CONSUMER ENGAGEMENT IN HEALTH INFORMATION EXCHANGE

September 30, 2012
Prepared for the Office of the National Coordinator for Health Information Technology by:

Genevieve Morris, Senior Associate
Scott Afzal, Principal
David Finney, Principal

Table of Contents

Disclaimer

This report was created by Audacious Inquiry, LLC under a contract with the Office of the National Coordinator for Health Information Technology (ONC). The content, views, and opinions do not necessarily reflect those of the Department of Health and Human Services or ONC.

Introduction

The ultimate goal of health information exchange (HIE) is to have the right patient information, in the right place, at the right time. There are a number of ways this can and is being accomplished today. An important but as yet not fully developed avenue of exchange is consumer mediated exchange. In a fragmented information environment, where silos of electronic data and paper records are the norm instead of an exception, many consumers have mediated the exchange of their or a loved one's health information among providers out of necessity. Traditionally, this has meant numerous, tedious phone calls to ensure that records are sent where they need to go or even shuttling paper records from one medical office to another. Even as electronic HIE becomes more prevalent, consumers will undoubtedly play an important role in managing their own and their family members' health information. Some of this engagement will occur by choice—as technology empowers patients to access and better control how information is exchanged—and some out of necessity, as health information organizations (HIOs) will not always be able to supply the right data at the point of care in every situation.

Surveys indicate that consumers desire a role, or at least like the idea of having a role, in information exchange. Yet few act to do so.[1] Only a few years ago, personal health records (PHRs) were touted as a game-changing innovation. So far, though, the impact of PHRs has been modest. Even Kaiser Permanente, whose patient web portal is a notable success among a number of high profile PHR initiatives, can claim only 63 percent of its membership as having signed up for an account, with 42 percent having used the PHR more than once in the last six months. It took about six years of aggressive outreach and communication to reach this level of member adoption and program success.[2] However, patients who use the portal, especially those with chronic conditions, believe they are better able to manage their conditions. They also say the portal helps them to make better decisions about their care.[3] The evidence is fairly conclusive that, while patients say they want more access to and control of their health information, it requires a major effort by sponsors of PHR initiatives to drive adoption and use of currently-available tools. What needs to change in order to finally see a shift in consumer engagement?

The answer remains elusive. A number of factors create barriers to consumer engagement and consumer-mediated HIE, including the paternalistic nature of medicine, the current structure of health insurance plans, the indirect nature of third-party payment, technology-related challenges, and factors related to behavioral economics (why individuals act in certain ways). Each of these categories is discussed in some detail in Appendix A. Still, it is important that health information organizations (HIOs) and policymakers continue to chip away at the barriers, as consumer engagement is ultimately part of the long-term solution to many of the problems plaguing modern healthcare. This report considers these challenges specifically as they relate to HIE and offers some concrete, near-term recommendations for beginning to overcome them.

[1] A 2012 Deloitte survey found that 44% of those surveyed wanted to use an app that let them access and share their medical record, but only 10% reported doing so. http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/Health%20Reform%20Issues%20Briefs/us_chs_IssueBrief_2012ConsumerSurvey_061212.pdf.

[2] Kaiser PHR Sees More than 4 Million Sign-on: Most Active Portal to Date. Erin McCann. HealthCare IT News: August 6, 2012. http://www.healthcareitnews.com/news/kaiser-phr-sees-4-million-sign-most-active-portal-date.

[3] Ibid.

HIOs and Their Role in Consumer Engagement

Consumer engagement is a concept that has been incorporated into the mission and operating principles of many HIOs. For good reason—patient centeredness and patient ownership of information are core tenants our nation's concept of protected health information. HIOs, as trusted stewards of the exchange of that information, do well to keep patients informed, engaged, and confident in the services they provide. In practice however, many HIOs have struggled with their mandate to engage consumers. They face the same challenges health plans and provider organizations do of investing great resources in consumer outreach and communication, while seeing little activity in return. Further, unlike health plans and provider organizations, HIOs have no preexisting relationship with consumers, meaning they must begin outreach from scratch. In the near-term, consumer engagement and consumer oriented services are also unlikely to be directly tied to financial sustainability, given that HIOs are unlikely to have a meaningful direct financial relationship with the patients themselves (and in fact important constituents may view such a relationship as competitive).

Consumer Use Cases for an HIO

Aggregator of Patient Data and Conduit for Exchange

HIOs are designed to aggregate and/or index data across disparate sources and make it available at the point of care, either via "push" or "pull." In this regard, HIOs may be uniquely positioned to support the emergence of rich PHRs, whether they are operated by the HIO itself, one or multiple of its participants, or even other third parties. One can imagine a number of scenarios where this role would positively benefit patients. For example, a consumer could log in to an HIO's portal and pull the discharge summary and lab results from a recent hospital visit. She could then utilize Direct to send this information to one or many providers or to a caregiver. Utilizing this type of portal may be most beneficial for self-referred care. In such cases, a primary care provider (PCP) may be unaware that her patient has seen a specialist, and therefore unaware that she should look for information by querying an HIO. HIOs need to consider existing contracts and establishing a legal framework for such functionality. In addition, some states prohibit lab results from being released directly to consumers; HIOs must be aware of and act in accordance with these state laws.

Consent Management

While many HIOs may not be in a position to unlock PHI for patients on a broad scale, there is a role for patients to play with regards to the other core services the HIO is offering. The ability for consumers to exert influence over how their information is shared across an electronic network is not only a responsibility of an HIO; it is also empowering to the patients. Whether an HIO is operating an opt-in or opt-out model, enabling a consumer to directly choose the provider who may access their health information helps to ease the burden on the HIO of central consent management (or potentially distributed consent management by participants) and provides consumers with legitimate control of their data. Consumer consent management through an HIO-provided application can support increasingly granular levels of consent choice as opposed to the "all in" or "all out" consent options commonly available today. The barriers to offering this service, including the difficulty of consumer identity proofing, are discussed in a later section; however, when implemented it can provide reductions in administrative overhead and empowerment for the consumer.

Access to Audit Information

Today, the audit capability of many HIOs is limited. The response to a patient audit request typically takes the form of a time-stamped list of providers and other HIO users who have accessed the patient's

information. Depending on the HIE platform, an HIO's ability to actually produce such a report may be cumbersome and expensive. Enabling real-time, online access to some form of audit reporting—which could be as simple or as sophisticated as an HIO wishes or the market demands-- can potentially do more for an HIO than simply reducing an administrative burden.. It can also help to build goodwill in its service area among patients as well as to enhance transparency and security of the HIO. In addition, it will enable providers to utilize an HIO for Stage 2 of Meaningful Use for transitions of care. After all, if users understand that a patient can view an access report at any time, the temptation for misuse could be reduced.

Business Models & Pressures

Various business models have been proposed to support consumer-mediated exchange. For example, William Yasnoff, M.D., has proposed models of consumer-mediated exchange through the Health Record Banking Alliance that incorporate a range of revenue opportunities and consumer choices. These approaches identify the consumer health record bank as the source of clinical data available for exchange. Further, consumers can choose to share de-identified data or be exposed to advertisements. These selections in turn drive what fees a researcher, an advertiser, or a consumer must pay to the operator of the health record banking infrastructure.[4] These models may drive renewed interest as Direct and consolidated CDA documents become ubiquitous through pursuits of Meaningful Use. However, they continue to rely on a scale of participation that underlying consumer behavior patterns have indicated are not realistic to date. They also would constitute a dramatic shift in focus and resources from the approaches virtually all State HIE Program grantees have taken to date.

While the offerings described above are worthwhile in themselves and complementary to common HIO core business offerings, they may reasonably be viewed by many HIOs as "nice to haves" and not "need to haves" in a time when transitioning to non-grant revenue is the highest priority. The uncertain business model of Microsoft HealthVault and the exit of Google Health from the PHR space are suggestive of the challenge in driving—and ultimately monetizing—consumer engagement. The transformative effect of "consumerism" that has brought significant choice, convenience, and general empowerment in other industries has not yet seen its day in healthcare. While there are certainly cohorts of patients who do actively engage with their health information, relying on a broad base of consumers to engage and to participate in mediating the exchange of data is unlikely to be a meaningful source of revenue in the near to mid-term. As such, it may be best for HIOs in the final stages of HITECH funding to consider consumer mediated exchange through the lens of its other, core service offerings—investments in the area may be best made when they complement core services and help to support their viability.

Electronic Authentication of Consumers

Any plan for enabling consumer mediated exchange must begin with a discussion of how to authenticate individual users. Unlike providers, consumers are not tied to an NPI or similar universal identifier. Neither are they associated with a specific participating organization bound by a contractual agreement with the HIO. Therefore, the authentication methods can range from manual, low-tech means such as a face-to-face visit, to relatively more sophisticated technical solutions developed for other industries. HIOs must balance the cost of authentication methods with the necessary level of assurance that an individual is authorized to see specific information. The challenges to authentication are best broken into

[4] These principles were taken from the Health Record Banking Alliance website: http://www.healthbanking.org/pdf/principles.pdf.

three distinct areas: identity proofing, identity authentication, and access/role management. Each area has its own distinct technology and/or business policies that must be considered.

Identity Proofing

The first step in providing patients' access to their health information is identity proofing; proving the individual is who she says she is. A Registration Authority (RA) is a person or entity responsible for identity proofing. Identity proofing can suffer from false-positives (authenticating a user who is not the individual) and false-negatives (not approving a user who is the individual). Good identity proofing processes seek to minimize both false-positives and false-negatives, at a reasonable cost. While in-person identity proofing would perhaps be the most secure method with the least amount of false-positives and false-negatives, it is not necessarily feasible for consumers or HIOs to perform in-person identity proofing; especially given consumers' expectations that they can be electronically proofed, having become accustomed to electronic identity proofing for their financial services. Unfortunately, the level of tolerance for loss of financial data due to identity fraud is very different than for health information, making it necessary for HIOs to determine how they will perform either in-person or electronic identity proofing. The goal of identity proofing is to pass through roughly 99 percent of individuals without manual intervention and without false positives. The ability to do this is dependent on a number of factors.

The National Institute of Standards and Technology (NIST) electronic authentication guidelines (including identity proofing and ongoing authentication) are required to be used by federal agencies when remotely authenticating an individual. The private sector also uses the NIST guidelines for identity proofing and authentication. NIST has four levels that vary in their security and complexity, with level 1 being the least secure and easiest to obtain, and level 4 being highly secure and very difficult to obtain. Appendix B provides a detailed list of what is required at each level for both in-person and remote proofing. Generally the following identity proofing is required at each level:

- Level 1: No identity proofing is required.
- Level 2: Single factor remote network authentication
- Level 3: Multi-factor remote network authentication
- Level 4: Proof of possession of a key through a cryptographic protocol. Requires in person identity proofing.

The appropriate level is chosen based on the consequences of an authentication error. Since there are potentially harmful consequences to an authentication error when accessing health information, Level 1, which provides no identity proofing is clearly not appropriate. Likewise, Level 4, which requires in-person identity proofing and hard tokens, is also not commensurate with the potential consequences, leaving HIOs a choice between Level 2 or Level 3 for identity proofing of consumers. It should be noted that ONC has recommended that identity proofing of providers who are accessing the HIO's data for treatment of their patients should be Level 3.[5]

In-person identity proofing can be performed at a provider's office when a patient presents for a visit. Many offices already ask for photo identification at the beginning of a visit and make a copy of the ID for

[5] Privacy and Security Framework Requirements and Guidance for the State Health Information Exchange Cooperative Agreement Program. ONC-HIE-PIN-003: March 22, 2012. http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_0_5545_1488_17157_43/http%3B/wci-pubcontent/publish/onc/public_communities/_content/files/onc_hie_pin_003_final.pdf.

the patient's record. This would be considered Level 2 in-person identity proofing. Level 3 adds a second factor to the proofing, such as sending credentials to a phone number on mailed to the address on record. A provider could identity proof his patient in-person during a visit, send a notification to the HIO to create an account for the proofed patient, and have the HIO mail the patient's credentials to her address on record. Alternately, an HIO can create an electronic remote identity proofing process that complies with Level 2 or 3. Patients could then sign-up directly with the HIO to receive access to her records.

A recent development in electronic authentication is the National Strategy for Trusted Identities in Cyberspace (NSTIC), a strategy designed to allow "individuals and organizations to utilize secure, efficient, easy-to-use, and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation."[6] NSTIC is working to create an identity ecosystem for both public and private use that provides a single credential for each individual that chooses to participate in the ecosystem. Overall, the strategy has four guiding principles: identity solutions will enhance privacy and be voluntary, be secure and resilient, be interoperable, and be cost-effective and easy to use. The federal government is supporting the private sector in developing the identity ecosystem through a number of methods, including being a leader in using the identity ecosystem in federal agencies. NSTIC is currently leading development of the standards and policies for a single online identity, but it is unclear when this will be a reality.

Identity Authentication

Once a user's identity has been positively proofed by the RA, the Credential Service Provider (CSP) issues both a token and credentials that are bound to the identity. The RA and CSP can be the same entity. An HIO could perform both roles, or alternately, an HIO can partner with an organization such as Equifax/Anakam or Experian to be the RA (when using remote electronic authentication). Credit bureaus are often leaders in the RA industry, due to their large databases of consumer information. According to NIST, identity authentication has three possible factors that are considered:

- 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 voice print or other biometric)

Tokens fall into one of these categories. NIST recognizes nine types of tokens:

- Memorized secret token: something you know such as a password, passphrase, or PIN.
- Pre-registered knowledge token: something you know, such as a challenge question where the user has registered a response with the CSP, or registered an image that she must choose at each authentication.
- Look-up secret token: something you have, such as an electronic table that stores responses to prompts.
- Out of band token: something you have, a physical device that can receive a one-time secret, such as a cell phone receiving a text message with a numeric code.
- Single-factor one-time password device: something you have, a physical device that can generate one-time passwords, such as a device carried with you.

[6] National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy. Whitehouse: April 2011. http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

- Single-factor cryptographic device: something you have, a hardware device that generates cryptographic keys, such as a digital signature or certificate.
- Multi-factor software cryptographic token: something you have, know, and/or are, a digital signature or certificate that is activated by a second factor.
- Multi-factor one-time password device: something you have, know, and /or are, a physical device that can generate one-time passwords and requires second factor to use, such as an RSA SecureID token.
- Multi-factor cryptographic device: something you have, know, and /or are, a hardware device that generates cryptographic keys and is activated by a second factor.[7]

The NIST levels have different minimum factor requirements, with Levels 3 and 4 requiring two factor authentication. Two factor authentication requires two token categories be used, meaning that both tokens cannot be something the user knows. Rather something the user knows must be combined with something she has or is. As with identity proofing, Level 1 is most likely not stringent enough, while Level 4 is overly stringent, leaving an HIO to choose between Levels 2 and 3. It should be noted that ONC has recommended that authentication of providers who are accessing the HIO's data for treatment of their patients should be Level 3.[8]

Credentials bind identifying information to a token. The information that is bound to the token must allow for the recovery of registration records, and a name that is associated with an identity, i.e. there must be enough identifying information to trace back to the record to ensure the user was positively identity proofed. Credentials can be both public and private. The most common credential is the X.509 public key certificate.

Identity authentication is performed each time a user logs into the system. If using NIST Level 2, a user would only need to provide something she knows in order to access the system. Level 2 can include a single-factor authentication, but two or more tokens. For example, many online banking systems require a password and the answer to a challenge question. This is NIST Level 2, but with two tokens required. If using Level 3 for authentication, the user will need to provide something she knows and something she has (it would be nearly impossible to provide something you are electronically) each time she logs in, or at specific time intervals (every 60 days), or when using a non-registered computer or mobile device.

Access/Role Management

The access a user has to the system or the role the user is assigned in the system is a business process decision, not a technical decision. The access a user is granted is typically based on the user's authentication. The access given to a user is very important, especially with health information. A user may require access to not only her own records, but also a family member or friend for whom she is the primary caregiver. This can become a larger issue when a user's child moves into adolescence and various state laws differ on the information a parent/caregiver can have access to. Additionally, when a

[7] Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-63-1: December 2011. http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf.

[8] Privacy and Security Framework Requirements and Guidance for the State Health Information Exchange Cooperative Agreement Program. ONC-HIE-PIN-003: March 22, 2012. http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_0_5545_1488_17157_43/http%3B/wci-pubcontent/publish/onc/public_communities/_content/files/onc_hie_pin_003_final.pdf.

physician accesses records, it is important to distinguish between when he is acting as a physician looking for treatment records, and when he is acting as a patient seeking his own records or those of his family. HIOs must determine how they will assign all of these roles and manage them over time.

Case Studies

The case studies provide real world examples of HIO and non-HIO entities that are working engage consumers in health information exchange. The information was developed based on interviews with the organizations. The individuals interviewed were provided an opportunity to review the content and provide edits where appropriate.

Aetna

The Aetna Personal Health Record (PHR) is an online record that is populated with health information from Aetna's claims system and gives users the opportunity to manually enter non-claims personal health information. The PHR is integrated with a number of Aetna's programs, including those from chronic disease management and the health and wellness program. It provides condition specific educational materials as well as alerts and messages to its users. This content is personalized for each individual based on the CareEngine rules system that continuously analyzes a user's data to provide up to date content. Users can download their health information in text or pdf format; Aetna provides a Blue Button download. Users can also share their data online with their provider or covered family members. Data is shared with providers via the Navinet platform. They can also transfer their health information to Microsoft HealthVault using an HL7 CCD release 3 format. In 2011, 858,665 Aetna members utilized their PHR. In the past 30 days, 179,373 members have logged onto the PHR, with care alerts and reminders being the most frequently used service.

Microsoft HealthVault

Microsoft HealthVault is an online service that allows individuals to store their health records from various sources in one central location. HealthVault uses standard APIs to allow for a robust ecosystem of apps, including those from pharmacies, labs, and PHRs. Users can choose which apps to use with their HealthVault accounts, including apps that pull in data and those that analyze the data. Prior to an app being connected to the platform, HealthVault signs a standard agreement with the company creating the app; the agreement states that the app complies with all HIPAA requirements, if appropriate for that app. HealthVault also works with the app developer to ensure that the minimum data necessary for the app to function correctly is all that is shared, rather than all data elements in a user's account. The apps allow patients to pull and share either individual data elements, such as lab results or medications, or a care summary, such as a CCD. HealthVault can accept a CCD (C32), CCR, or consolidated CDA CCD via three methods: uploaded as a file, sent as an attachment to a Direct message, or inserted by an app (either a PHR or EHR) using the HealthVault API. HealthVault is able to accept and correctly parse out a CCD or CCR from most vendors, some through an app connected through an API and others via Direct, or a third party connection. This is possible because HealthVault publicly shares its preferred CCD/CCR format, allowing EHR vendors to build to the same specification, and also extends its parsing code to support variations wherever possible. Users can download a CCD from HealthVault to share with their providers via Direct or the HealthVault API, which is an XML-over-HTTP interface (users can choose to mark some data as private prior to downloading). However, most EHR systems do not accept and parse out the CCD, except via a file upload. A few vendors, such as Allscripts, have built a way to pull a CCD from HealthVault into the EHR and tag the data as being patient entered. Likewise, Greenway is piloting

a connection with HealthVault that allows patients to pull data from the Greenway EHR into HealthVault and share a CCD from HealthVault with the Greenway EHR.

HealthVault does not perform identity proofing itself. A user can create an account and enter her personal information, without going through an identity proofing process. However, as a user begins to use apps that provide PHI to the HealthVault account, each app performs identity proofing, some in-person and some electronically, typically using NIST Level 3 two factor authentication. The appropriate level of authentication is chosen by the data holder, where stewardship of the clinical data resides. HealthVault does not provide any clinical information to the patient, that she does not enter herself or pull from an app. Consequently, HealthVault is not the responsible entity for identity proofing; the app that is providing the data is responsible. For example, if a user wants to incorporate her lab results from Lab Corp. into her account, she adds the Lab Corp. app and accesses Lab Corp.'s site, where she will be asked to enter date of birth and social security number, and then be presented with challenge questions. Once the user has been positively proofed, she will receive access to her lab results. Alternately, Quest utilizes in-person identity proofing. In order to receive Quest lab results, the user must enter a PIN she received from her provider to access results from that specific provider. The provider has positively proofed the individual in-person, when she visited the office. Both methods are secure, and both ensure that information does not flow into HealthVault that does not belong to the user. In addition, if an individual wants to share their health information with a new provider via Direct, the provider can in-person identity proof the individual at the visit, prior to incorporating the data into a patient record.

Rochester RHIO

The Rochester RHIO launched its patient portal about two years ago. The HIO utilizes Anakam as its Registration Authority (RA). The HIO uses NIST Level 3 identity proofing and authentication. When users request access to the system, they must answer knowledge based questions and verify account information. The authentication processes utilizes two-factor authentication, requiring a password and a passcode that is sent to the user via text message or email. Once a user utilizes the passcode on a computer to log in to the system, the passcode is valid for 60 days without being re-entered. If the user attempts to access the system from a different device, a new passcode is issued. Anakam provides these services in the cloud, and sends the information to Rochester RHIO. The HIO must then accurately link the information sent from Anakam to a patient in the master patient index (MPI). To date it has been difficult to automatically link the Anakam identity to a patient in the MPI, due to the difference in how demographics are recorded in Anakam versus the MPI. Rochester RHIO estimates that approximately 75-80 percent of users are not automatically linked and must call the HIO to manually link their records.

The HIO's portal has not experienced high patient usage or satisfaction, mainly due to the lack of data available. The HIO may not share data with a patient, unless the organization that is holding the data approves its release through the HIO. In addition, due to New York State law, lab results are not allowed to be shared directly with a patient, but rather must be reviewed by a provider first. Hospitals and providers have not yet demonstrated much enthusiasm for sharing data with patients through the HIO, finding direct patient connectivity through their own systems to be preferable; leaving users with no data to review or use once they access the portal. Patients are able to request an audit history, manage consent, and share advance directives via the HIO. However, the value proposition for these items is not very high, since access to data is what users expect when they register with the HIO.

UnitedHealth Group

UnitedHealth Group (UHG) has been working on a number of consumer facing initiatives, building a health IT ecosystem for members called eSync. The eSync platform includes a personal health record (PHR) offering. In June 2012, the company launched Blue Button capability in its PHR, using the VA licensing requirements. UHG's implementation of Blue Button allows members to download, save, and/or print their health information in ASCII text or PDF formats. UHG negotiated a format change within the VA licensing guidelines in regards to the layout of the document and the sequencing of its information. The company tested various formats for usability and modified the final format to best fit the needs of their members. Members can use http://www.myUHC.com to obtain their health information and share it with providers via multiple transport mechanisms, while UHG continues to research, develop and implement better, faster, and even more secure transports.

The Blue Button capability is available to commercial plan members, with the initial rollout being offered to 4 million members, with an expected availability to 26 million members in the next 12 months. As of August 7th, 2012, over 17 million members have Blue Button availability. The Blue Button feature has been utilized by more than 12,000 members since it was launched. UHG has found that adoption is not as much a technology problem as it is a cultural problem. The company is working with providers to present a standard message to patients about using the PHR and Blue Button. UHG believes that if providers are not willing to use the technology and encourage their patients to use it, then the patients will not use the PHR.

Moving forward, UHG is building upon the existing eSync platform to build a vendor and format agnostic ecosystem that will allow members and non-members (consumers) to pull all of their data into a central location. The envisioned PHR platform will be a central, patient-centered data hub that will pull together multiple data sources. Since providers tend not to trust data when they do not know the source of the data, UHG is working on the technology to be able to tag data with a data source, which will then allow providers to make their own judgment call on adding the data to their EHR. UHG believes that most of the data coming into the platform will be formatted, but some data will be unformatted and received via fax or scanned documents. UHG is working incrementally to be able to take in data and parse it out correctly to support a consumer-centric, consumer-controlled, portable, secure PHR.

Experian and Symantec

Experian and Symantec work together to provide multi-factor identity proofing, authentication, and credentialing. They act as both a Registration Authority and a Credential Service Provider. In early 2012, CMS contracted with Experian and Symantec to provide enterprise remote identity proofing and multi-factor authentication credential services. One of the projects Experian has been working on is the identity proofing and authentication process for the federal health benefit exchange that CMS is developing. CMS and Experian identified a number of challenges with both identity proofing and authenticating/credentialing individuals for the health benefit exchange. Due to the similarity of the data contained in the health benefit exchange, HIOs that pursue a patient portal offering will face some of the same challenges.

Federal agencies are required to follow the NIST 800-63-1 guidelines for electronic authentication. At the same time, they are also working to follow the NSTIC guidelines that are being developed. The Administration has stated that Federal agencies will be leaders in adopting the NSTIC guidelines; consequently while they must currently meet NIST guidelines, they must keep an eye towards future changes once NSTIC is fully developed. CMS and Experian have been looking at the NIST level 2 and 3

guidelines and are working to determine the best approach for identity proofing and credentialing individual users that balances NIST levels of assurance requirements, availability of identity data elements, fraud risk mitigation, and user experience, including online approval rates. CMS's goal is to pass as many online enrollment inquiries as possible. In order to do this, however, key identity data elements must be collected; the more data collected, the more likely Experian is able to assess risk accurately, meet a level of assurance requirements, and ultimately prevent users from having to engage in more costly phone-based or in person identity proofing routines. However, individuals are reticent to provide sensitive data in order to be identity proofed, especially financial account data specifically required for level of assurance 3.

In addition, individuals using the health benefit exchange may not have enough financial account data in order to be positively proofed at NIST level of assurance 3. This is especially true in cases where multiple "out-of-wallet" questions are used to verify such information. CMS and Experian are working on alternate options (including questions) that can be used to prove identity at level of assurance 2 and 3. While the goal is to pass through as many individuals as possible without fraud, a balanced realistic approach that recognizes the inherent tension between NIST level of assurance requirements, outlier populations with typically lower online data footprints and profiles (such as younger age groups, seniors, and even homeless individuals), and the burden to average users must be considered. Experian believes that risk-based approaches to identity proofing, such as those used in the financial sector, should be considered for healthcare. Risk-based identity proofing has the ability to identify fraud at a more efficient rate than traditional rules-based proofing.[9]

Conclusion

Most HIOs have consumer inclusion and engagement as part of their missions. However, engaging consumers and making them active participants in the exchange of their and their loved ones' health information has been a tall order, in spite of great hopes and some hype. HIOs need to possess a good understanding of the challenges of consumer-mediated HIE in order to develop plans for investing in it. Doing so is not only mission-fulfilling but also complementary and additive to core services which help to drive financial sustainability.

[9] Identity Proofing: A Risk-based Approach to Agency Identity Proofing: Experian's Lessons Learned and Best Practices for Government. Experian Government Services White Paper: 2010. https://annualcreditreport.experian.com/assets/government/white-papers/identity-proofing.pdf

Appendix A: Behavioral Economics & the Challenge of Consumer Engagement

Paternalistic Nature of Medicine

Historically, the doctor-patient relationship would not have been characterized as a partnership that involves shared decision making. Rather, the doctor would *tell* the patient to "take two of these and call me in the morning." Further, physicians and other healthcare providers, with the benefit of a decade or more of specialized training, are viewed in our society as holders of highly specialized knowledge and practitioners of an art and science that is all but incomprehensible to others. These factors have conditioned many patients not to ask questions or take an active role in making decisions about their health. In fact, many patients may feel intimidated by their providers, the healthcare system generally, and their own lack of knowledge.

If the physician is seen as the authority, than patients have little need to access their health information or be the conduit of exchanging that information with others. While most patients want their information to be available at the point of care, many just expect it to be there, and may not realize that physicians are not sharing information with each other. While patients have the right under HIPAA to access copies of their medical records, the paternalistic attitude in medicine discourages patient inquisitiveness. A 2011 survey of primary care physicians (PCP) on the use of OpenNotes with patients, found that almost half of PCPs that participated in OpenNotes were concerned patients would be confused by the information and worry more, and the majority of PCPs who did not participate cited this confusion and worry as reasons for their lack of participation.[10] Unless patients believe they are a partner in their health care, rather than a passive participant, and have the ability to understand their medical information, they will see little need to access or control their health information.

Data Ownership

Consumer health information is not owned by the healthcare organizations that create it. While patients have the right to access their health information under HIPAA, providers and hospitals tend to be reticent to provide it. There are two prevailing reasons for why this is the case. One is that a patient with open access to his own health information may be more likely to bolt for a competitor or drive their own referrals. Second, providers may rightly fear how a patient will interpret her own health information. A patient poring over test results could increase the number of calls that the doctor's office must field, or even worse the patient may be offended or upset by the physician's notes (which can be frank). Providers and hospitals may also fear litigation if a patient is unhappy with what she finds in her records. A shift in the way providers view patient health records—and the way they create them, without consideration that the patient may wish to read them—is required, though it is unclear what catalyst could cause this shift. For some providers, Meaningful Use may be a first step.

[10] Inviting Patients to Read Their Doctors' Notes: Patients and Doctors Look Ahead: Patient and Physician Surveys. Jan Walker, et al. Annals of Internal Medicine. 2011 Dec;155(12):811-819. http://annals.org/article.aspx?volume=155&issue=12&page=811.

Third-Party Payment

The majority of U.S. health insurance policies consist of premiums and copays to pay for services. The bill for services rendered is rarely presented to the patient, and the list prices for services are not the actual prices paid by anyone. The current system of third-party payment effectively masks the cost of care to the consumer. A consumer with a good insurance plan with monthly premiums and a low deductible has little financial responsibility for the medical care they receive. While the costs of overuse of the health care system accrue to the general public, the cost to the individual is masked. Consequently, individual consumers in these plans have little incentive to minimize their use of healthcare services or ensure that services are not duplicated at various facilities. From a purely financial standpoint, it is not important to that consumer that her health information be available at each point of care, because she does not pay any significant amount of money for duplicative services.

On the other hand, it is financially very important to payers and employers that the information be available—and in value-based purchasing models, it is also important for providers. However, neither the fee-for-service model nor the value-based purchasing model encourages consumers to mediate the exchange of their health information. There is no financial penalty (beyond the shared burden of rising premiums) to consumers if tests are duplicated and unnecessary care is provided in either model. High-deductible plans seek to shift some of the immediate financial burden to consumers and have become increasingly prevalent over the last year, even among Fortune 500 companies that may seem more equipped to share the premium burden with employees. Consumers with high-deductible plans will presumably feel increased motivation to ensure their health information is available at the point of care, but it is not yet clear if this motivation will be borne out as increased engagement.

Technology Challenges

Consumers who are so inclined may choose from "tethered" and "untethered" PHR options to aggregate their health information. The tethered category, where the PHR is connected to some other source of data, includes hospital and provider patient portals as well as most payer portals. A common limitation of tethered PHRs is the fact that they contain data from only one source—for instance the hospital or practice sponsoring the service. For payer portals the data is typically claims and encounter data rather than clinical data (i.e., it will list that a lab test was done but not the results of the test). Many untethered PHRs also have limitations. For instance, some have challenges importing data from various sources, parsing it, and then presenting it usefully. Many untethered PHRs require consumers to manually enter in their medical history or current lab results; this data entry may be worthwhile for some patients who have made plans for a hospital to be able to access the information in the case of an emergency, but most patients are unlikely to invest the time required. Importing a care summary, such as a CCD[11] is possible with many untethered PHRs; however, the data may not be parsed out into the patient history, and may only be available to view in an unreadable HTML format. The exception with CCD importing is if the CCD is from an EHR vendor that has worked to build an interface or an API with the untethered PHR. The same is true for exporting a CCD to an EHR system. The majority of EHR systems will not accept and parse out a CCD from a PHR. Consequently, the provider and patient are left with an XML document that is not human readable. The majority of consumers must choose either a tethered PHR that has some of their data or an untethered PHR that only contains data that they manually enter. In both cases, consumers will face challenges sharing the data contained in the PHR with all of the providers responsible for their care.

[11] CCD here refers to both the traditional CCD C32 document and the Consolidated CDA CCD.

Maximizing Utility

Most economic and behavioral economic theories postulate that individuals are rational and act to maximize their utility, i.e., individuals rationally make choices and behave in ways to ensure that the best possible outcome occurs. In order to maximize utility, individuals weigh the costs and benefits of specific actions to determine whether their utility will be maximized by the action. Within this concept of costs/benefits and utility maximization, there are a number of factors that lead individuals to believe either consciously or unconsciously, that engaging with their health information will not maximize their utility. First, when weighing costs and benefits, individuals tend to undervalue or underweight benefits that are separated over time from the initial cost. This is known as time discounting. The further away a benefit is from the initial cost, the less an individual perceives it as a high benefit, even though the actual benefit does not change. For example, currently an individual must pay a high cost for accessing and using her health information; the cost is typically in the form of time spent, but may also be strictly financial if a physician charges for records. The cost may also be the esteem of the individual's provider (if the individual feels the provider will be unhappy that she is requesting access to her records). The benefit of having this information will most likely be separated in time. Individuals must act now, so that some time down the road their records are at the right place, when the individual seeks medical care. The further in time the benefit is perceived to be, the lower an individual will value the benefit, and the less likely she is to believe the cost of taking action is outweighed by the benefit.

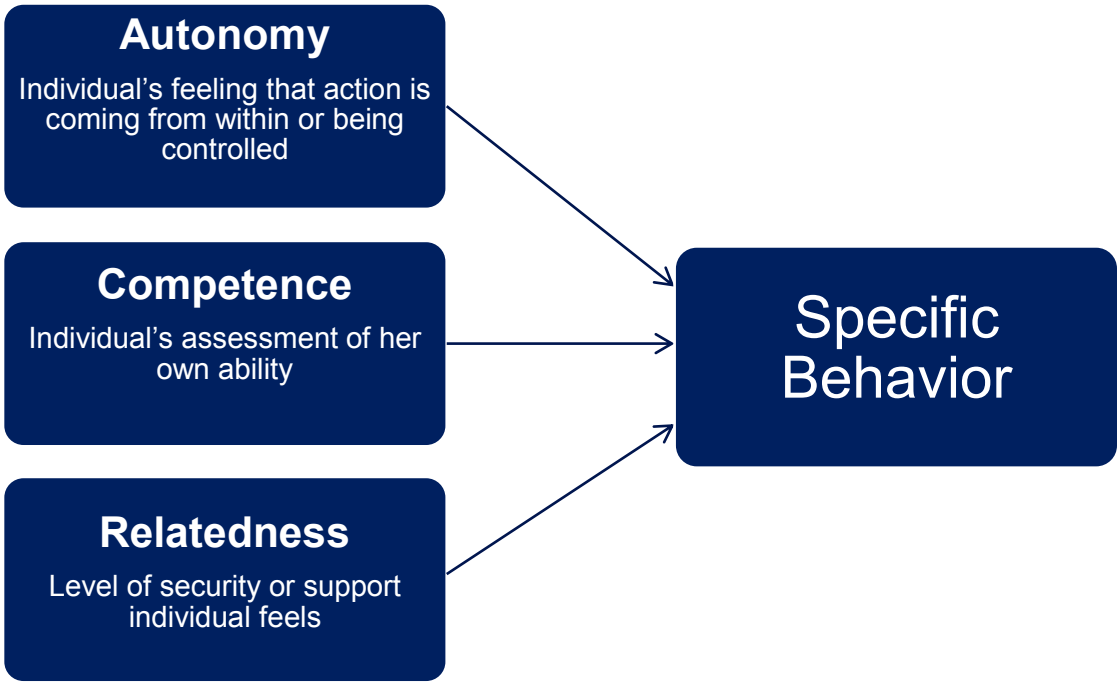
Closely linked with time discounting is the theory of unrealistic optimism. It has been proven that while individuals act to maximize their utility, they are not necessarily rational, especially in how they weight gains and risks. Especially when it comes to health, individuals have an unrealistic optimism about their susceptibility to risks; they tend to underweight their own susceptibility to a health risk and overweight others'. If individuals believe that they will not suffer from a health condition in the future, they are not likely to believe the cost of accessing and using their health information is worth the payoff. Not only is the benefit weighted lower because of time discounting, but the unrealistic belief that there will never be a benefit because there will not be a need for their health information to be easily accessible, leads individuals to be passive in their care, rather than active participants.

Self-determination Theory

Individuals' behavior is driven by both intrinsic and extrinsic motivations, intrinsic being the internal motivators of the individual, and extrinsic being external motivators such as rewards or punishments. The way that extrinsic and intrinsic motivators work together to cause behavioral change is known as self-determination theory. The social context within which an individual is operating can either foster tendencies to grow and involve or impede them. The diagram below describes the three factors that lead an individual to adopt a specific behavior.[12, 13]

[12] Self-determination Theory and the Facilitation of Intrinsic Motivation, Social Development, and Well-being. Richard M. Ryan and Edward L. Deci. American Psychologist, Vol 55(1), Jan 2000, 68-78. http://dx.doi.org/10.1037/0003-066X.55.1.68.

[13] For a detailed explanation of self-determination theory, see http://www.selfdeterminationtheory.org/theory.



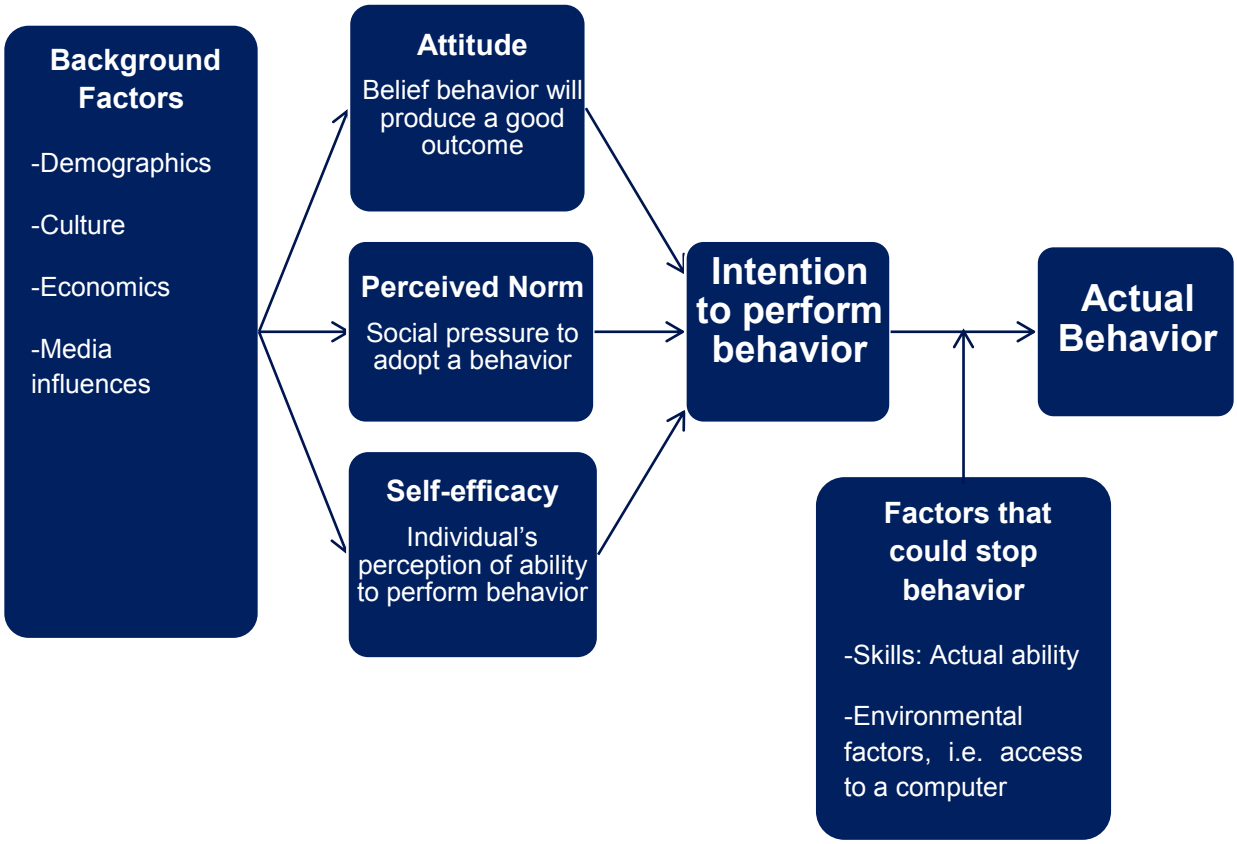
When this is applied to consumer behavior with regards to their health information, it partially explains why consumers are not more involved. As noted earlier, medicine tends to have a paternalistic attitude that does not encourage the autonomy of the patient. In addition, patients tend to feel less than competent when it comes to understanding their health information (although this is slowly changing thanks to the Internet) or they may not feel competent with technology, which is discussed in more detail in the technology acceptance models. Finally, patients are not likely to have a high level of relatedness in this area. In order for relatedness to be high, patients must feel that their provider is caring and supportive, especially in relation to accessing health information; recent studies have found that many patients do not view their provider this way.[14] If the social context does not support all three of these factors, then consumer engagement in mediating their health information will presumably remain low.

Integrative Model of Behavioral Prediction

The integrative model of behavioral prediction is similar to self-determination theory, in that it constructs a model of factors affecting intentions (these factors are similar to those seen in self-determination), and adds to intentions the intervening factors that explain why intentions do not always lead to expected behaviors. The diagram below shows the factors that affect an intention to perform a behavior, and the factors that can stop a behavior from actually being performed.[15]

[14] Shared Decision Making: Authoritarian Physicians And Patients' Fear Of Being Labeled 'Difficult' Among Key Obstacles To Shared Decision Making. Dominick L. Frosch, Suepattra G. May, Katharine A.S. Rendle, Caroline Tietbohl, and Glyn Elwyn. Health Aff May 2012 31:51030-1038. http://dx.doi.org/10.1377/hlthaff.2011.0576.

[15] The diagram was recreated from The Integrative Model of Behavioral Prediction as a Tool for Designing Health Messages. http://www.sagepub.com/upm-data/43568_2.pdf.



For consumers to actively engage in accessing, using, and sharing their health information, not only do they have to intend to do so, but the intervening factors must also be supportive. In general, consumers' attitudes, perceived norms, and perceived capability are not conducive to having a positive intention. The predominant attitude is not necessarily that accessing and using their health information will lead to a bad outcome, but may rather be a belief there will be no outcome, either good or bad. The perceived norm of consumers is that their social network is neither expecting them to access and use their health information and does not impose social penalties on those that do not, nor is the network performing this behavior itself. Finally, consumers' perceived capability is that they cannot access their health information, least of all electronically, nor do many feel that they can appropriately use the information to improve their health. Consumers, consequently, do not have an intention to access and use their health information. This negative intention is due to the background variables involved. The culture of medicine, the socio-economic factors, demographics, etc., combine to create a negative intention. When the background variables are changed, the intention is different. For example, consumers with a chronic condition have a background factor that influences their attitude and perceived norms. Likewise, patients who have been negatively impacted by errors in their data or a lack of data at the point of care, have background factors that influence attitude and perceived capability. All three factors that influence intention can be modified through the right messaging framework; leaving actual skills and environmental constraints to affect actual behavior. Consumers may have a lack of skills, mainly with computers, that impede them from accessing and using their health information even if they desire to do so. There are certainly environmental constraints that affect behavior—technology constraints with PHRs and EHRs, lack of access to a computer or the Internet, etc. When some of these constraints are resolved, consumer engagement should increase.

A good example is the Kaiser PHR referenced previously, which is called My Health Manager. The PHR contains all of a patient's data from all of the providers they see (as long as they are in the Kaiser network).[16] Kaiser's providers encourage patients to use the portal and support a positive attitude and perceived capability, as well as a perceived norm that this is expected of them. It should be noted that Kaiser did not change intentions overnight. The portal launched to all members in 2006, and currently of 9 million members, 4 million are using the system. Over time, Kaiser was able to change consumers' intentions, and ensure that both skills and environmental constraints do not intervene to stop behavior. Today, the mobile app version of the PHR accounts for about sixteen percent of all visits.

Technology Acceptance Model

As technology has developed, models of technology acceptance and use have also developed. The Technology Acceptance Model (TAM) 3 is a framework that explains an individual's intention to use technology and actual use of the technology. The framework is built based on self-determination theory, the integrative model, and other psychological models and is specific to technology.

TAM 3 has a number of familiar factors, including: subjective norm (whether the individual believes her social network thinks she should use the technology), result demonstrability (whether the individual believes the results can be shown and be positive), computer self-efficacy (whether the individual believes she has the ability to use the computer), objective usability (whether the individual actually has the capability), perceived usefulness and perceived ease of use. TAM 3 adds in a number of new factors that are more specific to IT, and can be applied to consumer engagement in health IT. Factors specific to IT include:

- Computer anxiety and playfulness
- Perceived enjoyment
- Job relevance – Whether the individual believes the system is relevant for her job, i.e., whether the health record is relevant to the individual's role as a patient.
- Output quality – Whether the individual believes the system performs her job tasks well, i.e., if the patient's role is to mediate her health information, does the system perform this.

The factors that are called anchors: computer self-efficacy, perceptions of external control, computer anxiety, and computer playfulness; are all items that affect an individual's perceived ease of use, but they can be mitigated if the system is enjoyable and easy to use. Experience and voluntariness can also mitigate the effects of perceived usefulness and perceived ease of use.

Much like the other models that have been discussed, the TAM 3 model can be used to explain reasons for the lack of consumer participation in exchanging their health information. When the model is boiled down to its most basic elements, perceived usefulness and perceived ease of use, the conclusion can be drawn that consumers do not believe engaging with their health information will bring about a useful outcome, and at least initially, many do not believe they are capable (or may actually not be capable) of doing so. While explaining why consumers do not engage, the model can be helpful for determining ways to help consumers engage.

[16] Kaiser PHR Sees More than 4 Million Sign-on: Most Active Portal to Date. Erin McCann. *HealthCare IT News*: August 6, 2012. http://www.healthcareitnews.com/news/kaiser-phr-sees-4-million-sign-most-active-portal-date.

Appendix B: NIST Identity Proofing Levels[17]

Level 1	In-person	Remote
	No identity proofing requirement	No identity proofing requirement
Level 2	**In-person**	**Remote**
Basis for Issuing credentials	Possession of a valid current primary government picture ID that contains Applicant's picture, and either address of record or nationality of record (e.g., driver's license or Passport)	Possession of a valid current government ID (e.g., a driver's license or Passport) number and a financial or utility account number (e.g. checking account, savings account, utility account, loan or credit card, or tax ID) confirmed via records of either the government ID or account number. Note that confirmation of the financial or utility account may require supplemental information from the applicant.
RA and CSP actions	RA inspects photo-ID; compares picture to Applicant; and records the ID number, address and date of birth (DoB). RA optionally reviews personal information in records to support issuance process "a" below. If the photo-ID appears valid and the photo matches Applicant then: a) If personal information in records includes a telephone number or e-mail address, the CSP issues credentials in a manner that confirms the ability of the Applicant to receive telephone communications or text message at phone number or e-mail address associated with the Applicant in records. Any secret sent over an unprotected session shall be reset upon first use; or b) If ID confirms address of record, RA authorizes or CSP issues credentials. Notice is sent to address of record, or; c) If ID does not confirm address of record, CSP issues credentials in a manner that confirms the claimed address.	RA inspects both ID number and account number supplied by Applicant (e.g., for correct number of digits). Verifies information provided by Applicant including ID number **OR** account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, DoB, address, and other personal information in records are on balance, consistent with the application, and sufficient to identify a unique individual. For utility account numbers, confirmation shall be performed by verifying knowledge of recent account activity. (This technique may also be applied to some financial accounts.) Address/phone number confirmation and notification: a) CSP issues credentials in a manner that confirms the ability of the applicant to receive mail at a physical address associated with the Applicant in records; or b) If personal information in records includes a telephone number or e-mail address, the CSP issues credentials in a manner that confirms the ability of the Applicant to receive telephone communications or text message at phone number or e-mail address associated with the Applicant in records. Any secret sent over an unprotected session shall be reset upon first use; or c) CSP issues credentials. RA or CSP sends notice to an address of record confirmed in the records check.

[17] Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-63-1: December 2011. http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf.

Level 3	In-person	Remote
Basis for issuing credentials	Possession of verified current primary Government Picture ID that contains Applicant's picture and either address of record or nationality of record (e.g., driver's license or passport).	Possession of a valid Government ID (e.g., a driver's license or Passport) number and a financial or utility account number (e.g., checking account, savings account, utility account, loan, or credit card) confirmed via records of both numbers. Note that confirmation of the financial or utility account may require supplemental information from the applicant.
RA and CSP actions	RA inspects photo-ID and verifies via the issuing government agency or through credit bureaus or similar databases. Confirms that: name, DoB, address, and other personal information in record are consistent with the application. Compares picture to Applicant and records ID number. If ID is valid and photo matches Applicant, then: a) If personal information in records includes a telephone number, the CSP issues credentials in a manner that confirms the ability of the Applicant to receive telephone communications at a number associated with the Applicant in records, while recording the Applicant's voice or using alternative means that establish an equivalent level of non-repudiation; or b) If ID confirms address of record, RA authorizes or CSP issues credentials. Notice is sent to address of record, or; c) If ID does not confirm address of record, CSP issues credentials in a manner that confirms the claimed address.	RA verifies information provided by Applicant including ID number **AND** account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, DoB, address, and other personal information in records are consistent with the application and sufficient to identify a unique individual. For utility account numbers, confirmation shall be performed by verifying knowledge of recent account activity. (This technique may also be applied to some financial accounts.) Address confirmation: a) CSP issues credentials in a manner that confirms the ability of the applicant to receive mail at a physical address associated with the Applicant in records; or b) If personal information in records includes a telephone number, the CSP issues credentials in a manner that confirms the ability of the Applicant to receive telephone communications at a number associated with the Applicant in records. CSP records the Applicant's voice or using alternative means that establish an equivalent level of non-repudiation.
Level 4	**In-person**	**Remote**
Basis for issuing credentials	In-person appearance and verification of: a) A current primary Government Picture ID that contains Applicant's picture, and either address of record or nationality of record (e.g., driver's license or passport), and; b) Either a second, independent Government ID document that contains current corroborating information (e.g., either address of record or nationality of record), OR verification of a financial account number (e.g., checking account, savings account, loan or credit card) confirmed via records.	Not applicable

RA and CSP actions	*Primary Photo ID:* RA inspects photo ID and verifies via the issuing government agency or through credit bureaus or similar databases. Confirms that: name, DoB, address, and other personal information in record are consistent with the application. Compares picture to Applicant and records ID number. *Secondary Government ID or financial account:* a) RA inspects secondary Government ID and if apparently valid, confirms that the identifying information is consistent with the primary Photo-ID, or; b) RA verifies financial account number supplied by Applicant through record checks or through credit bureaus or similar databases, and confirms that: name, DoB, address, and other personal information in records are on balance consistent with the application and sufficient to identify a unique individual. **(Note: Address of record shall be confirmed through validation of either the primary or secondary ID.)** *Current Biometric: RA* records a current biometric (e.g., photograph or fingerprints) to ensure that Applicant cannot repudiate application. *Credential Issuance:* CSP issues credentials in a manner that confirms address of record.	Not applicable