How TraitWare™ Can Secure and Simplify the Healthcare Industry

January 2015

Acuity SYSTEMS

"Secure and Simplify Your Digital Life."™

Overview of HIPPA Authentication Standards

When Title II of the Health Insurance Portability and Accountability Act (HIPPA) was established in 1996, the Internet was still in its infancy. This Act was passed with best intentions in order to protect the privacy of every American as it related to their individually identifiable health information. Privacy was important then as it is now, but the means to invade, steal, and use personal information to crippling effect has continued to grow over time. Nearly twenty years later we are in the midst of a more mature digital world that reaches far beyond the Internet into nearly every facet of our daily lives. Due to this inescapable reach it has become increasingly necessary to safeguard the one thing that is most dear to us, our very identities.

Standards and safeguards have continued to evolve and the Federal Government has continued to provide guidance and regulations to persuade the healthcare industry to stay vigilant with respect to best practices in securing our Protected Health Information (PHI). Putting even more pressure on the industry, the HITECH Act became effective on Nov 30, 2009, which increased the penalties for HIPPA rules violations up to $1.5 million.

One of the largest threats to privacy as health records move into the electronic realm is the lack of means to ensure they are only accessed by those who are authorized. The recent security breach at Sony-Pictures signaled that even large multi-national corporations are susceptible to massive digital attacks when systems continue to rely on the combination of usernames and passwords. This long standing industry standard has become a security pariah and has been directly responsible for the loss of data from some of the most recent and high-profile hacks, Sony-Pictures included.

In a recent Reuters article it was reported that, "Your medical information is worth 10 times more than your credit card number on the black market."[1] This alone is a startling fact. Couple that with the mind of a profit-seeking, disruptive-motivated hacker group and you can be sure the threat is persistent and real. In fact, the hackers are probably ahead of the industry as only a few of our health records are available via patient or provider portals. These portals are protected by, you guessed it, a username and password. The hackers are ready and waiting for the healthcare world to move to electronic records.

Fortunately, TraitWare™ is dedicated to *Secure and Simplify your Digital Life*™ by eliminating the need for usernames and passwords. When it comes to the healthcare industry, we are excited to offer solutions that keep our customers in compliance with the latest HIPPA authentication requirements and recommendations while offering vastly improved security. In a recent interview

[1] http://www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924

with Jeremy Grant, Senior Executive at the National Institute of Standards and Technology (NIST) and head of the government's National Strategy for Trusted Identities in Cyberspace (NSTIC), he spoke to the goal of the complete elimination of usernames and passwords for authentication. Jeremy stated that he is, "optimistic that we're nearing a tipping point right now with new types of technologies that are emerging."[2] With the latest developments provided by TraitWare™ that goal has now been reached. With our current platform release we are excited to help all of our authentication customers completely get rid of usernames and passwords to significantly reduce or eliminate their potential exposure to security breaches and subsequent fines.

Now is the Time to Finally Get Rid of Usernames and Passwords

The HIPPA Security Rule defines Technical Safeguards in §164.304 as "the technology and the policy and procedures for its use that protect electronic health information and control access to it." These policies and procedures allow covered entities to, "use any security measures that allow it reasonably and appropriately to implement the standards and implementation specifications."[3] More specific to authentication standards it is stated in §164.312(d) that covered entities should, "implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed." The Centers for Medicare and Medicaid Services (CMS), who are tasked with enforcing the HIPPA Security Standards, report that the majority of healthcare-related authentications are performed using passwords.[3] This is unfortunate and potentially disastrous. According to the 2014 annual Data Breach Investigations Report compiled by Verizon approximately 79% of data breaches or data loss could be traced back to some form of password compromise.[4]

While the HIPPA technological guidance on authentication is currently a recommendation and not a requirement, one can easily see why it is of paramount importance to stay proactive in this area rather then wait for an almost inevitable data breach. Even more, passwords do not truly meet the recommendations of verifying that the person accessing EPHI is the correct person. TraitWare's™ patent pending technology is ready to help our customers make the switch to a world without passwords and keep several steps ahead of those wishing to compromise PHI while at the same time increasing the simplicity of logging in for the user.

---

[2] http://www.bankinfosecurity.com/interviews/slow-path-to-password-replacement-i-2467

[3] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf

[4] http://www.verizonenterprise.com/DBIR/2014/reports/rp_dbir-2014-executive-summary_en_xg.pdf

How TraitWare™ Can Meet Your Authentication Needs

We realize that EPHI can be accessed in a variety of ways from a variety of locations. Specifically related to mitigating risk for lost or stolen logon/password information for remote access to EPHI, the CMS recommends implementing two-factor authentication.[5] Two-factor authentication uses a combination of factors to help prove your identity during a login. These factors are 'something you know', like a password or PIN, 'something you have' such as a smartphone, and 'something you are' which refers to a biometric like a fingerprint. From internal private networks to consumer web portals, TraitWare™ has been built as a platform to support the numerous avenues our customers and their user base have to login to access EPHI.

Many are familiar with the one-time passcode (OTP) method of two-factor authentication. A user attempts to log in with a username and password and a short numerical passcode is sent to your phone in a text message. You enter the passcode into the prompt and you are logged in. While that is one method of two-factor authentication there are still security risks and the user experience is error prone and cumbersome.

TraitWare™ has been developed as an authentication solution that eliminates usernames and passwords and simplifies the user experience while providing the additional security needed to prevent data compromise and loss. We do this by using your smartphone for the entirety of the login and authentication process. A person with a registered TraitWare™ app on their smartphone only needs to authenticate the app using a fingerprint or visual PIN, which we call PhotoAuth™. Once authenticated the person can log into a PC website by scanning a QR code on the PC screen using the app, or the site can be automatically opened on their TraitWare™ registered mobile device. Behind the scenes TraitWare™ is handling all of the security and authentication to instantly and seamlessly log you in without a username or password.

There are many actions that take place behind the scenes that are unique to the TraitWare™ process and which are used to verify the identity of the user. All of these pieces work in tandem and are seamless and nearly invisible to the user.

User Authentication

From the user perspective, they only need to perform one action to authenticate their smartphone for use in logging without a username or password. This would be either using a fingerprint reader on the smartphone (such as those on the iPhone 5S, 6, 6 Plus or the Samsung S5) or entering a PhotoAuth™ sequence, which is a visual PIN. Once this is done, the device releases a unique key that represents a

[5] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/remoteuse.pdf

correctly used fingerprint or valid PhotoAuth™ sequence. This key is sent to the TraitWare™ server for verification and does not contain any biometric information. This represents "something you are" (fingerprint) or "something you know" (PhotoAuth™ sequence).

Device Fingerprinting

When a person first registers the TraitWare™ app after an initial identity proofing process decided by each customer, we take a digital fingerprint of the user created content on the device on which the app is installed. This content is items such as contacts, music, and the list of user installed apps. However, that digital biometric is mathematically converted to prevent any possible recovery of personal information. Based upon the device fingerprint comparison, using TraitWare's™ patent-pending specially designed algorithm, we are able to confirm it is a unique device to that user, with odds of 1 in 360 billion. On subsequent authentication attempts, TraitWare™ executes an updated device fingerprint for comparison. Even when a person substantially changes the content on their device, the TraitWare™ algorithm is able to confirm it is the same user. This represents a highly unique and completely confidential combination of "something you have" (your smartphone) and "something you are" (your unique digital biometric).

Cryptographic Safeguards

We create a unique public/private cryptographic key pair that we use to digitally sign communications to our authentication server. Once the public key is registered with our server during the initial app activation, each authentication attempt is digitally signed by the private key, proving possession of the device. This helps to prevent man-in-the-middle type attacks and allows the TraitWare™ authentication server to verify the integrity of the data it receives from the user's smartphone during an authentication attempt. In addition to data integrity, possession of the correct cryptographic keys represents 'something you have' (your smartphone).

TraitWare™ Authentication Server

After the user has authenticated their smartphone they are able to use it to login to protected sites, such as those with EPHI. On a PC login screen used to access EHPI, instead of a username or password, the user is presented with a QR code unique to your system, which confirms to the user that they are working with your server and not one that is has been spoofed. They scan the QR code with their authenticated TraitWare™ smartphone app to login. For logging in on a mobile device, users can either select a site from a list of allowed websites within the app or navigate directly to a mobile site to login. Each of these login methods set off a behind-the-scenes sequence of steps that are based on the OAuth 2.0 authorization protocol.[6,7] The

---

[6] http://www.traitware.com/wp-content/uploads/2014/07/Traitware-Integration-Document-v1.0_FINAL.pdf

[7] http://www.traitware.com/wp-content/uploads/2013/10/TraitWare-OAuth-2.0.pdf

server containing the EPHI communicates directly through an encrypted channel with the TraitWare™ Authentication Server. If the user has been successfully authenticated, the TraitWare™ server passes an authentication token to the EHPI server, which is then able to grant access to the user. This happens instantaneously and is hardly perceptible to the user, creating a seamless and secure login experience without usernames or passwords. You are assured it is the correct user and their smartphone attempting to gain access and they are certain the server they are accessing is yours.

TraitWare™ also has the ability to use location awareness to help make authentication decisions. Each time a person attempts to authenticate the TraitWare™ app on their smartphone, the TraitWare™ Sever can check to verify that the person's smartphone is in a location that has been pre-approved for access. For example, a person may be given permissions to access protected information from both a work and home location, but not anywhere else. This helps prevent unauthorized access attempts from stolen or cloned devices and discourages users from accessing sensitive information in unsecured environments.

There are a variety of options for different needs, however TraitWare™ offers solutions for both remote access login authentication as well as internal network authentication. Concerning Federal authentication guidelines, the TraitWare™ platform by design is ready to provide Level 3 Assurance for e-authentications as defined in NIST SP 800-63-2.[8] Level 3 Assurance requires identity proofing based on verification of identifying materials and information, proof of possession of a cryptographic key, and cryptographic mechanisms that protect authentication tokens. This is the highest level of authentication assurance available for mobile devices.

Summary

TraitWare™ offers cutting edge technology to *Secure and Simplify Your Digital Life*™ by eliminating usernames and passwords in order to protect EPHI. We strive to meet, and when possible, exceed the authentication recommendations and guidance provided by HIPPA, CMS, and NIST. We do this while at the same time reducing overall user friction when it comes to logging in to websites. Several filed patents cover the proprietary processes we employ to achieve these standards of security and simplicity. TraitWare™ can help our healthcare customers in terms of compliance, user experience, and overall security. We highly encourage everyone to consider the TraitWare™ solution and eliminate usernames and passwords from their workflows forever.

[8] http://www.nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf