WHITE PAPER

Touchless Multifactor Authentication for Healthcare

Intel's user experience research highlights the benefits of touchless multifactor authentication (MFA) for data security, clinician satisfaction, productivity, and patient care

Authors

Barbara M. Sheehan, PhD, RN, PNP
Senior Healthcare Researcher,
Health and Life Sciences,
Health Strategy and Solutions
Intel Corporation

Arlene Strugar, PsyD
Health Researcher,
Health and Life Sciences,
Health Strategy and Solutions
Intel Corporation

David Houlding, MSc, CISSP, CIPP
Healthcare Privacy and Security Lead
Intel Corporation

Multifactor authentication (MFA) is a key part of an effective security toolkit for healthcare organizations. But strict authentication processes and complex password-based systems can lead clinicians to error-prone workarounds that may cause frustration for users and compromise security and patient care.

New, touchless MFA solutions can save time and increase convenience for clinicians while thwarting common types of breaches, including cybercrime hacking that seeks to capture username and password credentials through key-logging. The increased convenience can further enhance security by reducing the likelihood of user workarounds.

Studying a Touchless MFA Solution

Healthcare environments present unique and varied challenges for technology adoption. To understand how clinicians would interact with a touchless MFA solution, Intel ethnographic researchers conducted a usability study of a next-generation touchless MFA solution that combines biometric (facial recognition) and device recognition capabilities for two-factor user authentication. The pilot solution used Dell laptops with 6th Generation Intel® Core™ i5 processors, Intel® RealSense™ technology, and the Windows Hello* capability in Windows* 10.

Intel conducted the study with MedStar Health's National Center for Human Factors in Healthcare. The Human Factors Center focuses on improving safety and quality in healthcare and is part of MedStar Health, a leading not-for-profit health system and the largest provider in Maryland and the Washington, D.C., area. Intel researchers observed ten MedStar clinicians (four physicians and six registered nurses) as they used the solution in a simulated healthcare environment. Researchers also held small-group discussions with the clinicians to explore users' experiences and identify ways touchless MFA could be utilized in different healthcare settings.

Touchless MFA Overview

Today, the most common type of MFA at provider organizations is “tap and go,” where a healthcare worker taps a badge on a reader to log in and out. If dual-factor authentication is used, clinicians may also log in with a password, typically just the first tap of the day. Fingerprint systems are perceived to be fast, but still tend to have problems, particularly for clinicians who are concerned about hygiene and must wash their hands frequently.

The clinicians in our study use a variety of clinical applications, each requiring separate authentication. Because current authentication processes are cumbersome and time-consuming, clinicians often do not log out of clinical applications. Even though these applications eventually time out, there is often a significant window of opportunity in which another user could inadvertently access another user’s session on a shared machine. This could potentially interfere with audit and compliance functions, resulting in “false insider snooping alarms” or worse. It can also lead to errors when clinicians sharing different machines accidently enter patient information under another clinician’s previously logged-in session and patient record.

Touchless MFA has the potential to address these issues. Touchless MFA uses factors such as facial or voice recognition (what you are) and a proximity wireless device such as a smartphone (what you have). Touchless authentication does not use any username and password (what you know) credentials, so it is not vulnerable to key-logging attacks, which are common in recent high profile, damaging cybercrime hacking attacks.

Value for Healthcare Providers

The touchless MFA solution used for the pilot performed well under standard daylight conditions, with a 94 percent success rate. The face recognition success rate decreased to 56 percent under dim lighting, and was not appropriate when clinicians were wearing goggles. The solution achieved an above-average rating (median score of 68) on the widely used System Usability Scale.

Participants saw significant value in touchless MFA:

- **Convenience**. Clinicians were positive on biometrics authentication technologies generally, perceiving them to be safer than passwords. Users liked not having to remember or change their passwords. This was particularly appreciated by physicians who work at multiple facilities and have to remember different passwords and procedures for each location. They emphasized the need for speed and reliability in any authentication solution.
- **Improved hygiene**. Clinicians were enthusiastic about the hygienic benefits being able to log in without touching anything, such as tapping a badge or keying a password. Solutions that combine multiple touchless technologies (for example, using gesture or voice interaction after authentication) can allow technology access even to clinicians who have sanitized hands and historically have not been able to access IT resources.
- **Efficiency and time savings**. The touchless MFA solution had a mean time to login of 2.8 seconds in the simulation study. Data obtained from Intel’s time-motion study on site at MedStar showed that clinicians spent an average of 8 seconds to log into an app using their current user id/password process, so the touchless solution offered significant potential time savings and efficiency gains. These benefits would increase for mobile clinicians or those who log in multiple times during a shift. The touchless feature also enabled users to multitask, which they viewed favorably.

Design and Deployment Considerations

The research highlighted important capabilities for solution designers and healthcare IT leaders to note.

- **System enrollment**. Clinicians frequently move from one unit or setting to another, using machines that are intended to be shared. Enrolling into a biometric system individually on every machine they may use may not be practical. It may reduce user satisfaction and contribute to workflow inefficiencies. Clinicians want an integrated, one-time enrollment that will provide secure access on any unit they may need it.
- **Seamless access to multiple applications**. A single sign-on (SSO) process with auto logout function across multiple clinical applications is needed to create the best user experience, improve workflow, and mitigate the workarounds associated with cumbersome authentication processes.
- **Feedback on system status**. Login solutions should provide an instantaneous response if possible. When that’s not feasible, the user interface should clearly communicate what is happening and anything the user can do to facilitate the process. If this feedback is lacking, it can contribute to user frustration and system fatigue, and lead users to try workarounds that may add to security risks.

Clinician Comments

"I like that I'm not touching anything, so it's sanitary as far as germs and everything. That is fabulous."

"The idea is very good. No need to memorize password."

"I like that I can have my hands free and do something else like mix drugs while I'm at this stage."

"I think I would love using this. It's like, 'Hi, bye,' and I'm in. I don't have to remember my password and keep resetting it when I forget it."

Adoption Recommendations

The research also suggested capabilities and practices that can enhance the adoption of touchless MFA.

- **Incorporate multiple touchless factors**. MFA solutions that support multiple touchless factors (such as facial recognition, proximity wireless token, voice recognition, and so forth) can offer the greatest convenience and utility across the broadest range of provider environments.
- **Provide policy-driven fallback**. No MFA factor is 100 percent reliable, and clinical users should never be locked out or prevented from accessing critical patient information. IT should establish policies specifying the preferred MFA factors and the recommended or required fallback sequences to other factors if a user's authentication based on an initial set of factors is not successful.
- **Match technologies to users and work settings**. As always in healthcare, technology teams must choose solutions with an eye to user role requirements, space constraints, variable lighting conditions, and other issues that might affect the solution's suitability and usability. Tailor MFA authentication and factors to user preferences and work settings for the best user experience and security. Deploy facial recognition in well-lit environments, and provide fallback methods for use as needed.

User Experience Research to Improve Security

Touchless multifactor authentication can help healthcare organizations mitigate security risks while improving clinician efficiency, convenience, and patient care. By exploring how clinicians interact with emerging touchless MFA solutions, Intel's ethnographic research can help solution designers and IT/security professionals deliver the full value of touchless MFA solutions for the demanding and highly variable healthcare environment.

For more information

Technologies and expertise from Intel® Security and McAfee provide a strong foundation to protect vital health data and enhance productivity for both clinicians and IT professionals. Learn about Intel® Security Solutions at **http://www.intel.com/content/www/us/en/healthcare-it/solutions/healthcare-security.html**.

Work with Intel and our collaborators to conduct a confidential breach security assessment, including MFA, and see how you compare to the healthcare industry. Visit **http://Intel.com/BreachSecurity**, or contact **BreachSecurity@Intel.com**.

Solution provided by:

No computer system can be absolutely secure. Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Learn more at intel.com, or from the OEM or retailer.