters, employers, and others in decision-making, which can result in overall poor outcomes. Medical data needs to remain private but accessible to those who treat us.

Ultimately, we aspire to live in a world where security and interoperability can complement the convenience of the digital age, rather than thwart it. We often define trust as past performance acting as a predictor of future behavior. It is no wonder that the notion of our medical providers not having access to our medical history evokes such disbelief. We should be outraged that this has not already been cured. We should be resolute in our determination to fix it once and for all, for ourselves and for the generations to come.

Indeed, SAFE Identity is setting its sights on making this world a reality for healthcare.