Industry Overview

The threat landscape around medical data security continues to escalate. According to Don Jackson, director of threat intelligence at cyber-crime protection company PhishLabs, health credentials are worth 10 to 20 times the price of US credit card information. This puts both practitioner and patient credentials at very high risk. This has caused rigorous scrutiny by Health and Human Services (HHS) and ultimately led to a September 6th, 2012 mandate by the HHS Office of the National Coordinator for Health IT regarding multi-factor authentication controls for electronic health record (EHR) systems. At the same time, HHS is requiring practitioners to provide ever-increasing access for patients to their own records.

While there has been much focus on application and network hardening, over 81% of data breaches are the result of weak or stolen credentials.[1] Efforts to force or assign users long, complex passwords that must be changed at some interval results in a negative user experience. Often those credentials are written down or saved in password applications. Couple that with the finding that almost two thirds of all users re-use the same passwords[2], and IT security professionals must assume that user credentials are known to the hacking community or can be easily discovered.

Practitioners and staff need to have remote access to provide timely care and responses to patient needs. Patients want easy access to their own medical data.

What Should You Do?
EHR solution providers should have an active and progressing user authentication strategy in place.
(HIPAA Standard § 164.312(d))

While the minimum **Meaningful Use Stage 3** authentication requirements do not require adaptive multi-factor authentication, simple username and password is virtually no security and two-factor solutions are highly intrusive to the user experience. All remote access to patient information should be protected by multi-factor authentication (NIST 800-63-1 Level of Assurance 3 (LOA 3)) according to the Health IT Policy Committee Tiger Team recommendations to the National Coordinator of Health IT in a memorandum dated September 12, 2012. This was subsequent to a September 6th vote by the Tiger Team to require multi-factor authentication. The current timeline for Meaningful Use Stage 3 is optional in 2017 and required by 2018.

While the Tiger Team recommendations focused on practitioner and clinician remote access, the threat and financial consequences of unauthorized access to patient information from stolen or weak patient credentials is just as real.

That said, all but one available solution has serious drawbacks.

- The licensing fees of most solutions are simply out of line with the reality of today's budgets
- Some solutions upset users by requiring them to jump through additional hoops every time they log in resulting in a poor user experience.
- Physical tokens are expensive to deploy and manage, especially with large user groups
- Some solutions lack the integration necessary to ensure that higher-risk transactions require additional layers of security
- Other solutions lack the ability to align transaction risk with the appropriate additional layers of authentication and the capability to monitor and evaluate risk analytics.

---

[1] 2018 Verizon Data Breach Report
[2] Ibid.

aPersona's Adaptive Security Manager™

aPersona's Adaptive Security Manager™ (ASM™) is an affordable *and* scalable, adaptive multi-factor authentication solution. ASM™ provides adaptive learning using patent-pending Patterns of Behavior (PoB) technology and a customized set of factors that can be dialed-in and tuned to reach any required level of risk and compliance. These additional factors include:

- Public and private IP addresses
- Geo Location
- Progressing one-time-use soft Tokens
- User device attributes (ASM™ device IDs consider over 100 device factors including connected devices)
- Application-specific factor verifications and factor time-outs
- User-specific factor verification overrides
- Device category factor time-outs
- "Man-in-the-middle" detection, and real-time risk scoring
- Analytics Reporting

aPersona operates with multiple modes, including invisible adaptive learning, invisible monitoring risk without challenging users, and full adaptive risk challenge mode. aPersona can be deployed everywhere, monitor everything, challenge where needed, and modify risk settings over time. Thus, aPersona is able to match your data risk requirements, reduce your data breach exposures, and easily adapt to changing regulations over time all at a price point that fits reality.

The aPersona ASM™ allows identity and access security professionals to easily implement a layered security approach and exceed the authentication requirements of Meaningful Use Stage 3 while preserving a great user experience. Add to that the lowest total cost of ownership in the industry, and ASM™ delights both IT professionals, risk management, and the CFO.

Industry Use Cases

Use Case 1: Practice Portal Remote Login

Dr. Ima Smarty needs to log into her practice portal from her home office so she can check patient records and lab results before she makes her rounds prior to heading into her office.

Dr. Smarty navigates to the secure web page for her practice management (PM) / EHR solution. She logs in using her username and password. Once her username and password are confirmed, aPersona ASM™ evaluates the transaction factors and verifies that her login pattern of behavior is allowed. If so, Dr. Smarty is allowed access into her portal. The whole process has been transparent to Dr. Smarty and occurs in milliseconds.

If the pattern is not recognized by ASM™ as one associated with Dr. Smarty's normal behavior, she is sent a one-time password via email, SMS, or phone call to confirm her identity. Once confirmed, the system learns the confirmed scenario as a valid pattern of behavior for Dr. Smarty.

Use Case 2: Fraudulent Practice Portal Remote Login

Somehow Dr. Smarty's PM/EHR credentials have been purchased by a cybercriminal looking to write fraudulent prescriptions for pain medications to sell on the black market.

The fraudster is also able to purchase a list of practices and the EHR systems in use. With a small amount of research the fraudster is able to determine the URL of the remote portal. The cybercriminal then uses the purchased credentials to attempt access. However, because ASM™ does not recognize this pattern of behavior via its adaptive multi-factor evaluation, a one-time password is sent to Dr. Smarty. This alerts her to the fraudulent attempted access.

She notifies the EHR helpdesk immediately. The helpdesk fraud team are able to view the ASM™ logs and see not only the IP address of the fraudster, but multiple machine forensics from the fraudster's computer. The fraudster has been stopped, and Dr. Smarty does not have to update her credentials and learn a new password.

Use Case 3: Patient Personal Health Records Portal Login from Her Laptop or Home Computer
Dr. Smarty's patient, Suzy Q, wants to see if her lab results have posted in her patient portal. She also needs to check her balance to see what she owes after the insurance payments have posted.

Suzy Q navigates to her patient portal and enters her username and password. Because the aPersona ASM™ recognizes this as a normal PoB for Suzy Q, she is not bothered with a challenge and is sent directly to her home screen in her patient portal.

Use Case 4: Attempted Patient Personal Health Records Portal Login by Identity Thief
Suzy Q received what she thought was an email from Dr. Smarty's office. She clicked on the link in the email and went to a Phishing web site that looked exactly like her patient portal login screen. After entering her username and password a couple times with no success, she finally gives up and figures they will call her it is something serious.

The identity thief attempts to login with Suzy Q's credentials, but is stopped by the ASM™ because there are too many factors that do not match with Suzy Q's normal PoB. A one-time password is sent to Suzy Q, who realizes someone must be trying to login to her account and notifies the fraud help desk.

Use Case 5: Employee Attempting a Fraudulent Narcotics Prescription
Ann, Dr. Smarty's new receptionist, has managed to get a copy of Dr. Smarty's EHR login credentials and smartcard. She successfully logs into the EHR system from Dr. Smarty's PC to attempt writing oxycodone prescriptions for her friends. However, because the ASM™ recognizes that Dr. Smarty has never written a prescription for oxycodone for those individuals, Ann is prevented from completing the prescription orders.

At the same time, Dr. Smarty receives a notification of the attempted fraudulent activity and immediately contacts the IT Support Desk. The IT team is then able to pull the log files from the ASM™ to determine the computer from which the attempt was made and trace the fraud back to Ann.

Use Case 6: Attempted Access on Stolen Device
Dr. Smarty's tablet PC is stolen from her car while at the gym. Dr. Smarty was specifically targeted as a known local physician. She immediately reports the laptop stolen, but asks to keep her credentials active because she still has charts to read from her home computer.

Though the tablet is protected with biometric authentication, the thief is able to bypass it and login to Dr. Smarty's Windows user account. From there, the thief is able to click the desktop shortcut to Dr. Smarty's EHR application. After several attempts at username and password combinations the thief bought on the dark web, the thief hits on the correct combination. However, the login attempt is still thwarted because ASM™ does not recognize the network as part of Dr. Smarty's normal behavior. At the same time, Dr. Smarty is able to continue to login and complete her work.

Dr. Smarty is alerted to the attempted login. She notifies the IT Helpdesk. The Helpdesk pulls the forensics from ASM™ to turn over to the proper authorities allowing them to track down and prosecute the thief.

For more information on how aPersona's Adaptive Security Manager™ can help your organization exceed the authentication requirements of Meaningful Use 3 today, contact us at 1-919-584-5098 or sales@apersona.com.