Why Two-Factor Authentication in Healthcare?

“Anakam.TFA® Two-Factor Authentication Platform helps health care institutions and health information networks secure remote access to confidential health information in a cost-effective and scalable manner, without disrupting provider workflow.”

William Braithwaite, MD, Ph.D

The Challenge?

The security of patient information is an ethical and legal mandate for healthcare. 100% security is impossible, especially in the healthcare environment where the sharing of information about a patient is a critical component of the process of improving their health. As threats to the security of health information increase, appropriate administrative, technical, and physical safeguards must be put in place to secure the privacy of protected health information (PHI). As more and more health information becomes available electronically, more risks arise. For example, it is common these days, for usernames and passwords to be shared between family members and within providers’ offices. Sometimes these private credentials are shared with staff to allow for legitimate access; sometimes they are written down and picked up by the curious; sometimes they are guessed at or captured by malicious software. This increase in exposure has led to an explosion in information breaches, identity theft and numerous violations of the HIPAA privacy and security provisions.

There are three major types of authentication used to identify a person attempting to login remotely: “Something the user knows” (e.g., username and password) is the most common and weakest authentication factor; “Something the user has” (e.g., ID card, security token or a mobile or land line phone); and “Something the user is or does” (e.g., fingerprint or retinal pattern, voice recognition, DNA sequence, bio-electric signal or other biometric ID).

Requiring the entry of only a static password is no longer considered adequate to prevent fraudulent or unauthorized access to private or sensitive information. Two-factor authentication (using two different types of authentication), provides a higher level of security and assurance. It is now widely believed that two-factor authentication must be implemented in order to provide adequate security to protect remote access to sensitive or private information and, in fact, is offered by the Department of Health & Human Services/Centers for Medicare & Medicaid Services (CMS) as guidance for remotely accessing Electronic Protected Health Information (E PHI) for entities that must adhere to the HIPAA security regulations.

The vulnerability of static passwords has led to a wide range of regulatory provisions, in addition to HIPAA, mandating the use of two-factor authentication to secure remote access to sensitive or private information, such as PHI. The National Institute for Standards and Technology (NIST) recently issued a draft update to their Special Publication 800-63 Electronic Authentication Guideline providing technical guidance to all Federal agencies implementing electronic authentication. These standards, in conjunction with the Office of Management & Budget (OMB) Memorandum 07-16, apply to all Federal information and information systems and require “remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access.”

Exorbitant costs and significant scalability issues have limited the implementation of two-factor or “multi-factor” authentication almost exclusively to small internal user bases and portals hosting highly sensitive information, such nuclear weapons and government secrets. Logistical and scalability challenges include the difficulty

Authored by:
William R. “Bill” Braithwaite, MD, Ph.D, FACMI
Chief Medical Officer, Anakam Inc.
and cost of distributing and managing thousands of authentication tokens or specialized hardware. Wide-scale adoption has been hampered by issues oriented to the end-user experience, such as requiring end-users to download software on each computer they login from and requiring them to carry a different token or other specialized device for every single account or application they wish to access.

The Solution

After considering these many challenges, Anakam®, a software development firm whose team members have spent decades developing advanced technology for the Federal government, developed the first, cost-effective two-factor authentication platform that is scalable for user bases in the tens of thousands to millions. The platform secures access to sensitive data in a way that is highly intuitive for end-users, easy to administer, and does not require any specialized hardware, cards, fobs, tokens or client-side software downloads.

Anakam.TFA® Two-Factor Authentication Platform delivers ‘true’ two-factor authentication through the use of existing devices your patients, partners and employees already have and use every day, such as cell phones, pagers, land line phones, and web connected computers. For example, after you enter your username and password, the platform can text a random, one-time passcode to your cell phone, which you then enter as the second factor to complete the login process. This one-time passcode can be sent to your pager, your email, or be heard by you on any phone you designate. If you can’t use your cell phone and you are not at your office or home, you can call in from anywhere and use your voice print (a biometric you provide when you register) as the second factor to identify yourself.

Anakam’s platform also has the ability to securely recognize a user on return visits when they login from the same machine at the same location within a configurable time period, reducing the need to provide the second factor on subsequent visits. This minimizes the impact on busy healthcare providers of adding the second factor challenge. If the machine is moved to another location or the time period expires, then the user is once again challenged.

For only a fraction of the cost of competing token based systems, the Anakam Identity Suite® is the most comprehensive and scalable identity management solution in the marketplace. Deployed seamlessly into any identity management architecture, the Anakam TFA® authentication platform delivers all the benefits of strong authentication without the logistical burdens associated with issuing and reissuing hardware and device dependent software. Anakam’s intuitive user-friendly interface drives higher eHealth adoption rates for patients and practitioners, while providing a high degree of confidence that their personal information is being protected.

Anakam.TFA® Two-Factor Authentication Platform has been implemented in government and healthcare institutions across the country, including the Carespark RHIO as part of a pilot implementation of the National Health Information Network (NHIN). The Anakam Identity Suite® includes Anakam.TFA® as well as other tools that provide low cost identity proofing and certification for online users.

“The information contained herein is subject to change without notice. The only warranties for Anakam® products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Anakam® shall not be liable for technical or editorial errors or omissions contained herein.”