An Executive Summary

The State of Digital Identification and Signatures

A conversation with Mollie Shields-Uehling, President and CEO of SAFE-BioPharma.

When leading biopharma companies founded SAFE-BioPharma in 2005, it was with a vision of a not too distant future with major changes in the industry: the move to collaboration with many partners, make business processes fully electronic, and to take advantage of all of the benefits of online operations. It's safe to say that the rate and scale of the digital revolution was even greater than most observers predicted, but this foresight proved correct.

The founders of SAFE-BioPharma knew that security would be vital in dealing with the kind of information that life science firms handle, including intellectual property, and personal health information, explains Mollie Shields-Uehling, President and CEO of SAFE-BioPharma. In order to move fully digital and/or to the cloud, the highest level of trust is a must when considering who is accessing the data, and who's signing it. A fundamental step for these companies has been to agree upon a digital identity and signature standard as these transitions occurred—thus the formation of SAFE-BioPharma, a 501(c)(6) nonprofit organization, to develop standards around identity trust and digital signing. These standards are global, meeting all US government requirements for the robustness and integrity of the signature, while, importantly maintaining interoperability with every US government agency. In addition, the standards meet European requirements for digital signing and for E-identity.

The organization's membership includes about 50 companies from large pharma as well as e-prescribing applications companies, CROs, diagnostics companies, and others rounding out an array of groups across the life sciences, says Shields-Uehling. And the group is seeing its association extend further into the healthcare space with greater technological solutions around electronic health records, medical signing, e-prescribing, and so on.

In spite of the warning signals issued by SAFE-Pharma, the healthcare industry has not kept up to pace with the evolving tech environment. In many ways, since 2005 as everyone and everything has moved online, much of the internet world has treated identity trust solutions like a chaotic bazaar where anything goes, choosing solutions in an ad hoc manner. As one envisions their long list of usernames and passwords for numerous websites and accounts, it's not hard to see how frenzied this is when the stakes are raised. So there is a real lack of interoperability—It's like having telephone companies in different cities that can't talk to each other, she explains.

Keeping up with technology is always challenging, particularly when dealing with legacy applications. This only becomes more of a challenge in the context of a highly regulated environment. Just picture the difficulties validating a new IT system for a small, non-healthcare company. This can be a major overhaul even for a small organization outside of a regulated industry like healthcare.

And unfortunately, breaches are becoming are regular occurrence. We've seen numerous headlines from 22 million records hacked from the Office of Personnel Management, 80 million at Anthem and others. Each

SPONSORED BY

DocuSign®

Pharmaceutical Executive

one, notes Shields-Uehling was caused by poor trust in who was authenticating information. And criminals see healthcare records as targets. Where a financial record is worth $2 to $5 on the darknet, a health record is worth around $50. The pharma industry is also being targeted by certain nation states to steal their clinical and development information, in an effort to leapfrog the drug development process. So there's a growing realization that this "ad hocism" has not been good for the industry.

"In the context of severe breaches, we are thankfully starting to see a greater understanding in the industry and wide acknowledgement of the need for a strong identity trust," she said. We see industry developing much more robust IT departments, and the rise of CISOs, Chief Information Security Officers, with more and more visibility. Companies are making important strides, establishing special committees to examine what information is sensitive and what level of risk is associated with that information.

Much of SAFE-BioPharma's efforts have been around digital signatures for regulatory submissions. The European Medicines Agency requires an EU qualified signature which is, essentially, a digital signature, and the FDA is on a path to similar requirements. But more broadly, what a SAFE-Biopharma digital signature does is it guarantees an identity proofing event that is uniquely linked, algorithmically linked to that digital identity. Hence, you know that when the person signs, it was his or her signature, he or she intended to make that signature. After that, if the document is subsequently changed, the signature is invalidated.

This will be key because we're seeing many our member companies moving to an enterprise wide digital signing application, and there are several SAFE-Biopharma certified partners that do this. The goal is for companies to be able to make risk based decisions around access to the information and signing. For example, certain simple operations.

Looking forward, we're seeing huge growth today in what we call authentication—that is knowing that that person is who she says she is, and then granting them access to information.

Merck is working on a great program called the EngageZone. The program brings together ~70,000 external partners, all of whom have a SAFE-biopharma compliant credential that when they knock on Merck's engaged zone, virtual door, the door says, "Yes, this is Dr. Bob, and, yes, I'm going to let him in." It allows Merck to focus their resources on what applications Dr. Bob can actually get into. All of these 70,000 credentials can then be leveraged by Transcelerate, AstraZeneca, BMS, or whatever other company.

The Transcelerate shared investigator portal is another effort that is leveraging SAFE-Biopharma compliant credentials. This gives you, the industry, the capability of mining databases all over the world because you can get access with trust. And second, it makes it much easier on the user. You can have one digital identity for access to many partners across the ecosystem. It also reduces costs and is secure.

Considering another key stakeholder, the by working with the government, SAFE-BioPharma operated a bridge which is certified by the US government. "It's like a great big telephone exchange in the sky, linking the Department of Commerce, the Department of Health and Human Services, the FDA—every US Federal government agency with every other organization within the SAFE-Biopharma complex."

Speaking towards behaviors and change management, it's important to understand the challenges, added Shields-Uehling. People don't like to get identity proofed. People hate having 40 or 50 usernames and passwords, but ask them for their driver's license in order to get this digital identity, and they balk at the idea.

Changing these mindsets will be first, but in addition, SAFE-BioPharma is working with other companies to do identity proofing in the background, something called adaptive or contextual identity proofing, that takes the device, accessing the geolocation, along with certain behavioral characteristics like the swipe. We're trying to build our standards around that so that we don't have to do what is now thought of as kind of an initial hurdle. We're doing a lot of other things, working with commercial partners to make it really seamless and easy to have a single identity and use it.