ceocfointerviews.com

Issue: April 2, 2018

CEOCFO Magazine

Q&A with Joseph Infante, CFO of MedicFP, LLC, Evolving From a Pure Healthcare Fraud Prevention Play To an Integrated, Secure Identification Authentication Platform for the Delivery of Better, Coordinated Healthcare

Joseph Infante
Chief Financial Officer

MedicFP, LLC
www.medicfp.com

Interview conducted by:
Lynn Fosse, Senior Editor
CEOCFO Magazine

"To a large extent, we are leaving the password era and entering a more robust phase of identity protection through the use of biometrics."
- Joseph Infante

CEOCFO: ***Mr. Infante, would you tell us the idea behind MedicFP?***
Mr. Infante: The two co-founders found the company after realizing that there was no other company attempting to prevent healthcare fraud in the United States despite the enormity of the problem. For the most part, only healthcare fraud and payment errors occurring at the back-end were being targeted, with no regard to the identity specific errors and potential fraud occurring at the front-end, i.e. at the point of the patient checking-in was being disregarded and unaddressed. The total cost of healthcare fraud and improper payments in the United States is approximately $360+ billion annually. That's one billion dollars per day. Sixty percent of that fraud is actually occurring at the point of check-in, in the form of phantom billings - the billing of services by providers for services not rendered – and identity theft and sharing. These phantom bills are then processed and the physician is erroneously paid for services. Eighty percent of fraud today in the US is actually perpetuated by the physician community. The other 20% is associated with patients, primarily in the form of identity theft and sharing. On the front-end, the two types of fraud that our technology was designed to address are phantom billing as I mentioned, which is about 40% of all fraud, and the other 20% is the identity theft and identity sharing piece. Identity sharing is quite prevalent in those communities where a family member, relative or neighbor shares his insurance and identity documents with a non-insured person in order for this person to receive healthcare benefits. The other motivation is just pure theft, whereby a physician or someone else is trying to use healthcare services, while using the stolen ID of someone else. By way of example, there are over 100 million healthcare records of US persons sitting right now on the dark web, from theft due to hacking into medical databases, which allows fraudsters to sell the medical information associated with one in three Americans.

CEOCFO: ***Is much of the fraud by physicians deliberate?***
Mr. Infante: Some of it is deliberate and nefarious in the sense that there is the intent to de-fraud. There are other physicians that are just trying to get as much payment as they can because, just like many Americans, they are trying to maximize their take-home pay as much possible in reaction to increasing regulatory and administrative pressures. Some of

these physicians can devise very creative coding practices, and, at minimum, attempt to milk as much as they can from the system because they understand how the system works. This is particularly prevalent in the practice of what we call up-coding and unbundling, which is essentially the padding of the bill. This is the problem to which most resources have gone from a fraud and improper payment detection standpoint. The colloquial term for this is the pay-and-chase model, where potential outliers (suspicious activities) are identified through the use of data analytics and then relies on our highly ineffective or unsuccessful criminal justice system to ultimately prosecute and recover ill-begotten monies. The pay-and-chase model has proven to be so ineffective that gross recovery rates are less than 2%, without considering the resources and funding required to recover such monies.

CEOCFO: ***What have you developed?***
Mr. Infante: MedicFP has developed a streamlined and secure process to authenticate the identity and presence of patients and providers, if necessary, with the use of a 3D, live facial biometrics. We validate both the identity of the patient, clinician and/or caregiver and their presence through the use of liveness detection. As part of the initial registration of the patient, there is a comprehensive check of the veracity of a government-issued identity document (such as a driver's license) and a cross-check of the insurance card, prior to the creation of the biometric signature. The initial authentication and enrollment are completed, in under a minute. Thereafter, the patient check-in at subsequent patient visits takes only a few seconds. For each patient check-in, we are not only scanning to verify that it is the right person, but we are ensuring that person is actually present, and, by doing so, we can effectively eradicate 100% of phantom billing. We are then able to integrate with the claims process. Whereby we can now tie the presence and physical location of the person with the service date and times, and, as such, prevent a physician from issuing a phantom bill.

CEOCFO: ***Are patients accepting of this?***
Mr. Infante: The short answer is yes, and here's why. Patients are increasingly using facial recognition biometrics to identify themselves. Just look at what's happening in airports with Clear and Global Entry. In a broader sense, the rollout of the iPhoneX was a major step towards establishing wide-market adoption for facial recognition biometrics as the mechanism to gain access to your phone, which in many cases also acts as an electronic wallet. So, we are seeing a growing embrace of biometrics, generally, and facial recognition, specifically, with the lead of large hardware companies like Apple and others.

CEOCFO: ***If someone loses weight, grows a beard or wears colored contacts, is that alter effectiveness?***
Mr. Infante: When you take a live 3-D facial image of someone, you are basically mapping out a person's entire face, including the contours of the face. So even when you modify your appearance with facial hair or even eye glasses or what have you, the calculations are so in-depth and complex that these potential changes do not have an impact as the proportions of these facial points relative to each other will remain the same, irrespective of these types of changes in appearance over time.

CEOCFO: ***How does the doctor side work?***
Mr. Infante: Physicians are increasingly concerned about patient safety and security. In the US, there are about 440 thousand people who die annually as a result of medical errors rooted in patient misidentification.

To illustrate what this means, allow me to share a quick example. Let's say fake Jane Doe shows up to a hospital and checks-in with Real Jane Doe's stolen information. Fake Jane has a condition that can be treated with penicillin and Fake Jane happens not to be allergic. She's treated accordingly and recovers. Real Jane Doe shows up three months later with a similar condition, but Real Jane is allergic to penicillin. However, Real Jane's electronic records show that she is not allergic, so she's treated with penicillin. Real Jane Doe consequently dies. There are 440 thousand deaths on average each year due to the misidentification of patients for identity based errors and fraudulent activities. Some offices have added modules to their EMR systems that allow for the patient photo to be taken. I know this from personal experience because not too long ago I was at UCLA with my kids and they were actually photographed. When I asked the nurse why their photos were being taken, she explained the concept of "Waiting Room Swapping". This is when someone checks in and once the patient is called, another person goes into the examining room instead. It is a problem that occurs every day throughout this country. Notwithstanding, not all of this activity is intentionally fraudulent, but certainly is another source of potential patient misidentification as discussed earlier. However, photographing a patient without first validating their identity mostly serves to perpetuate misidentification and fraud.

CEOCFO: ***What about when a doctor is falsely billing?***
Mr. Infante: This is an interesting question given some of the new opportunities being explored with some of the major claims processors. Claims processors are evaluated in part by their payment error rates according to the Centers for Medicare and Medicaid (CMS). Some of them have expressed interest in using our technology as a means of more appropriately monitoring physicians with outlying billing and payment profiles, while at the same time, providing these same physicians with certain benefits and advantages for using solutions such as ours to improve compliance with proper coding and billing standards. These benefits and advantages may come in the form of the de-prioritization of a potential audit, quicker claim processing and payment, etc. The spirit of this approach is to provide physicians with better tools to increase patient throughput, improve patient outcomes, increase safety, improve safety, and reduce physician burnout.

CEOCFO: ***What is it about your technology that allows all of these checks and balances to be in place?***
Mr. Infante: I will start with our base product - Verify™- and then I will talk about some of the additional products we have added over the past several months that are making our entire product offering more robust and more valuable. In terms of the technology itself, we have flipped the paradigm. Most companies that use biometrics, including biometric companies themselves, apply what we call the model of "trust, and then verify". For example, they create a biometric signature without verifying the identity documents used by the subject to claim who they are. In our case, we validate and cross-validate the insurance card and the state ID, which in most cases is a driver's license, with the demographic information of the person associated with his or her health insurance card. We also validate the authenticity of the driver's license. All this is done in a matter of seconds. Apart from authenticating the IDs, we also perform a facial scan using 3D/live detection and compare this image with the image that is found in the patient's ID. By doing so, we are now ensuring that the ID is actually valid and the patient is present. As you

may appreciate, does anyone really verify who you are at a doctor's office? An office receptionist takes a photocopy of your ID and health insurance card and places these copies into a folder, where it is stored and forgotten. In essence, we are updating that protocol to the 21st century and making sure the person is in fact who they say they are, and in the process, we create a safer patient environment, streamline the process, increase patient throughput through, protect the integrity of healthcare records, and prevent identity-based fraud which represents alone in excess of $215+ billion.

Now let me turn to some of the additional capabilities and products that we have added to the mix, which extends our value propositions for all stakeholders. We have teamed up with HealthEC, the number one population health data aggregator in the United States based on adoption according to KLAS, to create a joint product called VerifyCare. VerifyCare provides a guaranteed patient-specific, validated and secure "gaps-in-care" reports real-time, i.e. at the time the patient checks-in. This is the "holy grail" as we are now able to provide the physician with an instant profile of the patient that just checked in through our system. This is amazingly powerful for the provider as he or she now has a detailed roadmap of what treatments/services this patient may require or more effectively managed (e.g. opioid addiction crisis). In addition, we have acquired a virtual coding technology, which allows us to address the remaining 40% of fraud that was previously not being addressed by our original technology through our new product, VerifyCode. As such, we have built a comprehensive solution that serves patients, providers, and payers, alike.

CEOCFO: ***How are you reaching out to potential customers?***
Mr. Infante: Fortunately, our senior management team and Board members have relationships with many of the key players in the healthcare industry. Most of our targeted customers are large organizations that cut across different parts of the healthcare system. Some are in the home healthcare setting. Others are large organizations that have patients across multiple settings: home healthcare, traditional office setting, virtual medicine as well as the delivery of medical equipment. We also are engaged in discussions with commercial and government payers as well as a number of Self Insured Groups and Labor Unions. We are also very interested in entering the Electronic Visit Verification market, which relates to the implementation of the 21st Century Cures Act that requires States to electronically verify the presence of providers and patients in the home healthcare setting as part of the Medicaid program. Clearly, there are several players, large and small, across several healthcare settings and geographies who have an interest.

CEOCFO: ***Why pay attention to MedicFP today?***
Mr. Infante: Accurately identifying individuals and entering into secure transactions has become a top concern across most industries. This is true in healthcare as it is in many industries and verticals such as hospitality, defense and transportation where a unique identity is critical to accessing the services and/or products being delivered. To a large extent, we are leaving the password era and entering a more robust phase of identity protection through the use of biometrics. Being able to ensure that the product or service is matching the appropriate individual is something that is becoming essential for service providers and consumers.