Patient Portal Identity Proofing and Authentication

Guidance from the HIMSS Identity Management Task Force
Table of Contents

Executive Summary ......................................................................................................................... 2
Summary Recommendations .............................................................................................................. 4
  Identity Proofing: .............................................................................................................................. 4
  Identity Authentication: .................................................................................................................... 4
Introduction ....................................................................................................................................... 5
  Background ..................................................................................................................................... 5
Identity Proofing: Guidance and Risk Analysis .................................................................................. 12
  NIST Summary of Identity Proofing .................................................................................................. 12
  HIMSS IDM TF Guidance on Identity Proofing ............................................................................. 13
Identity Authentication: Guidance and Risk Analysis ....................................................................... 15
  NIST Summary of Identity Authentication ..................................................................................... 15
  HIMSS IDM TF Guidance on Identity Authentication ................................................................... 16
Summary ........................................................................................................................................... 17
Special Case 1: Proxy Access to Patient Portals .............................................................................. 17
Special Case 2: Anonymous Access to Patient Portals .................................................................... 18
HIMSS Identity Management Task Force Leadership and Acknowledgments .................................. 20
Appendix 1: Proxy Access to Patient Portals .................................................................................. 22
  Definitions ....................................................................................................................................... 22
  Best Practices and Requirements for Proxy Access to Patient Portals ............................................ 23
  Summary ......................................................................................................................................... 31
  Additional Considerations ................................................................................................................ 32
Appendix 2: Anonymous Access to Patient Portals ....................................................................... 33
  Anonymity Principles ....................................................................................................................... 33
  Summary ......................................................................................................................................... 36
Patient Portal Identity Proofing and Authentication

- Guidance from the HIMSS Identity Management Task Force (HIMSS IDM TF)

All mechanisms or processes that provide electronic access by patients to their own protected health information (PHI, as defined by HIPAA) must be capable of employing user identity proofing and authentication at a high level of confidence, greater than or equal to National Institute of Standards and Technology (NIST) Level Of Assurance (LOA) 3 or equivalent (as determined by a documented HIPAA risk analysis).

Key 2015 Recommendation from the HIMSS IDM TF

Executive Summary

The U.S. Department of Health and Human Services (HHS) defines a patient portal as a secure online website that gives patients convenient 24-hour access to personal health information from anywhere with an Internet connection. The HIMSS IDM TF adds that a portal can also be an app accessed via any device. When patients access a patient portal today, they typically do so by using a UserID-Password combination for electronic authentication. The process by which they initially obtain the UserID-Password, i.e., the way they are proofed, typically involves them receiving a one-time code during an office visit (in-person identity proofing) or via paper mail. Some organizations also allow for online remote identity proofing by the asking of questions, the answers to which only the patient is expected to know (Knowledge Based Authentication or KBA). The U.S. Federal Government, via the Electronic Authentication Guideline (NIST SP 800-63-2) specifications, has provided an excellent starting point on the requirements, threats to and methods of classifying identity proofing and authentication solutions. Certain states and other proponents of health information exchange, such as DirectTrust, recommend that consumer/patients and persons acting on behalf of consumer/patients (“proxy”) be identity-proofed at Level of Assurance 3 to view such information and to communicate with the consumer/patient's provider(s) of care. The HIPAA Security Rule sets up generic requirements for providing individuals with access to their PHI through web portals with appropriate authentication controls to ensure that the person seeking access is the individual or the individual’s personal representative. The key to specifics

---

3 “Electronic authentication (e-authentication) is the process of establishing confidence in user identities electronically presented to an information system.” Defined in NIST SP 800-63-2 (see link below).
5 See: [https://app.box.com/s/s1hn82cn4gnza8i0ssxyy9tmrthd03pg/1/3809607958/31694947006/1](https://app.box.com/s/s1hn82cn4gnza8i0ssxyy9tmrthd03pg/1/3809607958/31694947006/1) and [https://app.box.com/s/s1hn82cn4gnza8i0ssxyy9tmrthd03pg/1/3809607958/46328464917/1](https://app.box.com/s/s1hn82cn4gnza8i0ssxyy9tmrthd03pg/1/3809607958/46328464917/1)
6 See discussion of the concept of identity assurance on page 6.
in the HIPAA requirements is the result of a required periodic Risk Analysis which we believe should, given the increased risks today, result in a requirement for a high level of confidence in the identity of anyone accessing PHI.

Although we believe that a high level of confidence in identity proofing and authentication is required to protect access to PHI, we find that strict compliance with the NIST requirements to operate at LOA-3 sets too high a bar for some healthcare patients. Our guidance is designed to attain a high level of confidence that is consistent with NIST LOA-3 as justified by risk analyses, without requiring such strict compliance to the specific methods required by NIST.

Due to the increased sophistication that attackers have developed, the traditional approaches to authentication are no longer adequate and more sophisticated methods are now necessary. This is especially true since the attackers have spent the last fifteen years honing their skills against online financial services which typically have sophisticated risk management systems. Bringing those hacking skills to bear against patient portals is likely to leave such portals very exposed. Better identity proofing and authentication, the subject of this paper, is only one of several areas of cybersecurity that those in charge of patient portals have to worry about. However, it is the front line of defense and an important problem to address now.7

Why have better approaches to identity authentication and proofing not seen widespread deployment as yet? We believe this is because historically the solutions tended to fall into the class of “too weak” (e.g., UserID and password) or “too hard” (e.g., biometric smartcard) or “too expensive” (e.g., cryptographic key fob). Security solutions in general, and identity authentication and proofing solutions in particular, should never be measured solely on how secure they are. Rather the solutions must be weighed against at least three equally important criteria: (i) the level of security risk, (ii) the total cost of ownership for the enterprise deploying the solution, and (iii) the ease of use for the user. This is our philosophy in constructing this guidance. We believe that certain changes in the technology landscape, especially the nearly ubiquitous use of smartphones, have allowed us now to raise the bar on security without significantly impacting the cost or ease of use criteria.

Our guidance first addresses the most widespread use case, namely patients who possess a smartphone accessing their own information. We then turn our attention to two related use cases of significance for healthcare, namely proxy access and anonymous access. Proxy access is when a user wants to access a patient portal on behalf of someone else. For instance, a parent who needs to access a minor child’s account, or that of an elderly parent for whom they are the caretaker. Anonymous access is for those patients with sensitive health conditions such as sexually transmitted diseases. Guidance for users without smartphones will follow in a future document.

This guidance should be considered “living guidelines” and our best judgment on what is a practical next step to improve identity proofing and authentication as of early 2016. We expect to update our guidance as new threats appear and as innovative new solutions come into existence.

**Summary Guidance**

We assume that a large majority of patients who use online patient portals will have an email address, a smartphone and are used to using video calling over Skype and other such applications. We believe that the incorporation of smartphones as a second factor into the processes of identity proofing and authentication will significantly improve the security of electronic interactions with patients while minimizing the additional cost and difficulty.

**Identity Proofing:**

- We require that the patient must provide a government issued Photo-ID, a health insurance card, a smartphone/cellphone number at which they can receive voice calls and an email address at which they can receive emails.
- The organization must compare the photo to the actual user and cross reference personal information. Although few health insurance cards include a photo, the organization should verify that the name on the card matches the name on the driver license presented. They should actively ensure that the user is in possession of the phone and email addresses provided.
- For remote identity proofing, a video call may be used to emulate in-person identity proofing with the same requirements. Knowledge based authentication alone, as it stands today, does not suffice and must be supplemented by other techniques.
- Simple proxy mechanisms must be incorporated into patient portals for improved security and can evolve to provide better and more automated services to users over time. Identity proofing of proxy delegates can use the approval of the patient if the process used for the patients themselves is not practical.
- Patients must be uniquely identified in some way so that the permanent records of their care are not confused with the care records of other patients but pseudonyms can be assigned to fully identity proofed individuals when needed for extra privacy protection. Anonymous users (no identity proofing) can be set up in very limited circumstances.

**Identity Authentication:**

- To access PHI online, we require two-factor authentication, specifically including a “something you have” factor. In practice this is likely to be the user’s smartphone incorporated into a secure authentication process. As smartphone biometrics and standards like FIDO (Fast IDentity Online) mature, this will effectively provide a path to incorporating biometrics in the future.
- Authentication techniques and strength for PHI access by proxy delegates or anonymous patients must not be different from those used for the fully identity proofed patients.
**Introduction**

The HIMSS Identity Management Task Force (IDM TF) serves as a multi-stakeholder industry liaison group, representing HIMSS membership with regard to national and industry initiatives on identity management, such as the National Strategy for Trusted Identities in Cyberspace Identity Ecosystem Steering Group (NSTIC IDESG) and other national policy and technical efforts and developing tools and resources that will assist HIMSS members on identity management issues related to patients, proxies, providers and IT asset identities (Internet of Things). In 2015, the IDM TF published (through HIMSS) a high-level policy recommendation entitled, “Recommended Identity Assurance for Patient Portals.”8 In that document, the task force indicated that it would issue guidance for implementation of the levels of identity assurance recommended to meet healthcare requirements. The task force created three sub-groups to discuss the issues and create such guidance.

This document provides our guidance on identity proofing, multifactor authentication, and how to incorporate appropriate NIST concepts into a HIPAA Risk Analysis to support implementation of that guidance. We also address proxy access and anonymous access as special cases. The detailed reports from our sub-groups on these special cases are provided as Appendices.

**Background**

As the healthcare industry transitions from paper records to capturing clinical information digitally using certified electronic health records (EHRs) that enable secure e-sharing of protected health information (PHI), doctors, nurses and care teams are required by law to have authenticated digital identities to perform certain, specific functions, such as electronic prescribing of controlled substances (EPCS)9, as well as more general access to PHI10.

The Affordable Care Act (ACA) has a patient-centric focus that embraces and empowers patients and families to participate in managing their care. To make this process more efficient and secure, people/patients will also need to validate who they are electronically in order to gain online access to their protected data and provide informed authorization to share their PHI or to delegate who can view their confidential health information.

Unlike some other industries where a one-to-one relationship can be established securely without much in the way of identity proofing, healthcare typically involves a long series of interactions with disparate organizations that provide different healthcare services in different locations with different health information systems over the course of a lifetime. In addition, healthcare liability is a differentiator that requires an elevated level of identity assurance.

9 DEA Regulations at: 21 CFR Part 1311
10 HIPAA Security Regulations at: 45 CFR 164.312(a)(1)
The concept of identity assurance is central to this discussion and to the guidelines in NIST SP 800-63-2 wherein it is defined as 1) the degree of confidence in the vetting process used to establish the identity of an individual to whom the credential was issued, and 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued. NIST defines the degrees of confidence at 4 Levels of Assurance (LOA) based on those first defined in OMB M-04-0411 as follows:

- Level 1: Little or no confidence in the asserted identity’s validity.
- Level 2: Some confidence in the asserted identity’s validity.
- Level 3: High confidence in the asserted identity’s validity.
- Level 4: Very high confidence in the asserted identity’s validity.

Since access to past records of care (including diagnoses, procedures, test results and prescriptions, among other facts) is critical to the provision of safe and effective healthcare, an accurate and unique digital identity must be created for each patient such that it can be securely trusted across all those organizations over time to accurately link to past records of care. When implemented in ways that engender trust in the privacy and security of their records, this digital identity will also empower patients to securely navigate the healthcare system electronically and help manage their health activities while mitigating risk and arming themselves against fraud and cyber-hackers.

From the perspective of these digital identities, a patient typically has two types of interactions with a specific and usually local healthcare system; the first encounter (identity proofing) and all subsequent encounters (identity authentication).

**First Encounter – Registration and Identity Proofing**

At the first encounter, the office or healthcare facility staff must register the patient by asking the individual for demographic information that can be used to establish their unique identity. This demographic data will also help determine whether or not the patient has been seen previously in an affiliated office and is potentially “Known to the Practice” through prior collaborating or clinical “coverage” agreements such as being “on call” for nights, weekends and vacations.

The ONC Report on Patient Identification and Matching12 recommended a specific set of standardized patient identifying attributes that should be required:

- First/Given Name
- Current Last/Family Name

---

11 OMB Memorandum M-04-04, 12/16/2003 at: https://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy04/m04-04.pdf

©2016 Healthcare Information and Management Systems Society (HIMSS) Page 6 of 36
• Previous Last/Family Name
• Middle/Second Given Name (includes middle initial)
• Suffix
• Date of Birth
• Current Address (street address, city, state, ZIP code)
• Historical Address (street address, city, state, ZIP code)
• Current Phone Number (if more than one is present in the patient record, all should be sent)
• Historical Phone Number
• Gender

Additional, non-traditional data attributes to improve patient matching that the ONC report recommends should be studied include:

• Email address
• Direct address
• Mother’s first and maiden name
• Father’s first and last name
• Place of birth
• Driver’s license number
• Passport number
• Eye color

This extensive constellation of demographic information is used to match against existing records to assure that this is a new and unique person, at which point they are assigned a new, unique numeric/other coded identifier or Medical Record Number (MRN) to facilitate searching and collating relevant documents in the Electronic Health Record. Today, the MRN is only unique to the issuing healthcare organization. The demographics also have many medical uses, but that is out of scope for this discussion.

In addition, an almost universal policy is to ask the patient how the practice will be paid for the upcoming service and ask for evidence of insurance or of a third party reimbursement system, if cash is not offered.

Notwithstanding the ONC recommendations discussed above, the first-time patient is usually asked to prove who they claim to be by providing verifiable identification credentials that could include some subset of the following documents:

- Driver’s License
- Green Card
- Food Stamp Card
- Passport
- Insurance Card
- Employer Card
- Government Issued Card
- Utility bill
- Other
Very commonly, the typical patient will be asked for their driver’s license or other government issued Photo-ID (a government issued ID card which can be verified by comparing the picture to the patient or by checking against DMV records), and an insurance card (documentation of a financial account which can be verified electronically with the insurance company, i.e., a real time “eligibility check”). Although most healthcare institutions treat all patients irrespective of their financial ability to pay for the service, to assure safe continuity of care there will still be an attempt to establish a unique identity using other documentation if a health insurance card is not provided. Although this combination satisfies the technical requirements for identity proofing at Level of Assurance 3 (LOA-3) as specified in National Institute of Standards and Technology (NIST) Special Publication 800-63-2 entitled “Electronic Authentication Guideline,” it is not the only means that healthcare institutions use to establish identities at a high level of confidence.

Some healthcare systems also allow initial registration to be done remotely through a similar process. If there is no human visual verification of the person’s face against their picture ID, both documents must be verified against the original sources to add confidence in the identity proofing. Automated methods of such image comparison have yet to be proven equal to the task easily done by a human. Another method for remotely proving identity is called “Knowledge Based Authentication” or KBA, where a user is asked several questions to which only the user is likely to know all the correct answers. However, currently there is no remote KBA performance metrics standard and few KBA performance metrics that are not proprietary. This uncertainty in KBA performance can affect and weaken remote identity proofing and create vulnerabilities (risks). Although already accepted by certain federal government agencies (e.g. the Social Security Administration, HealthIT.gov, and the Drug Enforcement Administration) for specific functions, without a clear understanding of the causes of variability, potential remedies and ultimately a standard, KBA remains a weak link in establishing identity.

Of course, there are many other variants that may be used to establish high confidence in the identity of the patient that do not meet the specific criteria of NIST for LOA-3, and it is the intent of this group to provide guidance on how to justify a conclusion that they are equivalent. After successful registration and identity proofing, the patient is deemed to be ‘Known to the Practice’.

First Encounter – Issuing Identity Tokens

To make further use of this newly established digital identity and to augment confidence in future interactions, the system has to issue one or more ‘tokens’ which are associated with the individual patient. The patient can use them remotely to securely identify themselves to the system at another time. For each subsequent online interaction, the system will either utilize the original token(s) or require the patient to register new tokens that they already possess (such as their cell phone) or create new ones.

13 The HIPAA-mandated Accredited Standards Committee (ASC) X 12 270/271 eligibility transactions are commonly used.
from a growing number of options (such as a new password, a number texted to a mobile phone, or even more simply, a code on a piece of paper). In any case, the mechanism for transporting a token from the token origination point to the patient must be secured to ensure that the confidentiality and integrity of the newly established token is maintained and that the token is in possession of the correct person.

There are many different tokens that can be used to establish factors that authenticate the patient’s identity for online transactions. Authentication factors generally fall into three types: something you know (such as a password or username), something you have (such as a card or device that can be read electronically and supplies a code – typically a onetime password - or a properly equipped cell phone), or something you are (a biometric such as voice print, fingerprint or facial recognition). Most healthcare systems now use only one factor, typically username and password (two facts you know but which amount to only one authentication factor), for authenticating remote access to their patient portal.

To provide a high level of confidence when starting a remote interaction with the system, at least two different identity authentication factors must be used. Guidance on how to improve the security of remote patient access to PHI by implementing two factor authentication (TFA) is provided below.

**Subsequent Encounters: Identity Authentication**

In all subsequent encounters, whether in-person or remote, the patient’s identity can be established securely by using the token(s) that were issued at the first encounter. Although many healthcare organizations are still requiring presentation of driver’s license and insurance card(s) to establish identity and financial responsibility at subsequent encounters, some are now automating that process by having the patient check in electronically at a kiosk using their digital identity. This trend is expected to increase as low cost mechanisms for two factor authentication spread in the industry. Of course, remote access using the assigned identity tokens is supported in the same way. We contend that in order to keep PHI secure at this point in the development of electronic mechanisms for sharing such information, digital identity authentication using two factors must be implemented for all remote access to PHI. Our guidance is intended to show how such factors could be implemented cost effectively in typical healthcare environments. There are certain instances, such as delivery by unencrypted email, which may be allowed as exceptions to this basic principle when elected by the patient for delivery of their PHI, but we believe that does not apply to patient portal access and in any case there is no excuse today for any healthcare organization not to implement two factor authentication for access to PHI as the default.

Regardless of the security of this authentication, all it proves is that this is the same person who was given the identity tokens, and says nothing about the confidence with which their identity was established at first encounter. Only those identities that meet the criteria for a high degree of confidence in identity proofing can be used across institutions. Realistically this could occur if there were national

---

15 See: [http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html](http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html)
standards or a recognized trust framework that binds the participating institutions to follow certain protocols that promote and support collaboration and allow for legal redress. Currently, however, very few healthcare institutions have a mechanism to trust identities established at other institutions. As we move toward the goals of The National Strategy for Trusted Identities in Cyberspace (NSTIC), perhaps this can change in order to provide more efficient, safer healthcare.\(^\text{16}\)

**NIST Specifications**\(^\text{17}\)

The NIST document, “Electronic Authentication Guideline,” is designed for use by the Federal Government. It specifies four levels of assurance (LOA-1 to LOA-4) with increasing levels of security and assurance. These four levels are specified across five areas:

1. **Proofing.** The User interacts with a Registration Authority (RA) to prove their identity.
2. **Tokens.** The RA lets a Credential Service Provider (CSP) know it has proofed the user. Then the CSP and user interact to establish electronic credentials that bind the user identity to one or more tokens (password, cell phone, biometric, etc.).
3. **Token and Credential Management.** The lifecycle management of tokens and credentials by the CSP.
4. **Authentication Protocol.** This is the protocol that plays out between the User and the Verifier, by which the user proves that they indeed are in possession of the tokens.
5. **Assertions.** These are statements from the Verifier to a Relying Party (RP) about whether or not the user was successfully verified. The interaction between the Verifier and the RP are in practice often handled through redirections via the web browser using protocols such as SAML or OpenID Connect.

Note that the above description accommodates situations where the RA, CSP, Verifier and RP might belong to different organizations with unique systems, but equally applies to a single organization with a monolithic service that includes all functions. Where implemented currently in healthcare, all such functions are typically conducted by the same organization. Their interactions are shown in the attached figure excerpted from the NIST document.

---

\(^{16}\) See: [http://www.nist.gov/nstic/about-nstic.html](http://www.nist.gov/nstic/about-nstic.html)

\(^{17}\) See definitions of terms and abbreviations starting on page 6 at [http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf)
NIST SP 800-63-2, while intended for the U.S. federal government, can be used by other industries. Although some believe that industries such as healthcare should adopt the NIST specifications because interoperability with the federal government is essential, we note that strict compliance with the NIST document means that to operate at a high level of confidence (LOA-3), all five areas must meet the specifications for LOA-3 or LOA-4, a very high bar for healthcare patients. The NIST document is lukewarm about the use of Knowledge Based Authentication (KBA) and specifically argues against relying too much on biometrics. It states: “Certain authentication technologies, particularly biometrics and knowledge based authentication, use information that is private rather than secret. While they are discussed to a limited degree, they are largely avoided because their security is often weak or difficult to quantify, especially in the remote situations that are the primary scope of this document.”

Caveats
Before proceeding, we would like to note the following:

- It is our understanding that NIST Special Publication 800-63-2, “Electronic Authentication Guideline”, is being revised, and we have attempted to maintain consistency with the new direction which is likely to allow for a more graduated scale as opposed to four discrete levels. Further, it is our intent to set up a dialogue with NIST, including sharing this guidance as input to their process of refinement.

- Our focus is limited to credentials for patient access to healthcare portals. Some of the guidance may indeed be applicable for providers, insurers, administrators, and others to securely access PHI, but that is out of scope for this document.

- There are five areas in the NIST document: identity proofing, tokens, token and credential management, authentication protocols and assertions. This document concentrates on the
identity proofing step, and then on multifactor authentication, which incorporates much from the areas of tokens, token and credential management, and authentication protocols. The area of assertions is out of scope of this document, although we believe that assertions will be important in the future to support a patient using their employer/banking/insurance credentials to access their patient portal.

- We assume that upon completion of identity proofing, ‘record matching’ is performed accurately and verified. How that is achieved, and all discussion of related topics, such as universal patient identifiers, are out of scope for this document.

- Historically, local healthcare policy makers have set the bar too low when it comes to security. The end result is a climate of breaches and lack of trust in protecting PHI. Conversely, security professionals tend to set the bar too high, and such requirements can be difficult to implement in healthcare because of technical, cost or usability issues. Our goal is to identify a balance that meets a standard of high confidence by providing very practical, economically tenable guidance that results in solutions which healthcare organizations can efficiently deploy and patients can easily use.

### Identity Proofing: Guidance and Risk Analysis

**NIST Summary of Identity Proofing**

NIST SP 800-63-2 deconstructs the identity proofing process into two areas, the basis and the actions, and further separates the in-person and remote cases. Our summary below is only meant to give a sense of the requirements, and the reader is referred to the actual document for the precise definitions.

For in-person identity proofing, NIST recommends:

- The basis for issuing the credentials: A driver’s license or other government issued Photo-ID.
- The required actions of the RA/CSP (which for our purposes we assume is a single organization) are:
  - Verify that the ID is a valid ID
  - Verify the personal information on the ID
  - Verify the photo by comparing it with the human being
  - Verify that they can receive calls/texts at their phone number
  - Notify them via paper mail that credential issuance happened (hence verifying physical address of record)

For remote identity proofing, NIST recommends:

- The basis: in addition to the above, verification of an account number (i.e., checking account, savings account, utility account, loan, credit card, or tax ID) is required. This requirement for an additional document likely stems from the assumption that the Photo-ID cannot be compared to an actual human in a typical remote session.
- The required actions: in addition to the applicable items from the in-person case, there is a requirement to ensure the address and other information on the additional document (say a utility account)
bill) matches that on the government ID. Further, there is also provision to bind the email address to the record if possible.

From a risk analysis perspective, NIST identifies the following threats to the identity proofing process:

- During registration, an imposter (e.g., using a forged driver’s license) could pretend to be someone else. Another risk, not commonly considered, is the risk of repudiation, namely, a user can deny applying for a credential, claiming that someone else must have pretended to be them and acquired the credential. This latter threat is avoided by collecting biometrics, physical signatures, voiceprints or equivalent.
- During the credential issuance, various attacks are possible. For instance, a smart attacker could let a legitimate user do the entire identity proofing process and then steal or divert the credential(s).

**HIMSS IDM TF Guidance on Identity Proofing**

Our guidance is intended for patient access to healthcare portals. Further, our guidance is informed by the trends in the industry in the three years since the NIST guidance was developed. Specifically we observe the following:

- Over 90% of American adults now have cellphones and 64% own a smartphone. Since this 2014 study, we believe that percentage has increased significantly. If current trends continue, by the time the guidance in this document is implemented, it is likely that smartphone deployment will be nearly ubiquitous (especially for the population that wants online access to a patient portal). Our guidance does not wish to exclude anyone and we expect to make modifications for those who do not have smartphones at a future time.
- Video calling technology is now extremely cheap and is likely to be familiar to most patients who want online access. In an age when tele-medicine for actual patient-provider interactions is being considered seriously, and where video calling based notarization of documents is already legal and being used in at least two states, Virginia and Montana, we felt it appropriate to leverage this technology for identity proofing.

In this context we provide the following guidance.

**In-Person Identity Proofing**

**Basis:**

1. The patient must provide a government issued Photo-ID, which in practice is most likely to be a state issued driver’s license.
2. The patient must provide a health insurance card.

---

19 See: [http://www.lexology.com/library/detail.aspx?g=dc727f0b-d4b7-4ea6-b3ac-c97028009a73](http://www.lexology.com/library/detail.aspx?g=dc727f0b-d4b7-4ea6-b3ac-c97028009a73)
3. The patient must provide a smartphone/cellphone number at which they can receive voice calls and/or text messages.
4. The patient must provide an email address at which they can receive email.

We note that there will be exceptions; our intent here is to initially provide guidance that will raise the level of security for the majority of users. We expect to produce additional guidance in the future for those patients who cannot meet the above requirements.

Organizational Recommendations:
1. Compare the photo to the actual user and cross-reference the personal information. We do not require, but recommend, that the organization verify that the ID is valid (something that is rarely done today).
2. Ensure that the email and phone number are in possession of the patient through a process that “closes the loop”. For example, an SMS message to the identified cell phone containing a short, random code that is returned in a reply to an email could validate both.
3. Validate the health insurance information and cross reference the personal information. For example, a successful HIPAA-standard eligibility transaction will validate the insurance information electronically.

Identity Proofing Using Video Calling
We allow for this additional category where the user is not in person, but is indeed interacting with a human being at the organization over a video call. The guidance for the basis and the organizational actions remain the same.

Remote Identity Proofing
Here the patient is interacting with a system at the organization and there is no human being at the other end. In this circumstance we allow for two methods to substitute for the human examination of the government issued Photo-ID:

1. It is acceptable to use a derived credential as long as the original credential meets the criterion above for in-person or video calling identity proofing. It is up to each organization to decide which antecedent credentials to trust. For example, a patient can use a credential issued by another organization (e.g., a notary, an employer, an insurance company) to proof a new healthcare identity. The NIST document lays out an excellent discussion on acceptable derived credentials. It does, however, require that the credential from which the derivation is made be one level higher on the LOA hierarchy, a requirement we do not include.
2. Following the NIST guidance on KBA we do not include KBA based remote identity proofing as adequate by itself. However, we believe KBA augmented with proof of a government issued ID is acceptable. For instance, some vendors now offer technology to photograph the Photo-ID and then record a selfie video, with the combination being validated off-line (or in near real time) by a human. We would like to emphasize that KBA technology is under constant improvement, and there could well be future KBA technology (for instance that asks questions about clinical data) that might well be acceptable. It would be useful in supporting its adoption if KBA service
providers could agree on a standard for evaluating the effectiveness of KBA across various populations. 21

All other requirements remain the same as for in-person identity proofing. Note that we are dropping the requirement for paper mail being sent to a home address. While we do not believe it adds much to protection against real threats, it might be necessary for legal reasons. We note that a validated email address and phone number can be thought of as the equivalent of a physical address today. For example, when providers are identity proofed for electronic prescribing of controlled substances under DEA rules, the provider’s mobile phone number can be validated if the billing address for the mobile phone is the provider’s known address.

Identity Proofing Risk Analysis
Basis: Like in the core NIST standard, forgeries of Photo-IDs will remain a threat vector for us. Our strategy to mitigate this risk is to also require validation of an email and phone number. The difficulty in forging all three is likely to raise the bar sufficiently for now.

Process: The risks to the process highlighted in the NIST document are discussed in conjunction with our guidance on authentication. In a December 2015 paper, “Measuring Strength of Identity Proofing,” NIST points out there are a variety of technical, policy and implementation considerations associated with determining the strength of identity proofing methods that should be considered to improve risk-based decision making. NIST also believes it would be useful to separately consider each function that supports identity proofing, such as: identity resolution; identity validation; identity verification, and activity history. 22

Identity Authentication: Guidance and Risk Analysis

NIST Summary of Identity Authentication
The NIST document covers identity authentication primarily in the section on tokens but other sections are also relevant. NIST identifies three factors as the cornerstone of identity authentication:

- Something you know (for example, a password)
- Something you have (for example, an ID badge or a cryptographic key)
- Something you are (for example, a fingerprint or other biometric data)

Multi-factor authentication refers to the use of more than one of the factors listed above, which NIST requires to reach a high level of confidence in authentication. At least one of the factors must contain a secret that is securely presented to the electronic process that is verifying the user’s identity. A second


©2016 Healthcare Information and Management Systems Society (HIMSS)
factor can be used to protect or activate the first, so that a biometric such as a fingerprint can be incorporated in this way, even though NIST does not consider it to be adequate by itself.

**HIMSS IDM TF Guidance on Identity Authentication**

We would like to reiterate the primary observations motivating our guidance:

1. This document is focused on the “consumer use case”, namely patients accessing healthcare portals. Most secure authentication solutions currently used for providers or administrators are too costly or too hard to use for consumers, although that is changing rapidly.
2. We note that access to patient portals is somewhat sporadic in that such sites are not accessed on a regular basis. This increases the likelihood of a “forgotten password” result.
3. The overwhelming majority of all access today is based simply on static passwords because, for all its security defects, passwords are affordable and users have (grudgingly) learned to use them. Any replacement MUST not deviate too far from the cost and ease of use of passwords.
4. We do however believe that we simply must raise the bar beyond the “something you know” technology of passwords.
5. We believe we must take advantage of the near ubiquity of smartphones.

Based on the above, our guidance is as follows:

We require that the patient portal identity authentication process include a “something you have” factor, and that the token or the process implicitly or explicitly prove knowledge of a “something you know” factor. In practice we expect that our guidance will lead to a process using a smartphone, or potentially some other addressable portable communications device, which is initialized, and periodically updated, by the user without the need for intervention by IT staff. We observe that as more and more smartphones are unlocked using biometrics, and standards like those from the Fast IDentity Online Alliance (FIDO) mature, this guidance puts us on the path to incorporating a “something you are” factor with little additional cost or effort.

Experience has shown that solutions that require portals to implement sophisticated, or for that matter even fairly standard, cryptography prove to be a barrier to implementation. Today almost all patient portals are based purely on static passwords. Therefore our strong recommendation is that implementing the server component of this solution should not require cryptography beyond standard SSL/TLS. In addition to smartphone apps that can generate one-time passcodes securely, voice print matching and other mechanisms using the cell phone microphone or camera are being tested which require no app to be downloaded and no physical input by the user. For example, certain financial institutions have successfully implemented authentication by comparing a smartphone “selfie” with a preregistered facial image.24 We believe all these mechanisms are developing quickly and will be available broadly for

---

23 See: [https://fidoalliance.org/specifications/overview/](https://fidoalliance.org/specifications/overview/)

cost-effective implementation in the near term, both directly by larger healthcare organizations and through identity service providers for smaller organizations.

**Identity Authentication Risk Analysis**

The NIST document provides a comprehensive litany of the various threats against authentication, including theft, duplication, discovery, eavesdropping, off-line cracking, phishing and social engineering. Any proposed solution must be analyzed along all these fronts in a risk analysis. Using a smartphone as a “what you have” factor does not by itself mitigate against all the threats, as a lot depends on the specifics. Some such implementations will not meet the current NIST specifications for LOA-3. However, we reiterate that incorporating a cellphone or smartphone into the authentication process significantly raises the bar from where we are today and we believe that any such multifactor implementation can be rationalized with a risk analysis to provide a high confidence authentication of identity.

Another December 2015 NIST paper, “Measuring Strength of Authentication,” states that biometric technologies as the primary authentication factor are expanding in use in the consumer market but the strength of this style of authentication is not yet fully understood. They go on to point out that a biometric identity system may be attacked in any number of ways and propose that analysis of potential vulnerabilities for biometric systems across the stages of presentation, capture, enrollment, comparison, and decision could be the basis for calculating the strength of biometric authentication.25

**Summary**

We believe that the incorporation of smartphones as a second factor into the processes of identity proofing and authentication will significantly improve the security of electronic interactions with patients while minimizing the additional cost and difficulty.

**Special Case 1: Proxy Access to Patient Portals**

Patient portal systems which permit the set-up of proxy relationships help broaden patient engagement in meaningful ways. That is, not everyone who can benefit from the information and services available through a patient portal can use a patient portal. This includes children, and people with cognitive and more severe disabilities. Portals can also help those who are capable of managing their own care to allow others to manage care on their behalf as a matter of convenience or practicality.

---

Permitting proxy relationships through patient portals also reinforces good identity management practices, such that the system is more confident of the identity of any person accessing a portal, as proxy relationships reduce the circumstances under which a caretaker takes on the portal identity of another person in order to access portal services for someone under their care.

Establishing a system of proxy access for patient portals requires both software capabilities and a set of policies which describe conditions for establishing, modifying, and terminating proxy relationships. When available, the automation of procedures for the set-up of basic proxy relationships, such as a parent acting for a child or one adult requesting help from another is recommended. Making the provisioning of proxy relationships available through self-service tools speeds the setup of proxy relationships and reduces the burden of manual setup. However, some types of proxy relationships can be difficult, if not impossible, to automate given current tools and technologies. Given differences in patient portal systems, and their lack of maturity in providing proxy access, it is reasonable to see the extension of proxy permissions as a program which can start with basic access and mature over time.

Our guidance is that all patient portals must establish a system of proxy access for improved security. Proxy mechanisms may be simple “all-or-none” types at first and then can evolve to provide better and more automated services to users as policies and techniques improve. Identity proofing of proxy delegates can use the informed authorization of the patient if the usual identity proofing process is impractical, since they are only being authorized to represent the patient in interacting with the patient portal. Authentication techniques for PHI access by proxy delegates or anonymous patients must not be different from those used for the patients themselves. The strength of authentication for proxy access must be at least as strong as for the original user.

Some of the issues of proxy access are addressed in the HHS Office for Civil Rights (OCR) guidance explaining how the HIPAA Privacy Rule deals with personal representatives. The considerations for proxy access in healthcare are extremely complex and we recommend reading Appendix 1 for the full discussion of proxy access to patient portals.

**Special Case 2: Anonymous Access to Patient Portals**

In a typical healthcare environment, all patients must be uniquely identified in some way so that the permanent records of their care are not confused with the care records of other patients. Most healthcare organizations also want a validated mechanism for being paid which often provides a secondary means

---

of identity proofing. Regardless of the level of identity proofing done for an individual patient, they have a right to ask for anonymity to add a layer of privacy protection to their records.\textsuperscript{27}

In healthcare, if a patient wishes to have anonymity so that their medical records cannot be associated with their true identity except in extraordinary circumstances, they may be assigned a pseudonym\textsuperscript{28} and a multifactor authentication mechanism to help protect the privacy and confidentiality of their records. This authentication mechanism is identical to that issued to a fully identity proofed patient, so no special provisions need to be made to maintain the anonymity. The difference resides in the limitation that such an authenticated digital identity can only be relied upon by the originating organization, whereas a fully proofed identity could be used across organizations, each of which have carried out the appropriate level of identity proofing and authentication.

In the future, it may be possible for anonymous or pseudonymous identities to be more easily deployed across clinical practices, organizations and enterprises which share participation and contractual agreements in a recognized, common trust framework.\textsuperscript{29} We also foresee emerging technical developments which engage patients in more easily determining most of the conditions surrounding disclosure of their PHI with the possible effect that the need for anonymity will be reduced.

Please see the Appendix 2 for the full discussion of anonymous access to patient portals.

\textsuperscript{27} Note that this paper only addresses anonymization for patient data and assumes that health care providers can take advantage of these same processes when they are patients but should expect no anonymity in their roles as providers. IHE has also done work in this area regarding De-Identification, Pseudonymization, and Relinking. See: http://ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Handbook_De-Identification_Rev1.1_2014-06-06.pdf

\textsuperscript{28} Pseudonym: Use of a persona or other identifier which is different from that normally used by an individual with the intention that information be not linkable to that individual. [ Adapted from ISO TS 25237 ]

\textsuperscript{29} Trust Framework: a complete set of contracts, regulations or commitments that enable participating actors to rely on certain assertions by other actors to fulfill their information security requirements (Kantara Initiative).
HIMSS Identity Management Task Force Leadership and Acknowledgments

Identity Management Task Force Chair:
William Braithwaite, MD, PhD, FACMI, FHL
Founder of Braithwaite Consulting
bill@braithwaites.com

Level of Assurance Sub-Group Lead:
Ravi Ganesan, PhD
Founder, Identity.Ninja
ravi@findravi.com

Proxy Access Sub-Group Lead:
Tim McKay, PhD, CISSP
Senior Director, IT Product Management and Delivery
Corporate Services and Digital Technologies (CS&DT)
Kaiser Permanente Information Technology (KPIT)
tim.a.mckay@kp.org

Anonymous Access Sub-Group Lead:
William Braithwaite, MD, PhD, FACMI, FHL
Founder of Braithwaite Consulting
bill@braithwaites.com

Additional Contributors:
Noam Arzt, PhD, HLN Consulting
David Batchelor, LifeMed ID
Frederick D. Cox, CISSP, CISM, CISA, CRISC, Varian Medical Systems
Anupam Goel, MD, MBA, Advocate Health Care
Barry Hieb, MD, GPII
Jim Kragh, Independent Healthcare Consultant
Sreedhar Madullapalli, Lucile Packard Childrens Hospital
Michael Magrath, VASCO Data Security
Frederik Mennes, VASCO Data Security
Michael L. Nelson, DPM, Equifax Inc.
Beth Pumo, MBA, CISA, CISM, Kaiser Permanente
Ann Racuya-Robbins, Virtual Democratic Countries
Catherine Schulten, LifeMed ID
Aaron Seib, National Association for Trusted Exchange (NATE)
Renee Smith, Walgreens
Tom Sullivan, MD, DrFirst

HIMSS Support Staff:
Mike Kroll, MBA, PMP
Manager, Technology Solutions, HIMSS North America
mkroll@himss.org

©2016 Healthcare Information and Management Systems Society (HIMSS)
The authors of the paper would also like to acknowledge the members-at-large of the HIMSS Identity Management Task Force for their contributions to group discussions and feedback throughout the paper’s development process.
Appendix 1: Proxy Access to Patient Portals

Report of the Proxy Sub-Group of the HIMSS IDM TF

Through the HIMSS Identity Management Task Force, as part of a broad initiative to address issues of patient identity in healthcare, an ad-hoc group was formed to address issues of proxy access to patient portal information and services. This paper summarizes the ad-hoc group’s findings and consensus recommendations about requirements and best practices for secure and easy-to-implement proxy access to patient portal accounts, with a focus on proxy access by non-professionals (such as parents who manage medical care for their children and adults who provide assistance to elderly parents receiving medical care).

Definitions

This paper uses the following terminology as a means to facilitate common understanding of the issues involving proxy access.

- **Subject**: person who is the subject of care or record of care. The subject may be a child, an adolescent, adult or senior adult. A subject is commonly a patient.

- **Delegate**: the person who is enabled to access a Patient Portal on behalf of a proxy subject. In most cases a Delegate is an Adult.

- **Adult**: a person 18 years of age or older (who has not been determined to be mentally incompetent).

- **Incapacitated Adult**: an Adult who is incapable of accessing or using medical services, online or otherwise, in whole or in part, without assistance. This status may be legal (e.g., a court has determined an individual is mentally incompetent) or practical (e.g., a person is in the early stages of a progressive dementia but still lives at home with a spouse or caregiver).

- **Adolescent**: a person under the age of 18 who can partially consent to receiving some medical care independent of decisions made by an adult caretaker. The lower end of the age range within the United States is dependent on state law, and ranges from 12 to 15 years of age. While also defined by state law, partial consent typically permits the adolescent to receive care for issues...
related to sexuality, sexual practice, behavioral health and substance abuse. In addition, case law allows for provider discretion concerning what care, above what is mandated by state law, can be consented to by any individual Adolescent.

- **Incapacitated Adolescent**: an Adolescent who is incapable of accessing or using medical services, in whole or in part, without assistance. This status is typically determined by a medical care provider, but may in some cases be court determined.

- **Emancipated Adolescent**: an Adolescent who by court order can make decisions, including decisions about their own medical care, independent of any parent or caretaker.

- **Child**: a person who by age alone cannot consent to receiving any medical care independent of decisions made by an adult caretaker. In most states, this means someone under the age of 13.

- **Patient Portal**: a software capability which permits patients to have access to select medical record information and associated services by a sponsoring entity. Frequently, this is a capability bundled with a provider-focused Electronic Medical Records (EMR) system.

**Best Practices and Requirements for Proxy Access to Patient Portals**

This section is organized around use cases highlighting different facets of proxy access. While the use cases are comprehensive, the list is not exhaustive. For each use case, issues raised are discussed, and derived requirements for a system of proxy access are stated.

- Requirements with a force of SHALL are those which a proxy system must have in place in order to be viable.
- Requirements with a force of SHOULD are those which a more mature proxy access would likely have in place.
- Requirements with a force of MAY are more advanced capabilities which system owners ought to consider in enhancing an established system of proxy access.

System actors referenced with terms that begin with capital letters (e.g., Adult Subject) are defined within the Definitions section of this document. For example, there are 2 general requirements that we derived from looking at all the use cases:

1. An audit record SHALL be created each time a proxy relationship is created, modified, viewed or deleted.
2. The strength of authentication for a Delegate SHALL be at least as strong for the Delegate as it is for the Subject who is accessing their own portal information.
Adults as proxy Delegates for other Adults

Use Case #1: I am an adult and want to let another adult access my health information through a Patient Portal. I want control over determining how long this access is given and want to be able to terminate access at any time.

Discussion

The ability for one Adult to extend access to another Adult to manage their care illustrates a basic pattern for proxy services. In this case an Adult Subject determines who will be a Delegate and the Delegate is another Adult. Both the Adult Subject and Delegate need to have established identities that are recognized by the identity and access management (IAM) system that governs the Patient Portal.

In general, Adults should be able to direct any other Adult to have access to their information, with no or very limited constraints. While access can be manually set within a system, some Patient Portals currently provide the ability for Adult account holders to authorize access to another Adult through self-service tools. It is assumed that the proxy Subject’s identity has been adequately vetted in the process of establishing a Patient Portal account. However, the identity of the Delegate may not need to be vetted by the Patient Portal system, as it is the Adult Subject who is directing the creation of the proxy relationship and as such it is primarily important that the Delegate be known by the Adult Subject. This concept of referential identity proofing of Delegates is less applicable when both the Adult Subject and Delegate already have portal accounts and their identities have been vetted by the system. In general, if the Delegate is not already a user of the Patient Portal, setting a higher bar for identity proofing may discourage the creation of an account, and instead encourage the Delegate to request the Adult Subject to share their existing credentials to provide access.

The duration of access by a proxy Delegate must be under the control of the Adult Subject, with the ability to modify the duration of access and the ability to terminate access completely, in a timely manner. In many cases the Subject may allow indefinite access to the Delegate’s information until such time that the Subject terminates such access. The capability to terminate access could occur through phone or email channels, so that an agent can perform this action on behalf of an Adult Subject, but a more effective means would be to provide this as a self-service action through the Patient Portal.

An Adult Subject’s authorization of a Delegate to perform actions on their behalf may be seen as a formal release of information request. As such, the action to designate a proxy Delegate must only occur with informed consent by the Adult Subject. If access is set through self-service means, a best practice is to treat this as a formal release of information following HIPAA Privacy rules, which the Adult Subject electronically signs, and must create an audit record reflecting this authorization.

Authentication techniques for PHI access by proxy delegates or anonymous patients must not be different from those used for the patients themselves. The strength of authentication for proxy access must be at least as strong as for the original user.

Derived requirements

3. An Adult Subject SHALL be able to designate another Adult as a Delegate who can access and can use information on the Adult Subject’s behalf through a Patient Portal.
4. Delegates for Adult Subjects SHALL NOT be able to delegate access to any other third party.

5. An Adult, regardless of affiliation with an organization sponsoring a Patient Portal, SHOULD be able to establish a portal account in service of serving as a proxy Delegate.

6. An Adult MAY be able to use identity credentials external to a Patient Portal system to establish an identity within a Patient Portal system IF such credentials adhere to a recognized, Trusted Framework Program certified by an entity such as the Identity Ecosystem Steering Group (IDESG).³¹

7. An Adult Subject SHALL be able to determine the length of time a Delegate can access and use services on their behalf through a Patient Portal within maximum lengths based on Federal and State/Province laws, rules and regulations pertaining to the release of medical records information.

8. An Adult Subject SHALL be able to terminate access by a Delegate at any time for any reason. Termination of access SHOULD be possible through self-service tools on the Patient Portal.

9. A clinician, or designee acting on behalf of a clinician SHALL have the ability to create, terminate, and modify proxy relationships, including changing dates of access and individual access rights for any Delegate.³²

10. An Adult Subject SHOULD be able to review the types of information to which the Delegate would have access before a Patient Portal creates a proxy relationship with a Delegate.

**Adults as proxy Delegates for Children**

**Use Case #2:** I am an adult and want to manage care of my children, including my teenager, through a Patient Portal.

**Use Case #3:** I am a teenager and don't want my parents to know very much about the things I tell my doctor, teachers, friends and others. It's ok for them to do some things for me on our Patient Portal, but not others. It's complicated.

**Discussion**

Parents and guardians who have general responsibility for the care of children have rights-of-access to the health care information of their children. The extent of access is determined by both age, and in the United States, by state law. That is, until a Child reaches an age, as determined state-by-state, at which they can consent to receiving medical care on their own in limited circumstances, a parent (or guardian) should have full access to that Child’s medical information; as a Delegate, a parent should be able to view and use all available portal features on behalf of a

---

³¹ The IDESG is a non-profit organization charged with creating a framework which allows for the creation of strong, interoperable online identity to fulfill the vision presented in the United States White House initiative, the National Strategy for Trusted Identities in Cyberspace.

³² This requirement addresses the need for administrative tooling which can enable the set-up and maintenance of proxy relationships when self-service methods are not available. It also provides a method to block or terminate a proxy relationship in cases of fraud or abuse.
Child Subject. This is the second main pattern of Patient Portal access, whereby a Delegate requests access to a Child Subject’s information. This is a pattern which can be automated. While patient demographics systems rarely have explicit information about parent/child relationships, these can be inferred when such systems show an Adult and a Child living at the same address. Some health plans have used this data, along with the Delegate electronically signing an affidavit saying they have the legal right to make medical decisions for a child, as a means of automating the creation of an Adult-for-Child proxy relationship.

However, when a child reaches the age at which they can consent to receiving some forms of medical care, things change. At the age of partial consent the Child Subject becomes an Adolescent Subject, and as such, parental access rights in relation to Patient Portal information become more restricted. In most states this is when the child reaches age 13, but the age can be as young as 12 or as old as 15 years. The conditions for which an Adolescent can consent to medical care also differ state-by-state, but generally involve issues related to sexual practice, sexual orientation, alcohol/drug use, and access to mental health services.

This lack of uniformity in state laws can make it difficult to know what Patient Portal services should be offered to a parent once a Child becomes an Adolescent. Within the industry there is no set approach to solving this problem. Some Patient Portals will cut-off parental access to child accounts completely at the age of partial consent, and may not allow Adolescents to have Patient Portal accounts out of concern that a parent could coerce access to portal information (e.g., demanding the user ID and password for an Adolescent’s account). Other organizations enact less restrictions in parental access, such as extending access to a parent to some portal features (e.g., secure messaging, allergies) and not others where the likelihood of exposing information to which the parent should not have access is more possible (e.g., problem lists, lab results, medications).

Some Patient Portals have begun to address this issue by allowing specific conditions, medications, lab results and provider notes to be suppressed from view if a clinician marks this information as “confidential”. In general, this suppression occurs for both the Adult and the Adolescent—neither can see this information through the Patient Portal. This is because it is very easy for an adult with authority over an Adolescent to demand access to the Adolescent’s portal account if there is a belief that information is being hidden from the Adult. However, this approach of suppressing information is only a partial solution to the problem of preserving Adolescent privacy rights for a number of reasons. First, some information may be “leaked” through unstructured data, or by others who provide documentation to an Adolescent’s record (e.g., a Medical Assistant) who do not know to suppress certain information from view through the Patient Portal. Second, for most conditions for which an Adolescent could potentially seek their own care, most do not; that is, most parents and guardians already know about these issues, and support the Adolescent as they receive care for them. Third, billing information often includes reason codes which allow the adult who pays for the Adolescent’s health insurance to intuit a condition (e.g., their 14-year-old daughter is seen for an OB/GYN service).  

---

33 It should be noted that an account guarantor, the person responsible for payment of health insurance premiums for a subscription unit, has limited access rights to account billing information apart from any formal designation as a Proxy Delegate. However, an account guarantor has no automatic right to accessing clinical information about anyone in their subscription unit through a Patient Portal apart from a formal designation as a Proxy Delegate.
plan has dealt with this issue by assigning billing for such visits to a different financial account and writing-off any associated charges for that visit. Yet, without aggressive communications about such a policy, a provider may not know that this is an option.

In short, while a parent’s access rights to information about their Child through a Patient Portal should be as complete as possible, the parent’s access rights to their Adolescent’s information is nuanced, based on state law, the nature of the relationship between a parent and an adolescent, and software capabilities/limitations. As such, any restrictions on parental access to Child and Adolescent information through a Patient Portal should be documented in policy, and any baseline access permitted by the portal should be modifiable by a provider through manual methods.

Derived requirements

11. An Adult SHALL be able to serve as a Delegate for a Child Subject on a Patient Portal when the Adult is the parent or legal guardian of the Child Subject and the parent has the legal right to manage the Child Subject’s medical care.

12. A Patient Portal SHOULD have the ability for a Delegate to create a proxy relationship with a Child Subject using self-service tools.

13. A Delegate SHALL be able to access all applicable Patient Portal services on behalf of a Child Subject.

14. A Child SHOULD NOT have their own account for a Patient Portal which gives a Child independent access to their own health information and related Patient Portal services.  

15. A Delegate SHALL have access to a limited set of Patient Portal services for an Adolescent Subject according to State and Federal Law and organizational policy.

16. An Adolescent SHOULD have the ability to create and use a Patient Portal account.

17. A Delegate’s access rights to a Child Subject’s information SHALL be automatically changed to access rights to an Adolescent Subject’s information when the Child reaches the age at which he/she can partially consent to medical care according to state law where care was delivered.

18. A Patient Portal SHOULD have the ability for a provider of care to suppress information from view by a Delegate by marking specific information as confidential.

---

34 Within the United States, the Children’s Online Privacy Protection Act (COPPA) restricts Web sites from collecting personal data about children without explicit parental permission, and while there are algorithms for ensuring that parental access has been obtained, there are few reasons why a Patient Portal account accessed only by a Child should be created. Children typically only participate in their medical care at the direction of a parent or guardian, and it is more likely that a “Child account” would be accessed by someone other than the Child themselves. In short, independent Child-access accounts have a low likelihood of being used by children and have a high potential for inappropriate access.

35 The applicability of this requirement extends to information for Adult Subjects as well as for Adolescent Subjects when suppressing information from view is determined by a provider to be in their patient’s best interests (e.g., suppressing information about domestic violence when there is likelihood of an abusive partner coercing the Adult Subject to create a proxy relationship allowing access to their medical information through a Patient Portal).
Granularity in proxy permissions

Use Case #4: I am an adult and want to let another adult do some things, but not others, for me through my Patient Portal.

Use Case #5: I am an adult and want my sister to be able to take my kids to the doctor, if necessary, while she is caring for them over the next two weeks. It is easy make appointments through our Patient Portal, so I’d like her to have limited access to appointment features for my kids while I’m away.

Discussion

Current proxy access schemas for a Delegate acting for an Adult Subject tend to be all-or-nothing. That is, an Adult can extend access to their information to another Adult but cannot further restrict access to some features and not others.

Granular proxy access is recommended when an Adult either wants to keep select information private, or to fulfill a use case relevant to the Adult’s care such as when a friend is helping to make appointments for the Adult but should not know details of treatment.

Granular access can be difficult to implement technically, and is often difficult for the person who is restricting access to do so knowing exactly what is being restricted; for these reasons, granular access may be viewed as an enhancement (or future functionality) to existing proxy system capabilities. When granular access is offered, a best practice is for ALL access to be initially set to “off” and then allowing the Adult to select each feature or service one-by-one that they want to extend to a particular individual; in making a selection, the feature/service should be clearly described (not just giving a summary label such as “lab test results”) in order for the individual to better understand the extent of sensitive information which can be disclosed—now or in the future.

Granularity can also be enabled through an Adult Subject being able to mark certain entries (particular items in a problem list, specific medications, and specific office visit summaries) as confidential, and giving the Adult Subject the ability to suppress the information: 1) in only their Delegate’s view, or 2) for both the Delegate and themselves.

Granularity should be enabled if Patient Portal policies permit a Delegate who manages care for a Child Subject to give a different Delegate limited access to their Child’s information through a Patient Portal. For example, a parent may give their Adult sibling the ability to view a digital health plan card and make appointments for their Child while on a two week vacation, but not permit their sibling to know details about the Child’s chronic medical conditions. Note that a parent delegating access to a Child’s information is an exception to the general sense of rule #4; a Delegate managing care for an Adult Subject should not be given the ability to delegate access to another Adult; the right to extend access to anyone must rest with the Adult Subject alone.

Derived requirements

19. An Adult Subject SHOULD have the ability to express granular access permissions so they can determine which Patient Portal features a Delegate can and cannot access.

20. A Patient Portal SHOULD have the ability for an Adult Subject to suppress information from view by a Delegate by marking specific information as confidential.
21. A Patient Portal MAY have the ability for a Delegate to extend their access on behalf of a Child Subject to another Delegate for a limited period of time. If implemented, the Patient Portal: 1) SHALL give the Delegate extending access the ability to implement granular proxy access permissions; and 2) SHALL give the Delegate extending access the ability to determine the length of time the secondary Delegate can access and use services on their child’s behalf through a Patient Portal.

Nuances in proxy relationship set-up

Use Case #6: I am an adult who has caregiving responsibilities for my elderly parent with dementia, and want to manage his care through his Patient Portal.

Use Case #7: I am a caregiver for my child who has Downs Syndrome. I want to be able to manage care for her throughout her life, no matter what her age.

Use Case #8: I am 15 years old and have two children. I want to manage their care on our Patient Portal.

Use Case #9: I am 17 years old and emancipated. I take responsibility for my health and want to manage my own care through my Patient Portal.

Discussion

The typical pattern for giving access to an Adult’s account is through an Adult Subject extending access permissions to a Delegate. However, this pattern must not be used when the Adult Subject cannot give true informed consent concerning some or all medical decisions related to their care. For such cases, a Patient Portal needs capabilities to allow for a Delegate to request and receive access to an Adult Subject’s portal account.

Such a determination can be made through a number of methods, but this often requires inspection of legal documentation concerning a person’s lack of ability to care for themselves, in whole or in part. Even when an Adult is determined legally to be an Incapacitated Adult, complete access to Patient Portal information and services should not be the reflexive answer. Individuals with significant cognitive and/or developmental disabilities should be able to exercise access rights where they are capable of making decisions with informed consent, unless the Subject waives their rights (again, with informed consent).

Competency of potential Delegate caregivers must also be assessed, and any documentation which extends legal rights of access (such as a Durable Medical Power of Attorney) periodically reviewed and updated.

As such, determination whether access rights should be extended to a Delegate based on the cognitive limitations of the Adult Subject, should be made in-person. This gives the opportunity for review of documentation, discussion, and clinical assessment. A Patient Portal system needs to be able to have a manual means for a clinician making a determination of access rights so that only those features and services which the Adult Subject can no longer use effectively on their own behalf are assigned to the Delegate. To deter fraudulent and/or coercive access, the Patient Portal system must provide the ability to not permit the Incapacitated Adult’s account to use self-service tools for delegating Adult-for-Adult proxy access.
Similar issues arise when a Child or Adolescent with developmental disabilities reaches 18 years of age. Assessment of capabilities by a clinician is necessary in order for access by a parent to the Subject’s Patient Portal information to continue without consent by the Subject.

Patient Portals need flexibility in the assignment of access decisions for practical and legal reasons beyond the incapacity of a Subject. Emancipated Adolescents should have the same access rights as an Adult. A person under the age of 18 years of age who has children should have the ability to manage care for their children, with the same access as an adult.

Still, proxy access in these situations should not be extended on the basis of situation or documentation alone. For example, an Adolescent mother with young children may herself have limitations so that another responsible adult (e.g., Aunt, Grandfather), should be the individual managing care for the children.

Derived requirements

22. A Patient Portal SHALL provide administrative tools which can block self-service set-up of Adult-for-Adult proxy relationships.

23. A Patient Portal SHALL authorize one or more designated entities to block, modify, and terminate proxy relationships following written policies.

24. Written policies SHALL govern the functionality of a Patient Portal based on law and/or organizational policy to:
   • Permit access by a Delegate to Patient Portal services for an incapacitated Adult or Adolescent;
   • Permit an emancipated Adolescent to have full access to their Patient Portal information and services as if they were an Adult;
   • Require an in-person evaluation of a person said to have developmental or cognitive limitations by a clinician before proxy access rights are extended to a Delegate by the same clinician;
   • Require evaluation of a potential caregiver requesting non-normative proxy access by phone or in-person before extending proxy access to the caregiver;
   • Limit access by a Delegate to select Patient Portal services for an incapacitated Adult or Adolescent when the incapacitated individual can use a portal service to manage their own care and the individual has not permitted the Delegate to use this portal service on their behalf; and
   • Periodically review access decisions related to incapacitated individuals such that access rights are modified as an individual shows an improved capacity to make their own medical decisions with true informed consent.

Inadvisable proxy relationships

Use Case #10: I am a recent immigrant and don’t speak English. I want my unrelated friend to be with me and speak for me in all my interactions with the health care system, including through my Patient Portal.

Use Case #11: I am a friend of an adult who has episodic health issues. While I don’t routinely provide care for this person, I have brought her to the emergency department on occasion and have been asked
by the attending physician to provide background on my friend’s medical history, allergies and medication. Should I also have an account on my friend’s Patient Portal to make things easier when I do help her out?

**Use Case #12:** I am an undocumented immigrant and do not speak English. I want my son who is 12 year old and also undocumented to access my record through a Patient Portal and translate it for me, but I want to hide my history of drug abuse from him.

**Discussion**

Individuals will present many situations in which access to a Patient Portal may be helpful in some way, but in which each individual set of circumstances should be weighed before such access is extended.

In general, casual relationships in which the potential Delegate is aiding a non-incapacitated adult with aspects of care should NOT be given Patient Portal access, especially when the Delegate is not related. Non-familial relationships are more apt to quickly change, and permissions may be extended which give ongoing access to an individual’s medical information well beyond the time of it being helpful or appropriate.

Children should not be designated as proxy Delegates for Adults. Reversing parental and child roles creates dependent relationships with inappropriate boundaries which can be harmful to both parent and child.

While beyond the scope of this white paper, many issues of proxy access due to language limitations can be reduced or eliminated as Patient Portals offer information and services in languages beyond the majority-language of the population served by the portal. When offered, self-service portal account set-up and proxy account set-up services should be in all languages in use on the Patient Portal.

**Derived requirements**

25. Access to an Adult Subject’s information and services SHALL NOT be given without explicit permission from the Adult Subject.

26. If a Patient Portal offers self-service tooling to establish proxy relationships, these capabilities SHALL be offered in all languages in use on the Patient Portal.

**Summary**

Patient Portal systems which permit the set-up of proxy relationships help broaden patient engagement in meaningful ways. That is, not everyone who can benefit from the information and services available through a Patient Portal can use a Patient Portal. This includes children, and people with cognitive and more severe developmental disabilities. Portals can also help those who are capable of managing their own care to allow others to manage care on their behalf as a matter of convenience or practicality.

Permitting proxy relationships through Patient Portals also reinforces good identity management practices, such that the system is more confident of the identity of any person accessing a portal, as proxy relationships reduce the circumstances under which a caregiver takes on the portal identity of another person in order to access portal services for someone under their care.
Establishing a system of proxy access for Patient Portals requires both software capabilities and a set of policies which describe conditions for establishing, modifying, and terminating proxy relationships.

When available, the automation of procedures for the set-up of basic proxy relationships, such as a Delegate acting for an Adult or Child Subject is recommended. Making the provisioning of proxy relationships available through self-service tools speeds set-up of proxy relationships and reduces the burden of manual set-up. However, some types of proxy relationships can be difficult, if not impossible, to automate given current tools and technologies.

Given differences in Patient Portal systems, and their maturity in providing proxy access, it is reasonable to see the extension of proxy permissions as a program which can start with basic access and mature. However, even when proxy capabilities are available, they frequently remain unused due to a lack of awareness and training. A first step for initiating any system of proxy access is to designate a “Champion” within a provider office who understands how to set-up proxy relationships through manual tools within the Patient Portal system. The Champion need not be a clinician, but should always be someone who is acting with the knowledge of a clinician recommending that a proxy relationship be established. The Champion should have the ability to set-up both routine types of proxy access and proxy relationships which require more granularity (access to some, but not all, portal features).

**Additional Considerations**

Systems for enabling proxy permissions will continue to grow in sophistication, such that Patient Portals will be capable of receiving, and acting, on permissions embedded in identity credentials which are external to a Patient Portal system. For example, the HEART Working Group, a collaboration between the OpenID Foundation and the Office of the National Coordinator for Health IT, is in process of developing set of privacy and security specifications which will enable an individual to control the authorization of access to health-related data sharing APIs, which could include information about proxy access designations. Finally, while this whitepaper has focused on proxy relationships within Patient Portals, the principles discussed are generally extensible to other forms of proxy access. This includes access to other types of patient documentation and applications (such as a Personal Health Record or a mobile health smartphone app), and to digital tokens themselves which can assert proxy rights more broadly.
Appendix 2: Anonymous Access to Patient Portals

Report of the Anonymous Sub-Group of the HIMSS IDM TF

Anonymity Principles

NSTIC guiding principles state that cyberspace identities should be: 1. Privacy enhancing and voluntary, 2. Secure and resilient, 3. Interoperable, and 4. Cost effective and easy to use. Within the first guiding principle there is recognition of the need to include “the preservation of the capacity to engage in anonymous and pseudonymous activities online36”.

We agree there is a rapidly growing need to accommodate online transactions and its inherently less secure environment. Patients have a legitimate right to privacy protection that includes the request to use Anonymity and Pseudonymity37 as part of the choices they make to deal with the growing risk of data breaches that compromise the trust and confidentiality that must be part of a viable, 21st century healthcare system. Anonymity is also important for public health, research and education activities where portions of a person’s clinical information may be made public but the person’s identity must remain unknown.

Although Anonymity and the use of pseudonyms may complicate certain specific transactions in cyberspace, there are several principles that can help balance the need to satisfy a patient’s request for anonymity as well as assure transactions in cyberspace do not diminish safety considerations, encourage fraud or add to the liability burden that is often associated with healthcare.

Principle 1: To establish Anonymity or Pseudonymity a user must first be ‘known’.

Patients for a variety of reasons may request their physician or healthcare facility to create an anonymous cyberspace identity for a medical test or certain records and transactions while others may request an anonymous identifier38 or a pseudonymous identifier from their trusted provider for any reason. Here are some common examples:

A. Sensitive test result or diagnosis, e.g., HIV status, drug test or other studies that may also be protected by local statutes
B. A temporary identifier is needed as a result of a stolen or compromised identity or an identifier for an undocumented patient who wants to remotely access their record
C. Individuals, VIPs, celebrities and Politicians may also request Anonymity to protect their identity

36 See: http://www.nist.gov/nstic/privacy.html
37 Pseudonym: Use of a persona or other identifier which is different from that normally used by an individual with the intention that information be not linkable to that individual. [Adapted from ISO TS 25237]
38 Anonymous identifier: identifier of a person which does not allow the unambiguous identification of the natural person. [from ISO TS 25237]
D. Research subjects may be given special identifiers as part of the research protocol that calls for de-identification of the subjects’ information. This paper does not cover those cases where re-identification of data is not intended.

True anonymity, as defined in a document accepted by ISO\textsuperscript{39}, can never be established for all healthcare encounters. The majority of these encounters are based on a trusted relationship between the patient and a professional healthcare provider. Nevertheless, at the initiation of a patient’s request, a provider’s online clinical record system should be able – in selected cases, depending on the type and content of the information – to assign a pseudonym (or the patient’s choice of one) that can be linked to the patient’s true identity only through a process that involves the appropriate statutory or contractual authority. Thus, the scope of being anonymous in healthcare is restricted to specific providers, specific use cases, and specific classes of information (e.g., for a particular patient, it might acceptable to be identified for payments and for certain treatments, but a pseudonym must be used for storage of or access to specific test results). The pseudonym may be used only for whatever transactions are permitted through a signed agreement between the provider/practice and the patient. The agreement should also contain provisions for “breaking the glass” in situations that involve the safety and well-being of the patient. This use of a pseudonym is not intended to prevent aggregating patient data for purposes of treatment, payment or operations internally within the provider’s practice or to prevent legally authorized re-identification.

During an initial or subsequent exam a patient makes a request to create an anonymous identity to have a lab test for which they are going to pay cash. In these instances, a doctor must determine if a condition will be placed on such an anonymity request such that the lab results will be shared with the doctor within a defined time period which is acknowledged with a patient’s signature. This is desirable when a patient might have a serious communicable condition (e.g. Ebola, sexually transmitted disease, AIDS, etc.) and the potential to infect others in the community and, if the provider knows this fact, the result must be reported to public health officials. There are social service centers (e.g., both religious and secular agencies) that routinely provide such tests anonymously and the provider might refer the patient to them to avoid potential liability risk.

For the undocumented patients who want to access and view part of their health record remotely using an anonymous identity, a physician’s staff needs to adhere to their office policy when considering:
- Do they have a sufficient level of confidence about the patient’s identity to provide anonymized remote access?
- Should it be a one-time conditional access?
- Will it be two factor authentication or user-name and password?
- Is all data viewable or is there restricted viewing?

\textsuperscript{39} ISO/IEC 15944-8:2012(en) Information technology — Business Operational View — Part 8: Identification of privacy protection requirements as external constraints on business transactions

©2016 Healthcare Information and Management Systems Society (HIMSS)
Page 34 of 36
- Is this a first time request or a repeat request?
The physician should not lose sight of potential liability and risks that could be associated with undocumented anonymous identity activity and should also make the risk of harm clear to the patient.

Principle 2:
To be “known to a practice”, especially if there is a request for anonymity, a user-patient must first prove who they say they are or claim to be.

Although the term “known to the practice” does not represent a standard set of policies and procedures, there are common approaches to establishing a patient identity described above in the body of this paper. They may differ widely based on the size, location and nature of the healthcare facility or provider practice and both the facility and the patient must be aware of the limitations that may be introduced by an anonymity request.

Principle 3:
Unless the user-patient agrees to be known by an independent trusted framework system supplied by a certified entity that provides and/or securely manages online identities, a digital identity associated with a pseudonym can’t support a high level of confidence or assurance outside the issuing healthcare facility or provider’s office.

Stated another way, if the practice, the patient and the EHR vendor are all participants in a trusted framework that permits pseudonyms that adhere to the framework conditions, the level of assurance can be elevated and shared. Identity Proofing, Verification and Authentication Service Providers are certified in compliance with nationally approved standard guidelines for providing identity services, e.g., the Kantara Initiative or SAFE-BioPharma, and are a natural candidate to be a user-patient’s trusted identity source or a contracted agent for guarding and protecting a user’s authenticated identity and attribute information. Another identity source might be a trusted Relying Party (RP), keeping in mind that an RP can’t trust you until they know who you are! Once again, an acceptable alternative is that the Relying Party and the provider’s EHR and practice are all members of a Trusted Framework agreement that protect both parties against mismatches and identity fraud.

It is well known that identity fraud is commonplace in healthcare. Verifying credentials, particularly related to payment, at the initial as well as subsequent encounters is a widespread best practice in healthcare settings. If the validation test fails, the patient should be informed. At that point local policy should guide subsequent action. This may include a more detailed discussion with the patient, determining whether the requested service is an emergency and whether a process to revoke a token (if present) should be documented and initiated.

Principle 4:
A patient who wants to remain completely anonymous will be strongly considered for assignment to the lowest level of trust and assurance for all cyberspace transactions. This LOA-1 or equivalent “flag” will accompany any online transactions associated with this patient.
Although this may be a rare example of a patient request, here are some guidelines selected clinical practices may find helpful. For those patients who are unwilling to accept the usual conditions of being “known to the practice” or unwilling to sign any agreement acknowledging and accepting the conditions and potential harm of remaining completely anonymous, there are limited choices.

Nevertheless, a patient who presents to a provider office in-person with a request for service (e.g. a diagnostic test, a physical exam, etc.) can have a temporary record created and be assigned a pseudonym, or false name chosen by the patient, e.g., Donald Duck 7654, Anonymous 333, etc., as well as a unique code to retrieve results or reports online through a secure portal. The practice might choose to give the person a piece of paper (on letterhead) with the pseudonym and code and insist that the patient physically return to the practice with both in order to retrieve the results. It’s an example of two factor authentication at a minimum. This retrieval could also be accomplished online as an option.

Summary
In a typical healthcare environment, all patients must be uniquely identified in some way so that the permanent records of their care are not confused with the care records of other patients. Most healthcare organizations also want a validated mechanism for being paid which often provides a secondary means of identity proofing. Regardless of the level of identity proofing done for an individual patient, they have a right to ask for anonymity to add a layer of privacy protection to their records.

In healthcare, if a patient wishes to have anonymity so that their medical records cannot be associated with their true identity except in extraordinary circumstances, they may be assigned a pseudonym and a multifactor authentication mechanism to help protect the privacy and confidentiality of their records. This authentication mechanism is identical to that issued to a fully identity proofed patient, so no special provisions need to be made to maintain the anonymity.

The difference resides in the limitation that such an authenticated digital identity can only be relied upon by the originating organization, whereas a fully proofed identity could be used across organizations, each of which have carried out the appropriate level of identity proofing and authentication.

In the future, it may be possible for anonymous or pseudonymous identities to be more easily deployed across clinical practices, organizations and enterprises which share participation and contractual agreements in a recognized, common trust framework. We also foresee emerging technical developments which engage patients in more easily determining most of the conditions surrounding disclosure of their PHI with the possible effect that the need for anonymity will be reduced.