Who Are You? Authenticating Consumer Identity is Becoming Increasingly Important in Healthcare

Save to myBoK

By Tim McKay, PhD, CISSP

For consumers in the United States, the answer to the question “Who are you?” is becoming increasingly important, especially in relation to one’s healthcare. Safe and secure access to a person’s health information hinges on how their online identity is established and used—especially as more and more healthcare providers transition to electronic health record systems (EHRs) and offer patient portals. Understanding how patient identity is authenticated can help HIM professionals better secure electronically stored health information.

For US healthcare consumers, creating and using online identities is increasingly necessary to effectively manage one’s health. Mobile and web-based tools and portals can provide individualized information and services as well as offer a means to connect with others about health issues through social media. Healthcare organizations that are implementing EHR systems to achieve certification through the “meaningful use” EHR Incentive Program have obligations to provide online services that promote patient engagement—including online access to health record information and secure messaging services between patients and providers.

Establishing secure online identities for consumers is key to these efforts, but creating and implementing patient identity systems is challenging. Within healthcare, systems need to account for appropriate levels of identity assurance, and need to find the difficult balance of security and usability to support a wide range of users. This balance needs to account for individual, societal, and generational differences in determining methods and operational workflows for identity creation and ongoing user authentication.

Measuring Identity Security

Online health identities for consumers fall into two categories—anonymous and verified.

Most health management software and apps, such as fitness trackers and food diaries, can be accessed with an anonymous account. These types of accounts are set up online through self-service where an e-mail address serves as a user ID. After creating a password, the system then creates an account. As long as the same user ID and password are accurately entered for the account, the system will give perpetual online access to the app and to any information the individual creates after establishing the account. The actual identity of the person in any absolute sense does not matter.

In contrast, to establish an account to use a patient health portal, who you are is vitally important. Patient portals give access to health information that is pre-existing, and such systems must know exactly who is requesting a release health information. The system must establish that the person making the request is legitimate and authorized to view and use the health information the account contains.

To establish an online identity with a high degree of certainty, the potential account holder must be identity proofed. The National Institute of Standards and Technology (NIST), a division of the US Department of Commerce, has established a four-level identity assurance system—with each increase in level offering greater assurance.

At NIST Level 1, the entity providing identity credentials (which could be an app development company, healthcare provider, or a third party) does not need to confirm any user information. This level of assurance is appropriate for anonymous accounts.

At Level 2, an identity provider collects and verifies information that backs up an identity claim. This involves asking for information that, while not secret, is not generally known to the public at large. For example, a health system patient portal may ask for a medical record number and other demographic information that is checked in real-time against demographics databases maintained by the health system. If the information is validated, there are additional steps added to the workflow to improve identity assurance, including the use of knowledge-based authentication (KBA). KBA involves asking challenge questions which use publicly accessible, albeit obscure, information maintained by data aggregators such as credit bureaus. To pass a KBA challenge, an individual needs to answer a series of multiple choice questions accurately involving things such as prior addresses and mortgage lenders. From a NIST point of view, adding KBA to the workflow—while providing stronger assurance than document verification alone—is considered Level 2 identity assurance. However, some within the identity community consider the addition of KBA to an identity proofing workflow to offer assurance at Level 2.5.

NIST Level 3 is initially similar to Level 2 but to complete the identity proofing workflow an out-of-band passcode is sent to an address of record, usually a mailing address. The passcode may be sent to other types of addresses as well (if already known by the credentialing system) such as by sending the code via text message or e-mail. As a final step, the individual needs to retrieve the one-time code and enter it into a web or mobile form to prove they are who they claim to be.

NIST Level 4 requires an in-person inspection of identity credentials, although initial steps to verify account and address information may begin online.

So is it a good idea to always require Level 4, or at least Level 3, when an online patient service needs to know a person's identity with a high degree of assurance? Not necessarily. In reference to patient portal accounts, while Level 1 and 2 provide insufficient identity assurance, there may be little practical difference in identity assurance between accounts using Level 2.5, Level 3, and Level 4 identity proofing.

Medical Identity is Valuable and Must Be Protected

The most common attack vector for identity spoofing—pretending to be someone you're not—for online health accounts is the same for both Level 2.5 and Level 3 and is not random. That is, accounts are not created online by patients themselves, but by family members. In most cases this is done benignly when an identity system does not support the creation of caregiver accounts, such as when someone needs portal access to better care for an elderly parent. And, albeit rare, the second most common form of spoofing involves an adult setting up a portal account to spy on a partner; however, even Level 4 identity assurance is not immune to this type of coercive attack, as people can be forced to turn over their online account credentials to an abusive party after an account has been created by a very secure method.

Unless someone is a celebrity, hackers are not generally interested in the specific health information about an individual that can be accessed through a portal account. To establish a patient portal account online, a system needs a name, date of birth, and health record number. Additional identity proofing follows accurate entry of this information. However, if a hacker knows someone's name, date of birth, insurer, and health record number, they already have what they need for financial gain—using this information to create a portal account is tangential to their primary goal. In fact, setting up an account may only draw attention to the fact that a medical identity has been compromised.

Medical demographic information is valuable. On the black market, illegally obtained information that contains a name and credit card information currently sells in bulk for about 30 cents a record. In contrast, an individual's name paired with an insurer name, medical record number, and date of birth can sell for $50 or more.[1] The reason for the difference in cost is that the information shown on a health record card can provide at least one medical visit when used by an identity spoofer, and usually more than one. When credit card information is compromised, a card is typically cancelled and reissued, which blocks the ability of someone to illegally use the card beyond the point of cancellation.

However, if a medical identity is lost or stolen an individual will rarely think to contact their health insurance company to make a report. Even if they do, an insurer will not typically change a person's medical record number as it's extremely difficult to globally change this number in the myriad of administrative and care systems which use it. As a result, insurance card information can be presented, for example, in different emergency rooms to receive medical care over an extended period of time, and the fraud is only discovered well after the fact.

Converging Online and In-Person Identities through Digital Membership Cards

Most national health plans now provide a digital membership card (DMC) to their members. A basic DMC copies the information on physical membership cards, rendering the information as an image or PDF which is available on a smartphone.

Kaiser Permanente recently launched their DMC in its Southern California region, covering 3.3 million patients. It plans to complete the rollout of DMCs to all of its 9.3 million members in 2015. More than just a static image, the Kaiser Permanente DMC is interactive and integrated into its consumer mobile flagship app, available on iOS and Android platforms, and is designed to bridge physical and online identity. To access the DMC feature, a member must first sign in to use the flagship app using their online identity credentials. After signing in, members can access their own DMC and those of all their proxy subjects. Kaiser Permanente also plans to add a member picture to the DMC by the end of 2014. The picture displayed will be one that has been validated by staff during an office visit, and will be the same picture that is displayed within the member's electronic health record. This allows the DMC to be a valid form of photo ID for members checking in for medical appointments, which greatly reduces risks of misidentification and medical identity theft.

In 2015 the DMC platform will let members take "selfies" and upload their own photos for inclusion in their medical record with their smartphones. Validation of self-taken photos will use the same workflow as when a picture is taken by Kaiser Permanente staff.

Usability and Security Usually at Odds

Authentication refers to using identity credentials to prove you have a right to access account information. Online accounts can be protected by three classes of user authentication factors:

- Something you know
- Something you are
- Something you have

"Something you know" is typically a password. "Something you have" could be a cell phone, to which an out-of-band code is sent as a text message. "Something you are" involves a personal biometric measurement such as a fingerprint or voice sample that a system compares to a stored reference. Authentication of identity is strengthened when factors are combined.

One-factor authentication, which involves using passwords (something you know), is the most common form of online authentication. This holds true for most patient health portals. The use of passwords is familiar to most everyone who uses the Internet, but passwords are prone to compromise, and are easy to forget when an account is not used often.

Introducing a second factor strengthens user authentication. Although not often used with online consumer accounts, the use of two-factor authentication is increasing. For example, both Google and eBay allow their account holders to set an account profile value so that two factors are required for gaining account access. Under this schema, an account holder first must correctly enter an account password. They then receive a text message with a code that is sent to a phone number registered in the system prior to the authentication attempt. Entry of the code is needed before access to account information is permitted.

The use of a biometric as a second factor for authentication is relatively rare for online consumer accounts. This is because a biometric sample needs to be collected and stored by the entity providing authentication services, which means the user needs equipment that will read their biometrics, such as a fingerprint or a voice. This adds both time and cost to the authentication process. Yet, the use of biometrics in authentication may become more common as mobile devices can capture and transmit biometric information through published services.

Is the use of two-factor authentication practical for health portal accounts? The answer to this question relates to consumer preferences, system usability, and population characteristics.

The security of a system and its usability are generally at odds. At extremes the more secure a system is the less usable it is, and the more usable a system is, the less secure it is. While consumers want both security and convenience, they typically will tip towards convenience. In addition, security and privacy judgments are personal.

For example, while one individual may never want their HIV status to be revealed, another may post a positive HIV status on Facebook. Adding stronger security controls can be seen by some as irrelevant. Privacy decisions are also influenced by usability—if an authentication workflow involves too many steps or if it is perceived as hard, two-factor authentication will generally not be chosen when given an option.

Finding the right balance of security and usability is nuanced, and the best balance is achieved when both the nature of the protected information and the characteristics of the users of a system are considered. To be effective, account creation and authentication workflows must be validated against the intended population and ideally usability tested with these populations. For example, in older generations people may not have a cell phone, share a single cell phone with a spouse, or turn on their cell phone only when leaving their home. If a two-factor authentication system only uses text messaging as a second required factor, the method may block health portal access for the people who would normally most frequently use it.

Future of Consumer Health Identities Relies on Standards

In the near term, working to achieve industry consensus around standards for identity systems that allow access to patient portals is strongly advised. Standards need to be comprehensive and applicable to a wide range of identity services. If standards are not comprehensive, identity systems can be inadvertently made insecure—for example, by using two-factor authentication but having methods for resetting passwords that can be exploited through both automated processes and social engineering. Areas that consumer health identity standards should address include:

- Account creation and identity provisioning
    - Identity proofing
    - User ID rules
    - Password rules
- Authentication, including multi-factor authentication and biometric use
    - Proxy access
    - Account maintenance
    - Account recovery (forgotten password, locked account)
    - Account de-provisioning and reinstatement
    - Suspected fraudulent use

Standards are a necessary step in moving toward the interoperability of consumer health identity credentials. In 2011, President Obama signed into law a program called the National Strategy for Trusted Identities in Cyberspace (NSTIC), which promotes the development of secure consumer identities that can be used in multiple online services.

NSTIC revolves around four guiding principles, where identity solutions are:

- Privacy-enhancing and voluntary
- Secure and resilient
- Interoperable
- Cost-effective and easy to use

The Identity Ecosystems Steering Group (IDESG), a two-year-old organization, is attempting to promote NSTIC-centric standards development through promotion of pilot programs and cooperative work between different industry segments such as finance, government, and healthcare. IDESG meets in plenary sessions four times a year and between plenaries work is moved forward through committees, including an active healthcare committee. In addition, the Healthcare Information and Management Systems Society (HIMSS) has an active workgroup focused on patient identity.

Many have found it encouraging that conversations have begun to align work between IDESG and HIMSS, which may move standards efforts forward more quickly and begin to provide consumers the ability to use a single online identity with the patient portals of many health systems. Interoperable identities need not be limited to healthcare alone. For example, one set of identity credentials could give access to online banking accounts as well as to multiple patient health portals. However, identities that cross domains will likely need stronger protections, requiring higher levels of identity proofing and two-factor authentication, as they need to be robust in addressing a larger number of risks related to compromised identities.

Standards Needed to Secure Healthcare Information

Efforts to promote consumer identity standards in healthcare will benefit both consumers and providers. Standards promote common workflows and, when critiqued by communities of interest, make the building of systems more secure. Consumers benefit when common methods promote ease of use, and authentication methods follow recognizable, repeated patterns.

Promotion of interoperable identities also benefits both consumers and providers. Consumers benefit when one set of identity credentials can give access to multiple services and health portals. Providers benefit when costs related to the establishment and maintenance of identities are spread among a broader system with less duplication.

Note

1. Medical Identity Fraud Alliance. “The Growing Threat of Medical Identity Fraud: A Call to Action.” July 2013. http://medidfraud.org/wp-content/uploads/2013/07/MIFA-Growing-Threat-07232013.pdf.

Tim McKay (Tim.A.Mckay@kp.org) is a principal technology consultant at Kaiser Permanente’s Health IT Strategy and Policy Group.

Article citation:
. "Who Are You? Authenticating Consumer Identity is Becoming Increasingly Important in Healthcare" *Journal of AHIMA* 85, no.9 (September 2014): 32-37.