



P1

P2

P3

P4

P5

P6

P7

P8

P9

T1

T2

T3

T4

T5

T6

T7

M1

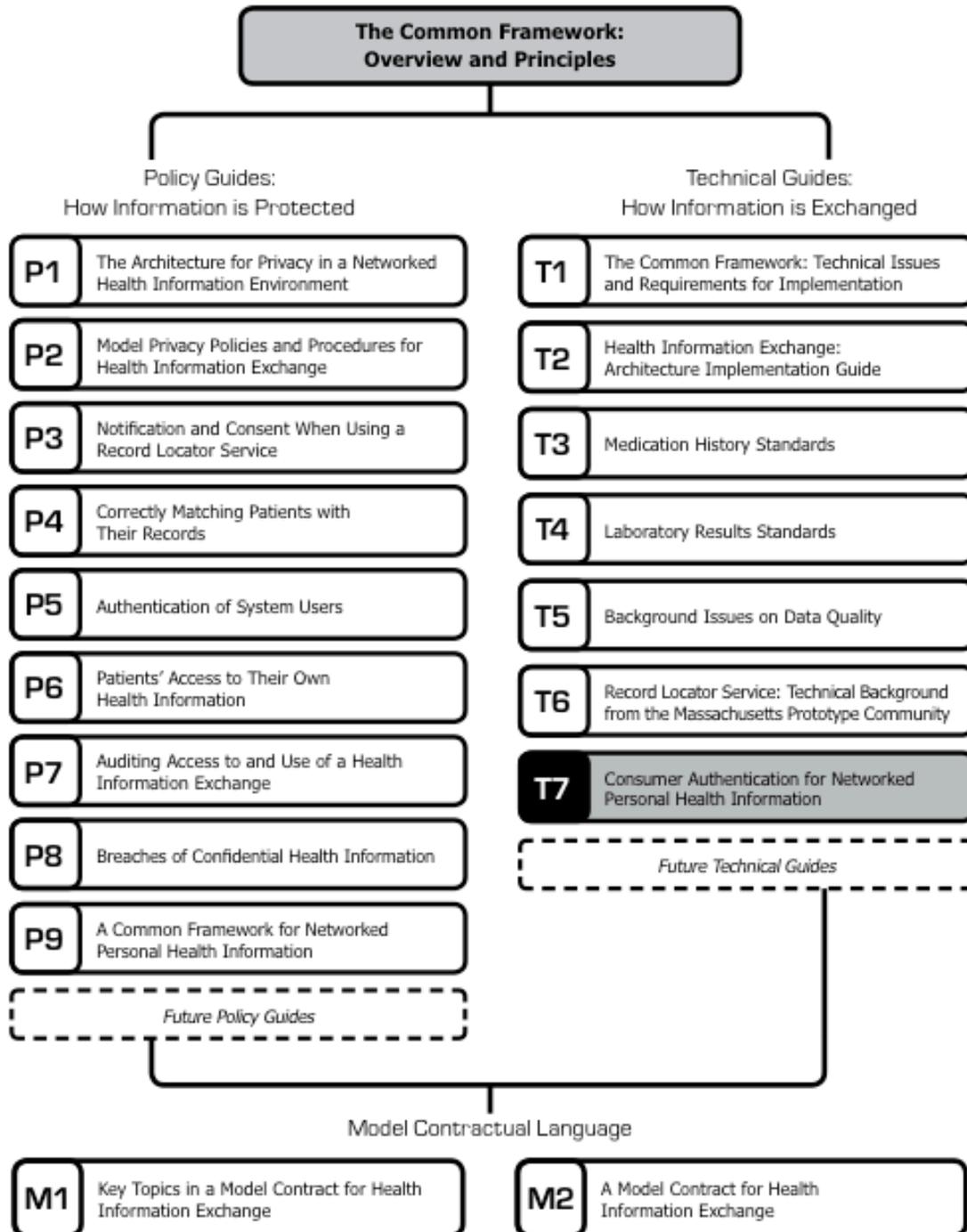
M2

Connecting Americans to their Health Care:

Consumer Authentication
for Networked Personal
Health Information

Connecting Americans to Their Health Care: Consumer Authentication for Networked Personal Health Information

The document you are reading is part of *The **Connecting for Health** Common Framework*, which is available in full and in its most current version at: <http://www.connectingforhealth.org/>. The Common Framework will be revised and expanded over time. As of December 2007, the Common Framework included the following published components:



Connecting Americans to Their Health Care: Consumer Authentication for Networked Personal Health Information*

INTRODUCTION

This paper stems from the **Connecting for Health** document *Connecting Americans to Their Health Care: A Common Framework for Networked Personal Health Information*.¹ The key goal described: Consumers have a choice of trustworthy “networked” personal health records (PHRs) to acquire electronic copies² of their personal health data captured at various points on a network (e.g., doctor’s offices, hospital systems, pharmacies and pharmacy benefit managers, labs, diagnostic imaging services, etc.). Key points include:

- We see a networked environment for PHRs as a foundation for Americans to improve the quality and safety of the care they receive, to communicate better with their health care providers, to manage their own health, and to take care of loved ones.
- To establish a chain of trust, the participating entities must have common understandings and information policy expectations, such as how to authenticate and authorize clinicians to use the network and how to protect sensitive personal information.
- Consumers also need a chain of trust to interconnect across networks. Yet they represent a greater challenge than clinicians for authentication, authorization, liability, and security by virtue of the fact that they do not have organizational or business relationships that can serve as a vehicle for common policies and their enforcement. There is no commonly accepted set of practices today to provide credentials to consumers for health information exchange across different systems and data repositories. It is reasonable to expect that consumer applications could become more easily “networked” if such a set of common practices existed — that is, if some type of enforceable arrangement required all participants to operate under a common set of policies and agreements to mitigate risks such as misidentification or identity theft.

Trust on an electronic network depends on several factors, including assurances to consumers and participating entities that the information they access and share will be kept confidential, i.e., only shared with authorized actors. One key policy for achieving this trust, which is the focus of this paper, is to make sure that consumers are properly authenticated.

This work is the product of the **Connecting for Health** Work Group on Consumer Authentication Policies for Networked Personal Health Information. The Work Group charge

* **Connecting for Health** thanks Clay Shirky of New York University, Josh Lemieux of the Markle Foundation, and Dan Combs, an independent contractor, for drafting this paper. See Appendix A for acknowledgements and the Work Group roster.

¹ Available online at: http://www.connectingforhealth.org/commonframework/docs/P9_NetworkedPHRs.pdf.

² We emphasize the word “copies.” PHR applications may store copies of an individual’s health data along with original information contributed by the consumer. A consumer may control those copies of information stored in her own PHR application. This does not equate to her having a similar level of control over the data about her that is captured and held by health-related organizations, such as clinics, hospitals, pharmacy services, labs, health plans, etc. It is within our scope to find solutions to enable the individual to collect and control copies of health data captured initially by health-related institutions. It is not within our scope or intent to enable individuals to be able to directly alter or delete original data held by health-related institutions, although it is important (and required by HIPAA) for consumers to have clear mechanisms to notify and request corrections of erroneous or incomplete data about them.

stems from the *Connecting Americans to Their Health Care: A Common Framework for Networked Personal Health Information* paper.³ The group was asked to address the specific challenges of authentication. A second Work Group, the **Connecting for Health** Work Group on Consumer Access Policies for Networked Personal Health Information, was also assembled to address critical policies such as privacy, consent, secondary uses, breach notification, etc.

A CRITICAL PROBLEM OF THE DIGITAL AGE

At birth, a baby's hospital nametag is the first of several tokens that society will use to assert "identity" throughout the rest of life. For a child born into this Digital Age, countless electronic transactions will be based on assertions of identity. There is no practical or affordable technology — at least, not yet — to flawlessly identify each person for each transaction. So we use a variety of imperfect tokens (driver's licenses, passports, PINs, passwords, etc.) to validate an individual's claim to a particular identity. And that identity will be created over and over again in electronic systems throughout a person's life.

All business sectors and all individuals are challenged — and to some extent threatened — by this burden of proving identity, and of issuing and using authentication tokens. The increasing scattering of personally identifiable information makes identity management critical for business and consumer activities, yet at the same time problematic, costly, and sometimes risky. In the health care sector today, many important transactions occur daily with little rigor to confirm the identity of individual consumers.

This paper addresses the problem of authenticating consumers in electronic health information exchanges involving PHRs. These include concerns such as the growing public anxiety regarding privacy and security of personal health information, the fear by primary sources of data of increased risk to the information they hold, and loss of provenance of data, resulting from extensive sharing and duplication that could affect the trustworthiness of the system.

Because PHRs store sensitive personal health data, it is critical to develop reliable and trustworthy mechanisms to ascertain the identity of anyone accessing the information. Health information has several characteristics that make it even more sensitive than similar access to bank accounts and lines of credit, because someone who loses money through inappropriate access can be made financially whole. Someone who loses control of sensitive health data, by contrast, can never arrange to have that information returned to a purely private sphere. As part of handling this sensitive data, accurately identifying and authenticating consumers is an important hurdle to be overcome in enabling institutional health data sources to share electronic personal health information with consumer-accessible applications.

This paper offers a framework for processes by which participants in electronic health information networks can be assured that an individual consumer is who she claims to be. The framework includes these four components:

Identity Proofing: This is our umbrella term for the steps by which a person's identity is verified. Specifically, it is the validation of independent evidence and/or credentials of "identity." It happens several times throughout life at various institutions. For example, to receive a driver's license, a person must present required documents in person at a state motor vehicle department.

Identifiers or tokens: Once identity proofing is performed, organizations issue or require users to use tokens or identifiers, which could be physical documents (e.g., driver's license), biological markers (e.g., fingerprint), or be based on knowledge (e.g., passwords), or some combination (e.g., ATM card plus PIN).

³ Available online at: http://www.connectingforhealth.org/commonframework/docs/P9_NetworkedPHRs.pdf.

Ongoing monitoring: After tokens have been issued or identifiers linked to an identity, systems are put in place to establish behavior patterns of individuals and alert authorized parties if behavior changes suspiciously.

Ongoing auditing and enforcement: If an organization relies upon third parties for identity proofing or the issuing of identifiers or tokens, then it must have mechanisms to audit those third parties and redress bad actions.

Note: The word “authentication” is sometimes used as an umbrella term for all of the above components to manage identity in an electronic environment.

BACKGROUND

The **Connecting for Health** Work Group on Consumer Authentication Policies for Networked Personal Health Information focused on the authentication policies for private and secure consumer access to their health information routinely over the Internet to support important aims of consumer empowerment and improved health care quality and safety. Any framework for authentication in this environment must guard against opening up new vulnerabilities at a time in which medical identity theft already is a growing and serious problem.⁴ Our Work Group's recommendations are consistent with principles articulated in the **Connecting for Health Architecture for Privacy in a Networked Health Information Environment**.⁵

See **Appendix A** for the membership of the **Connecting for Health** Work Group on Consumer Authentication Policies for Networked Personal Health Information.

See **Appendix B** for more detail on the scope and charge of this Work Group.

See **Appendix C** for the background and principles of **Connecting for Health**.

See **Appendix D** for a partial list of other groups working on the consumer authentication problem.

We use the following definitions in this paper:

- **Personal Health Records (PHRs):**

PHRs encompass a wide variety of applications that enable people to collect, view, manage, or share their health information or health-related transactions electronically. Although

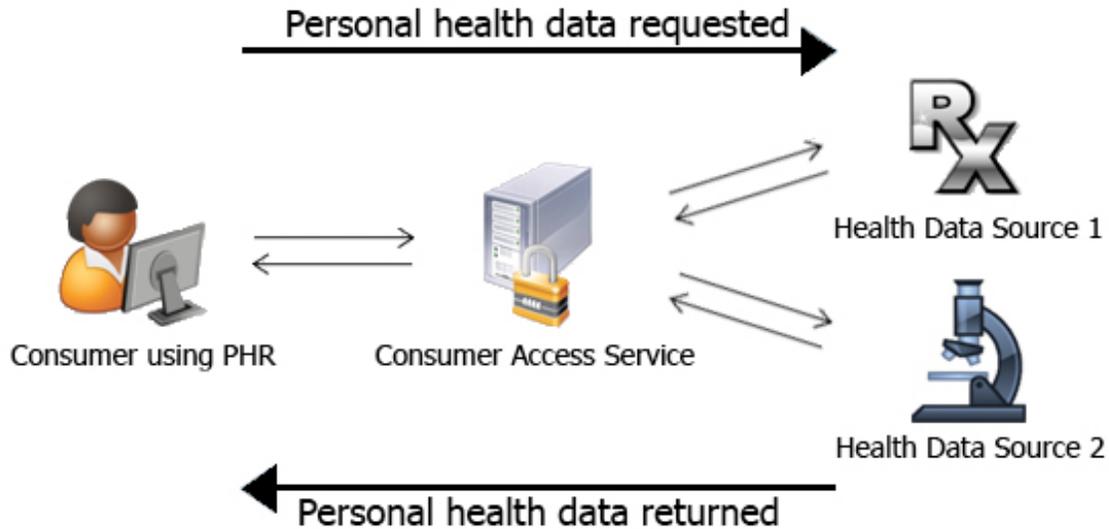
there are many variants, PHRs are intended to facilitate an individual's ability to compile personal health information into an application that the individual (or a designee) controls. PHRs may contain copies of data held by health-related institutions as well as information contributed by the consumer or health monitoring devices. We do not envision PHRs as a substitute for the professional and legal obligation for recordkeeping by health care professionals and entities.

- **Consumer Access Services:** This is a set of functions that enable an individual consumer to securely access copies of their health data from multiple sources in an electronic environment. Consumers may be offered such services by a variety of organizations, ranging from existing health care entities to new entrants. Some will be covered under the Health Insurance Portability and Accountability Act (HIPAA), others will not. Consumer Access Services may combine both authentication services as well as data management services.
- **Health Data Sources:** For the purposes of this paper, a health data source is any entity that serves as custodian of the individual's personal health data. This may include health care providers and clinics, hospitals and health care systems, health insurance plans, clearinghouses, pharmacies and pharmacy benefit managers, laboratory networks, disease management companies, and others that hold data related to the personal health of individuals.

The diagram below depicts a highly simplified data flow. In the center are Consumer Access Services, which include a mechanism to authenticate the individual consumer to the satisfaction of both ends of the exchange. (**Appendix F** contains a more detailed discussion of alternate models for conducting this authentication.)

⁴ *Medical Identity Theft – The Information Crime That Can Kill You*, World Privacy Forum, Spring 2006. Accessed online May 2, 2007 at: http://www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf.

⁵ Available online at: http://www.connectingforhealth.org/commonframework/docs/P1_CFH_Architecture.pdf.



The simplicity of the diagram obscures a few important points about our vision for Consumer Access Services:

First, PHRs (i.e., consumer-facing applications) could be offered by entities at either end of the diagram. For example, an independent technology company (left side of diagram) could supply a PHR, and so could one or both of the health data sources (right side of diagram). The site of the application is not relevant. The aggregation of copies of data that the consumer collects could be stored at either end of the diagram, or by an intermediary. For any of the entities to exchange data, however, there needs to be what we call Consumer Access Services (including authentication and the provision of access to records).

Secondly and similarly, Consumer Access Services may be performed by a third-party intermediary, but they also could be performed by the PHR applications or the Health Data Sources, or both. In fact, the Consumer Access Services and the PHR may be offered by the same entity and therefore indistinguishable to the end user. Our concern is with getting the process of authentication right, without regard to what sort of entity is doing the authenticating.

Third, our recommendations are designed to be compatible with existing networks — health care providers forming electronic health information exchanges, pharmacy networks, or large non-

geographic networks. As the *Networked Personal Health Information* paper points out, there is a great deal of electronically available personal health information in existing databases today. Existing networks (e.g., large scale pharmacy chains, the VA, Kaiser Permanente), Regional Health Information Organizations (RHIOs), or other new services (monitoring devices, disease management programs, etc.) emerging from continued innovation in the PHR space — all may eventually provide multiple avenues for consumers to receive copies of their health data.

Throughout its deliberations, our Work Group was fully cognizant that other issues — revenue models, business relationships and contracts, limitations of liabilities, enforcement mechanisms — are bigger hurdles to PHR development than consumer authentication, which is the narrow focus of this paper.

WORKING PRINCIPLES AND ASSUMPTIONS OF THE WORK GROUP

In addition to the **Connecting for Health** principles (see **Appendix C**), our Work Group agreed to the following guiding principles for solutions to the authentication problem:

Principle 1

Authentication systems should, as a whole, cover as much of the population currently using the U.S. health care sector as possible. Authentication processes that are ineffective or unavailable for particular groups of people (due to disability, expense to the user, lack of available credentials such as driver's licenses, etc.) should be balanced with alternatives appropriate for those groups, to the extent that such alternatives are available.

Principle 2

Consumers should have a choice in Consumer Access Services. Consumers should be entitled to a reasonable expectation of a choice of entities conforming to a published set of authentication standards. It's optimal, when feasible, to let informed consumers play a role in determining their Consumer Access Service provider and authentication stringency level of choice. However, given a widespread lack of consumer awareness about authentication techniques and identity threats, minimum consumer authentication standards for health information should provide relatively high security.

Principle 3

To be both effective and trustworthy, a distributed system of authentication needs oversight, accountability, and mechanisms of redress. The policies of the authentication system should be

transparent. Systems should allow the consumer to understand who has potential access to her data as well as when it has been accessed and by whom, ideally on demand and in real-time.

We prefaced our deliberations by stating that:

- Our recommendations must be reasonably affordable and workable in today's environment.
- Our recommendations must not be tied to existing practices and technologies that may preclude future innovations.
- Our recommendations should not depend on the promise of future innovations in order for organizations to act on them now.
- Our recommendations must not favor any one technology or vendor, or any business model or business relationships.
- Our recommendations must be fully cognizant of any non-proprietary frameworks that are broadly accepted by at least large segments of the health sector.⁶

⁶ On this final point, one key reference point for identity proofing and authentication stringency levels are those adopted by the E-Authentication Federation (EAF) among U.S. government agencies and its private sector companion organization, the E-Authentication Partnership (EAP). The National Institute for Standards and Technology (NIST) created a technical implementation guide for EAF based on industry standard Security Assertion Markup Language (SAML). The policies of the EAF have been licensed to the EAP.

A NEED FOR A NEW APPROACH

Frameworks that address the authentication problem typically do so based on a model of increasing stringency of identity proofing and authentication, corresponding with increased sensitivity of the data being accessed and the related risk. Requirements that are too low or loose create an unacceptable risk of the wrong person getting someone's information, compromising a consumer's accounts, defrauding providers or otherwise engaging in criminal acts. Requirements that are too stringent create unacceptable difficulties for the right person to get to his information, and may erect unacceptable barriers to adoption and implementation.

The development of networked PHRs is in its infancy, so there is no broad ecosystem to observe. Yet the problems of authentication are primarily ecosystem problems. If every organization dealing with a consumer managed its own authentication process from start to finish, there would be no systemic risk, and thus no need for a systemic solution. However, making every organization responsible for every one of its users pushes significant costs onto both the individual (who needs to manage multiple passwords) and the organizations that hold the consumer's data (each of which needs to be able to maintain a proofing and authentication infrastructure.)

A Consumer Access Service with insufficient proofing or authentication standards creates a risk for the security of the consumer's records. It also creates a risk to any clinical organizations and other entities that hold the consumer's data, to the degree that those organizations trust a Consumer Access Service to correctly validate a consumer's identity. If there is a race to the bottom for convenience to the customer, then there may be a high level of abuse (which could in turn inspire a draconian legislative or regulatory post-hoc remedy).

Therefore, it would be helpful to define an acceptable baseline identity proofing and authentication standard to which all

Consumer Access Services should conform. Ideally, the standard would have an understood and generally accepted threshold for reliability, so that new methods for authentication can be evaluated against the effectiveness of existing methods. We aspire to a situation where an affordable and accepted industry standard is based on a measurable reliability of performance. However, as we discuss below, such a standard is not quantifiable today.

Given the constraints of the environment today, we make the following recommendations as an appropriate approach to the four key components of authentication: identity proofing, the issuing of identifiers or tokens, ongoing monitoring, and ongoing auditing and enforcement.

COMPONENT 1: RECOMMENDATIONS FOR IDENTITY PROOFING

The first step — verifying the identity of an individual consumer to an acceptable level of certainty — is typically the most difficult, expensive, and important.

Recommendation 1A: Consider in-person proofing as appropriate in some, but not all, cases: By in-person proofing, we generally mean requiring a face-to-face encounter in which the consumer presents a verified current primary government ID that contains a picture and either address of record or nationality (e.g., driver's license or passport). This option is an acceptable industry practice that is particularly appropriate when the organization performing the identity proofing:

- a. Has no prior relationship with the consumer, and/or,
- b. Has the infrastructure and budget necessary to conduct face-to-face encounters with consumers.

Discussion:

A key presumed advantage of requiring face-to-face identity proofing encounters is that it lowers the risk of mass or automatic attacks to obtain false credentials. In the virtual world, in which people can easily pose as others online, a requirement for in-person proofing has a strong appeal: It seems like the best way to establish a baseline identity of an individual. It raises the presumed commitment of the individual submitting to the proofing process. It raises the cost of a conducting a fraudulent “attack” on an individual identity, and it reduces the likelihood of remote, automated attacks from many sources or on many identities at once. Requiring presentation of commonly used documents (e.g., birth certificates, driver’s licenses, and passports) sets a hurdle for registrants and brings into play a variety of laws that may be useful at a later time for enforcement or prosecution, if necessary.

Caveats:

However, this option comes with three critical caveats:

- First, although dissuading misuse is a key goal for any such system, these same hurdles dissuade legitimate use as well. In-person proofing carries a cost and inconvenience burden for consumers, particularly those who face mobility or transportation barriers. Given the potential utility of providing consumers with electronic access to their health information and services, this outcome is not ideal and risks systematic underuse of PHRs. In-person proofing may be in tension with Principle 1, above, that the authentication process be available to as much of the population as possible.
- Secondly, in-person identity proofing is a significantly costly and labor-intensive process, which many organizations are not well-positioned to perform. If in-person identity proofing were required of all organizations on the network, it would keep organizations that could offer potentially useful data or services from participating. This affects both

large and small organizations. For example, the Centers for Medicare & Medicaid Services (CMS) — the nation’s largest payer — has no direct way currently to conduct face-to-face identity proofing of its beneficiaries. Nor do most technology companies or web portals ever conduct in-person encounters with their customers.

- The third — and most critical — caveat is that, although in-person processes are a widely accepted starting point for identity proofing, we could not find (much less validate) any measurement of their effectiveness. If there were such a measurement (in the manner of “errors per 100,000” or similar), it would enable useful comparisons between various forms of in-person proofing, and between in-person and remote forms of proofing. Our Work Group found a dearth of publicly available research backing up the accuracy of in-person proofing. The assumption that in-person proofing is acceptably accurate is not based on empirical understanding. And certainly, the stringency of methods for in-person proofing varies from one organization to another. In fact, the existence of an in-person proofing process may create a false sense of security if those checking credentials are not well-trained or audited. Recommendations 1B, 1C and 1D below attempt to address this problem.

Approach 1B: Consider ‘bootstrapping’ of in-person proofing by other organizations:

We recommend that entities in the health sector consider “bootstrapping” other in-person encounters by third-parties to establish the consumer’s identity at acceptable levels of accuracy. We recommend that both current and potential holders of clinical data consider partnering with institutions that have effective authentication processes.

Discussion:

For many reasons, individual doctors’ offices are not well-equipped to authenticate 300 million Americans. (Their main authentication procedures relate to

confirming eligibility for health benefits.) However, there are other common places where in-person proofing can occur, including post offices, retail pharmacies, notary publics, and financial institutions. In the bootstrapping model, a laboratory could accept the authenticated identity of a consumer who had first been authenticated by another one of these parties. The entity would pass on the assertion about the patient's identity, along with enough demographic details for the clinical data holder to match the consumer's identity with her records, which could then be returned in any channel that could guarantee delivery. Note that such a system should never re-use existing identifiers. It would be potentially catastrophic, for example, to bind a consumer's PHR directly to a bank account number, as publication of the number would then compromise both categories of data.

This is not a general-purpose solution, as the issues of transparency and liability will have to be worked out as business relationships between the authenticator and the relying party that holds the consumer's health data. However, it would allow new interfaces to be offered to consumers for access to their records, and would do so without creating new proofing hurdles. (These kinds of relationships will probably form as point-to-point business agreements, rather than multilateral networks, at least at first.)

Approach 1C: Consider alternatives to in-person proofing: Because there are no metrics to evaluate the quality of existing proofing systems, the data holder is, de facto, left to judge the acceptability of various methods. We recommend that data sources consider adopting remote proofing on their own, or rely on remote proofing from acceptable third parties (see Component 4 section below), when such proofing methods:

a. Rely on combinations of at least two alternative methods or sources for validating identity that use separate data (i.e., don't use two different

sources relying on Social Security Number or the same account number).

- b. Are optimized to minimize the rate of false positives (i.e., when the wrong person is granted access based on an identity not his own).
- c. Provide an alternative identity-proofing protocol to mitigate false negatives (i.e., when the right person using his correct identity is denied access nonetheless). In such cases, the person denied access in a remote-proofing protocol should be given an alternative means, such as in-person, to establish that he really is who he says he is.
- d. Take precautions to minimize risk to the consumer, including but not limited to:
 - Not requiring consumers to use existing account numbers as identifiers. After the initial proofing step, nothing should be communicated from the consumer to the identity proofer that could provide access to the consumer's account if intercepted by a third party.
 - Securely storing and limiting the number of parties privy to any "shared secrets" to the absolute minimum necessary.
 - Refreshing interrogation questions and "shared secrets" so as to avoid overuse.

This is not meant to be a list but a guide. Security practices change, and the underlying concern should be to adopt practices that create the necessary security while minimizing the privacy risks of the security methods themselves.

Discussion:

Knowing when remote proofing is acceptable suffers from a Catch-22. The obvious threshold for remote proofing should be, at a minimum, "as good as or better than current practice." However, since there are no convincing metrics for current practice, it is impossible to say how any remote proofing system compares. With fake IDs readily available and with harried clerks often doing the checking, in-person

identity proofing does not guarantee that any particular individual is who he claims to be. In some cases it is possible that remote proofing actually works better in defending against a determined attacker than current in-person proofing practices.

There are examples, as with PayPal, where user-proofing is transactional (i.e., based on past or present transactions of information or money that serve to tie a person's identity to a location or service, such as a U.S. Mail box or a bank account), and requires no face-to-face encounter. This method is one of a subset of "Knowledge-based Authentication" (KBA) methods in which a consumer is identified by answering a set of questions only she could reasonably be assumed to know. Sometimes these questions involve historical information (past addresses, use of credit cards for certain transactions) and sometimes they involve information generated as part of the KBA process itself, as with the PayPal technique of generating specific deposits.

The ideal situation would be to measure effectiveness of proofing by a numerical target, such as: "Wrongful issuance of credentials must be kept to an error rate below one in X," where X would be at least a thousand patients. (This metric would be a 99.9% deflection of false positives, in other words.) In the absence of such precision, for either in-person or remote proofing (see 1D, below), the decision about when and how to use remote proofing will necessarily be in the hands of the person responsible for the security of patient data, to be undertaken with two principles in mind: Minimize false positives, and don't rely on a single method.

Our recommendation is that at least two methods or sources be used in remote proofing processes. (For example, the consumer presents authentication credentials issued to him by another institution and successfully responds to an online interrogation about information acquired through his relationship with a separate independent service.) This is because two methods are likely to have different strengths and weaknesses, thus raising the cost of an attack while lowering its chance of success. This is true for both

defense (i.e., it's less likely that a criminal could fraudulently obtain knowledge or credentials in two places than in one) and for sustainability (i.e., if one method becomes compromised, the system would still have at least one untainted method still running, to which it could add new methods without starting from scratch).

Approach 1D: Begin Federal research on identity proofing quality: This is not a recommendation to data holders, but to the federal government. We recommend that the National Institute of Standards and Technology (NIST), in collaboration with other interested agencies, study current identity proofing practice wherever consumers are given access to their records remotely to provide or create metrics expressing the effectiveness of those various methods.

Discussion:

The current administration has made increasing accessibility of electronic health records to providers and citizens a national goal, and the lack of well-understood and generally agreed-to authentication methods for consumers is clearly a hurdle. This recommendation is intended to lead to a benchmark for future proposed systems to meet or exceed, thus moving us out of the current situation of identity proofing ratified by habit, but uninformed by measurement.

Recommendation 1E: Do not use clinical data in the proofing process: As a matter of privacy policy, we recommend against using clinical data as validation data in a proofing process. The reasons for this are articulated in the **Connecting for Health** paper *Linking Health Care Information: Proposed Methods for Improving Care and Protecting Privacy*.⁷

⁷ Available online at: http://www.connectingforhealth.org/assets/reports/linking_report_2_2005.pdf.

COMPONENT 2: RECOMMENDATIONS FOR ISSUING TOKENS OR IDENTIFIERS

Upon successful completion of identity proofing, it is necessary to issue acceptable tokens or identifiers to the consumer.

Recommendation 2A: Bind the consumer's identity in such a way as to facilitate later authentication: At the time of initial proofing, the capture and retention of copies of the documents allows for re-verification if needed at a future time. If in-person visits are used in identity proofing, they present an opportunity to capture a biometric indicator, such as photographs or fingerprints.

Discussion:

This process of connecting or binding of particular information or attributes to a particular physical person, when combined with system monitoring, can provide improved ability to discover certain types of fraud attempts in which attributes are used by multiple registrants. However, it is important to note that improved information collection, of any sort, also raises the requirements for securing the database where the records are stored. Improvements in knowledge-based authentication methods generate, as an inevitable side effect, more stored knowledge about the consumer — knowledge that must be held securely to prevent near-term defeat of the authentication system itself and to prevent identity theft. Although database security is not in the scope of this paper, we note that care must be taken to evaluate the security of the data held in aggregate, as well as the security of person-by-person authentication.

Less reliable, although at times more economically practical, are password reminders as “shared secrets” that can be used to support later authentication, or

password reset requests. A common example is for the consumer to be forced to answer questions such as pet names or mother's maiden name. Care must be taken that these not be based on common questions that can be easily guessed or snooped. Another possible source of shared secrets are questions the service asks of the consumer. For example, PayPal makes two small deposits in a new user's account, then asks that the user report those amounts back to PayPal. This removes the risk of trivial guessability, though it requires a higher degree of integration with the financial system.

Interesting work is being done on “zero-knowledge” authentication systems, which reduce or eliminate the need for knowledge-based secrets to be held by the authenticating party. In a zero-knowledge system, the consumer proves who he is by using a secret that only he knows to perform a task that he could only perform with that secret. (Imagine that you see someone unlock a door that you know can open with only one key. You could conclude that the person has that particular key without you needing to see a copy of the key yourself.) “Zero-knowledge”-based systems have not yet been widely deployed, and have significant management issues in their current implementations. Still, they should be watched closely, as they may provide a way to increase authentication security without also increasing the privacy risk to consumers that comes with knowledge being held about them in various authentication databases.

Recommendation 2B: Choose an appropriate token or identifier: There are a variety of credentials available. PINs, cards, tokens, fobs with RF chips, antennas, and fingerprints are a few examples of a rapidly growing array of tokens.

Discussion:

Many different types of tokens or identifiers can be used to good effect in authentication processes. Much depends on the budget and infrastructure of the token-issuer and the tolerance of consumers to remember and use the token appropriately.

Recommendation 2C: If using passwords as tokens, enforce 'strong' passwords: Requiring and enforcing rules to create strong passwords⁸ — i.e., passwords that are not easily guessable — is one of the first relatively easy steps that will dramatically increase the security of the username and password token.

Discussion:

The username and password combination is the most commonly used token. Extremely valuable and potentially risky transactions are conducted millions of times each day employing the protection of username and password. Many of the tokens and identifiers listed in Recommendation 2B are essentially variations on the concept of username and password, incorporating a variety of technologies to improve on the basic concept. Used appropriately, the username and password combination provides significant protection at very moderate cost and user inconvenience. However, if unguided by a set of guidelines or password requirements, many consumers tend to create easily guessable passwords and

otherwise create the opportunities for compromise of their identity.

Many systems now prevent the use of dictionary terms as passwords, or consecutive or repeating strings of numbers or letters or other easily guessable phrases. Some require the use of at least one number, a letter and another keyboard character. Some systems will provide a rating of the strength of the password as it is created by the user. The fundamental challenge with strong password requirements is that they not only make it harder for illegitimate users to guess a password, they can make it harder for the legitimate user to remember it. If strong password requirements are too onerous, they may encourage legitimate users to compensate through insecure practices, such as writing down a password and leaving it next to an unattended computer.

It is increasingly common to supplement the username and password combination with monitoring of the requesting machine (e.g., source IP address, machine and browser characteristics). Such monitoring, which we discuss further below, requires no additional issuing of tokens to the user.

Recommendation 2D: Limit attempts on passwords:

Given sufficient time, access, and attempts, any password will eventually succumb to attempts to guess it. Limiting the number of consecutive and total attempts to enter a password, requiring periodic changes to the password, and other relatively low-cost, relatively low-inconvenience requirements for use of passwords make password guessing an unacceptably difficult approach to compromising tokens.

Recommendation 2E: Establish a clear policy on requirements for password changes:

Although an inconvenience to end users, it may be reasonable to require consumers to create new passwords at regular intervals. Each system should decide locally whether to enforce a policy requiring that consumers change their passwords over time. However, if such policies are enforced, it's critical that consumers be given clear

⁸ The following documents contain useful information about the issuing of tokens, including strong passwords:

NIST Special Publication 800-63: Appendix A- Estimating Password Strength and Entropy, pp. 46-53. Table A-1: Estimated Password Guessing Entropy in bits vs. Password Length, p. 53. Accessed online May 3, 2007, at: http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf.

Password Strength, Wikipedia. Available at: http://en.wikipedia.org/w/index.php?title>Password_strength&oldid=154706929.

National Institutes for Health, Password Policy for eRA. Accessed online May 3, 2007, at: http://era.nih.gov/docs/NIH_eRA_Password_Policy.pdf.

NIST Special Publication 800-12: Chapter Sixteen - An Introduction to Computer Security - The NIST Handbook: Identification and Authentication. Accessed online May 3, 2007, at: <http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/chapter16-printable.html>.

explanations on the methods and reasons for resetting their passwords.

Discussion:

The value of tokens can diminish over time. For example, many private and government organizations still use Social Security numbers not only as identifiers but also as tokens⁹, and it is precisely because of this ubiquity of uses that Social Security numbers have been a boon to identity thieves. Similarly, if a consumer uses the same password and password reminder at every site visited, it is much less secure than if the consumer uses different secret codes at each site's login. On the other hand, consumers may have trouble coming up with strong passwords that they can remember, and the burden of having to do so frequently could drive down utilization. The value of forcing consumers to change passwords is hotly debated, and our work group did not feel strongly about making a recommendation one way or the other.

⁹ The principal reason Social Security Numbers (SSNs) should not be used as tokens is that, if this approach is taken, then one number is used to provide the public and secret parts of authentication (i.e., you have an SSN that points uniquely to you, but you must reveal it as proof that you have it.) Without being accompanied by a second, secret token such as a PIN, the SSN is damaged in regard to authentication by the very use that makes it otherwise worthwhile. In addition, no one token should be relied on too heavily, as such ubiquitous use will increase the focus of malevolent actors on compromising that token, and any compromising of such a token will have disproportionately negative effects.

COMPONENT 3: RECOMMENDATIONS FOR ONGOING MONITORING

It is important to perform periodic or ongoing processes to continually improve upon the initial proofing and to weed out compromised identities.

Recommendation 3A: Conduct appropriate ongoing monitoring:

Ongoing monitoring is an essential third component of appropriate authentication because of inherent weaknesses in the first two components (i.e., identity proofing and issuing of tokens). Given the widespread compromise of documents used for initial identity proofing and the large and growing incidence of identity crimes, the function of authentication should be thought of as an ongoing process rather than a gateway to be passed through one time. Once the consumer's identity is proofed and the token is issued, systems should establish the behavior patterns of individuals and alert authorized parties when behavior falls out of the established pattern. For example, credit card companies have algorithms to detect sudden changes in charging behavior, triggering a telephone call to the consumer to investigate possible fraud.

Discussion:

Identity proofing is often used as a "gateway" process. It is merely a perimeter defense, performed once and not revisited. Once identity proofing is completed, a registrant is an "insider" of the system. And there is often much secondary reliance on this initial proofing, such as airport security relying on a state-issued driver's license. In the Digital Age, the outside/inside relationships change continually. Allowing network access to partners, customers, users, and some unintended participants quickly renders perimeter defenses insufficient. Additionally, much of the fraud and abuse comes from people accurately identified or from identities that were compromised after the initial proofing process, as well as from "inside" authorized users.

There is a robust and active population that continually probes and prods for opportunities to compromise systems and almost immediately shares with others any new intelligence gained. The risks and threats to systems change continuously. The practices and processes to respond to these threats must likewise change.

The automated ability to monitor individual behavior for fraud varies significantly from organization to organization, depending in part on the type of organization, what data it captures, and what it is permitted to do with the data. Valuable techniques include analysis of transaction history and location, keystroke patterns, and others. Detailed recommendations would rapidly become dated and ineffective. Decisions about an ongoing monitoring process must be made locally. The U.S. government provides some guidance for ongoing monitoring as an integral part of an authentication process in the *NIST Special Publication 800-100, Information Security Handbook: A Guide for Managers*.¹⁰

Behavior pattern monitoring can include information about the method of login (e.g., consumer's usual IP address, machine and browser type, etc.), or information about the types of resources or data that the consumer typically accesses.

Recommendation 3B: Enable consumers to view an immutable audit trail: Consumers can become powerful allies in detecting identity fraud when they have access to the transaction history of their accounts. We recommend that Consumer Access Services and PHR offerers provide authenticated consumers with online access to an immutable audit log displaying all accesses and data transactions involving their account.

Discussion:

¹⁰ *NIST Special Publication 800-100 - Information Security Handbook: A Guide for Managers*, pp. 14-15. Accessed online May 3, 2007, at: <http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf>.

Consumers now are able to review their own credit reports online, providing an important and highly invested check on potential fraud or errors. This recommendation is in keeping with Principle No. 3 of this document. The **Connecting for Health** Common Framework document, *Auditing Access to and Use of Health Information Exchange*, provides some guidance in this area of immutable audit.¹¹

¹¹ Available online at:
http://www.connectingforhealth.org/commonframework/docs/P7_Auditing_Access.pdf.

COMPONENT 4: RECOMMENDATIONS FOR EXTERNAL AUDIT AND ENFORCEMENT

When relying on a third party to perform proofing or issuing of tokens, or both, some mechanism of audit and redress is essential to establishing a chain of trust.

Recommendation 4A: Ensure that third parties are “observable” in how and how well they are performing identity proofing, token-issuing, and ongoing monitoring or any related services to authenticate consumers. One recommended practice is to have a contractual commitment for the parties to notify each other if either detects system compromise above a certain threshold or fails to comply with agreed procedures.

Discussion:

A fundamental premise of the *Common Framework for Networked Personal Health Information* paper is that Consumer Access Services will emerge to help consumers “network” their PHRs with connections to multiple sources of health data and services. In order to facilitate the consumer’s requests for digital copies of his information from Health Data Sources, all parties must be assured of the individual’s identity and bona fide authorization to share data. Simply put, such transactions require “trust.”

It will be impossible to trust and rely on any third-party’s authentication if those third-parties’ practices are not observable either directly among contracted parties or via some industry-accepted auditing and validation mechanism.

Recommendation 4B: Ensure a mechanism for enforcement and redress for bad actions: There needs to be a commonly accepted mechanism, agreed upon in advance, to redress unacceptable practices and eject bad actors.

Discussion:

Audit, enforcement, and redress are general issues for Consumer Access

Services, not just with the task of authentication. All this is framed against the larger issues of binding Consumer Access Services to policies and accountability generally, and against the general fragmentation of the health care industry (a fragmentation that may increase as Consumer Access Services enter the picture).

Recommendation 4C: Consider federation and/or other contractual means to address Recommendations 4A and 4B:

If the Health Data Source is considering a request from a third party (e.g., a Consumer Access Service) to pass information into the consumer’s possession, then we recommend that:

- The Consumer Access Service must be contractually bound to a group that sets and enforces shared policies, such as the E-Authentication Federation (EAF), Electronic Authentication Partnership (EAP), or similar.
- The Consumer Access Service must use at least Level 2 identity proofing as defined by EAF and adequate tokens (i.e., strong passwords, or tokens at EAF Level 2).

These recommendations are worded as a requirement on the Health Data Source, but apply equally to the Consumer Access Service.

We believe the EAF/EAP is a good framework for a discussion on finding an acceptable degree of authentication certainty and policy enforcement. Although some organizations might choose to join the EAF or the EAP, there is likely no one-size-fits-all answer. Different business relationships and different consumer populations will likely require a variety of authentication services for their transactions. Some consumers may even demand higher-level authentication stringency for certain services.

Discussion:

We emphasize that the above scenario is not the only way to approach the problem. (See **Appendix G** for a draft

architecture discussion.) Point-to-point trust is conceptually simplest from the point of view of any given pair of actors, but pairwise trust exposes the system as a whole to daunting complexity. Similarly, a single national actor coordinating trust on behalf of everyone is not feasible at this time, both because of the realities of fragmentation and the business context, and also because the policing problem for a single actor is acute. If these two extremes are in fact impractical, this suggests some sort of chain of trust with mutual policing, with various actors monitoring one another, possibly in contractually arranged groups.

In the absence of a federation, the following are among the most important demands that a typical health data source will make of a Consumer Access Service asserting the identity and a data request on behalf of an individual consumer:

- An authorization from the consumer to share data with the Consumer Access Service.
- A HIPAA covered entity-business associate agreement or contract with similar terms.
- A significant measure of accountability, including immutable audit logs and external audits.
- A contractual commitment to a policy of timely notification and recourse in the event of inappropriate access or breaches of personal health information.
- A cap on the Health Data Source's liability stemming from the health data exchange.

CONCLUSION: A PATH FORWARD

This paper is driven by a desire to allow U.S. consumers to access and gain value from their own health information. **Connecting for Health** accepts that much of our valuable personal health data is stored and managed by numerous entities. The next key challenge is to establish the rules and techniques that establish trust among participants over a “network of networks.”

Policy rules will be needed in a number of areas — including patient consent, secondary use, and data management. Identity has quickly emerged as a primary problem in network access — particularly given the sensitivity of personal health information. A well-understood and implemented Common Framework for managing health consumers’ identity is a prerequisite to networked use of personal health records.

The recommendations in this paper are based on the technologies and practices current at a particular moment, and our desire to stimulate national progress in addressing this particular obstacle to consumers’ electronic access to their health information.

The problems of identity proofing and authentication are widely felt by all industries handling sensitive data or electronic transactions, and as a result, there is rapid evolution in the tools available for authentication. Any process of authentication for consumer access anywhere in health care must be regularly re-evaluated to factor in both new threats and new capabilities.

Many health care entities have significant interest in some form of networked personal health records. The relationships they forge could have significant impact on possible trust scenarios for consumer authentication. In addition, there is a critical need to expand consumer education about techniques to safeguard identity in the Information Age. Consumers should understand, first, that there are tradeoffs between security and convenience

and, second, what the tradeoffs mean for them.

These many trends — new threats, new business relationships, emerging technologies, and consumer awareness and behavior — all warrant close monitoring. They certainly will have more impact on future health information sharing environments than the modest recommendations in this paper. We do, however, hope that this paper contributes to a growing consensus that the path forward on consumer authentication requires careful thinking, new research, and innovative approaches.

APPENDIX A: ACKNOWLEDGEMENTS

Connecting for Health thanks the following Work Group members for participating in the rich discussion that resulted in this paper.

Chair

Clay Shirky, New York University Graduate Interactive Telecommunications Program

Mark Johnson, Vanderbilt University and Medical Center

Work Group

Paula Arcioni*, New Jersey Office of Information Technology

Jennifer Kerber, Information Technology Association of America

Ernie Argetsinger, Omnimedix Institute

Kristy LaLonde*, Office of E-Government, Information Policy, and Technology
U.S. Office of Management and Budget

Siddharth Bajaj, VeriSign, Inc.

David Lansky, PhD, Markle Foundation

Dan Combs, Global Identity Solutions, LLC

J.P. Little, RxHub, LLC

Jeremy Coote, InterComponentWare, Inc.

Kathleen Mahan, MBA, SureScripts

Maureen Costello, Ingenix

Georgia Marsh*, United States General Services Administration, E-Authentication Initiative (former position)

Phillip D'Angio, VeriSign, Inc.

Phil Marshall, MD, MPH, WebMD Health

James Dempsey, JD, Center for Democracy and Technology

Daniel Matthews, Lockheed Martin Corporation

Carol Diamond, MD, MPH, Markle Foundation

Damon Miller, CapMed Corporation, A Division of Bio-Imaging Technologies, Inc.

Martin Fisher, MedicAlert Foundation International

Kim Nazi, FACHE*, United States Department of Veterans Affairs

Thomas Foth, Pitney Bowes, Inc.

Alison Rein**, AcademyHealth

Christopher Gervais, Partners Community HealthCare, Inc.

Eric Sachs, Google Health

Mark Gingrich, MS, RxHub, LLC

Charles Safran, MD, Harvard Medical School

Janlori Goldman, JD, Health Privacy Project

Scott Schumacher, PhD, Initiate Systems, Inc.

Philip Hagen, MD, Mayo Clinic

Jonathan Hare, Resilient

Donald Simborg, MD, Independent Consultant

Elizabeth Holland*, Centers for Medicare & Medicaid Services

Michael Simko, RPH, Walgreens Pharmacy Services

Michael Stokes, Microsoft Corporation

David Temoshok*, General Services Administration, Office of Governmentwide Policy

Robert Tennant, MA, Medical Group Management Association

Jeanette Thornton, MPA, America's Health Insurance Plans

Allison Viola, American Health Information Management Association

David Yakimischak, SureScripts

*Federal and state employees participated in the Work Group but make no endorsement.

**Participated in Work Group but makes no endorsement per employer policy.

The **Connecting for Health** Work Group on Consumer Authentication Policies for Networked Personal Health Information wishes to thank **Josh Lemieux** for his expertise and tireless help preparing this manuscript. In addition, we thank **Clay Shirky** for his leadership and work on this manuscript. Without his unique ability to parse very complex issues carefully and adeptly, we could not have achieved this paper. We also thank **Dan Combs** and **Stefaan Verhulst** for their help researching and drafting portions of this document.

APPENDIX B: SCOPE AND CHARGE OF THE WORK GROUP

The Work Group on Consumer Authentication and Health Information Exchange was charged with defining a framework to authenticate the identity of individual consumers consistent with **Connecting for Health** principles. This includes identifying a baseline of policies and technologies to assert, within acceptable thresholds of accuracy, the identity of an individual consumer requesting copies of her personal data in an electronically networked health information environment. The recommendations are intended to encourage a fresh approach to foster trust of all network participants, and specifically to protect the consumer, the health data holders, and the Consumer Access Services from the following threats:

- **Defense against illegitimate access to health records:** This is defined in this paper as externally targeted or automated attacks to gain access into an individual's health information. The attackers in this scenario could be either known to the consumer (as with a relative or colleague looking at material inappropriately), a targeted attack by someone not known to the patient (as with a private detective trying to access records), or an indiscriminate attack (someone looking for anyone's health records, possibly as a precursor to medical fraud).
- **Defense against identity theft:** The threat here is not to the clinical data per se, but to the consumer's identifiers and demographics — address, date of birth, Social Security Number, health benefit eligibility number, etc. Protecting against identity theft is an obvious goal. The key complication here is that it is very difficult to protect against family members posing as one another, and it is not possible to design a system that covers all state regulations of parental access to their children's data. Our Work Group did not focus on proxy access beyond the key principle that the identity of all proxies accessing the system be recorded,

as well as the identities of people for whom they are proxies, so that, should a proxy later lose access, their authentication tokens can be revoked separately from the main account.

The following issues fell outside of the scope of this Work Group, but we list them here to acknowledge their importance in creating a trusted health information sharing environment for consumers:

Consumer Issues:

- **Consumer Behavior:** We are not addressing what consumers do with their copies of personal health data. We live in an age in which individuals are increasingly self-publishing on the Internet intimate details of their personal lives. It was outside the scope of this Work Group to attempt to address the complexities of individual behavior and choice. Nevertheless, these are relevant concepts. Consumers' own experiences and individual preferences will no doubt shape this emerging area.
- **Phishing:** There is a parallel problem to consumer authentication, related to the assurances provided by the entity hosting the consumer's data. Mechanisms need to be in place to defend the consumer against "phishing" attacks, where a consumer is directed to log into a seemingly legitimate web site or service, but which is really a copy of an existing site, with a similar URL. The risk of such phishing in medical contexts is high; however, the defenses against the phishing problem require a different set of strategies than those outlined in this document.

Data Storage Issues:

- **Data Security:** Methods to encrypt and secure health data repositories are beyond the scope of this paper. We focus on defense against unauthorized users defeating authentication systems, not attacks on larger data stores. For purposes of this paper, we accept as a precondition that all actors have good physical security

practices. The digital signing of records is also outside the scope of this paper.

- **Data Policies:** Also out of scope of this paper are policies for data custodianship and data sharing other than those related to identity proofing and authentication. The parallel **Connecting for Health** Work Group on Consumer Access Policies for Networked Personal Health Information is working on recommendations for privacy policy, disclosure and consent, secondary use, etc. For purposes of this paper, we accept as a precondition that the consumer has voluntarily initiated a PHR account and authorized all uses and exchanges of personal health data consistent with **Connecting for Health** principles for privacy.¹²

Business Issues:

- **Business relationships:** This paper does not address the necessary business relationships that would provide motivations for health data sources and PHR services to share data on the consumer's behalf, or for intermediaries to emerge between them.

In summary, this paper focuses on a framework for the authentication process when the individual wants to access or contribute personal health information electronically among health professionals or other health-related entities (HIPAA-covered or not).

¹² Available online at:
http://www.connectingforhealth.org/commonframework/docs/P1_CFH_Architecture.pdf.

APPENDIX C: BACKGROUND ON CONNECTING FOR HEALTH

Connecting for Health, founded and operated by the Markle Foundation, with additional support over the years from the Robert Wood Johnson Foundation, is a public-private collaborative organization with representatives from more than 100 organizations across the spectrum of health care stakeholders. Its purpose is to catalyze the widespread changes necessary to realize the full benefits of health information technology (HIT), while protecting patient privacy and the security of personal health information. **Connecting for Health** is continuing to tackle the key challenges to creating a networked health information environment that enables secure and private information sharing when and where it's needed to improve health and health care.

Connecting for Health has produced the following documents that lay the groundwork for this current work product focused on consumer authentication:

- **Linking Health Care Information: Proposed Methods for Improving Care and Protecting Privacy** (February 2005) — which describes an approach to matching patient records among disparate health care institutions.¹³
- **Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange** (April 2006) — which elaborates and defines a set of policy and technical elements necessary to enable secure exchange of health records among providers across the Internet, including a set of principles for privacy and fair information practices in a networked environment. The **Connecting for Health** Common Framework is composed of nine policy documents on topics such as privacy, notification, audit, and authentication of non-consumer users of the network, and six technical documents that elaborate technical

specifications of a network approach based on those policies.¹⁴

- **The Architecture for Privacy in a Networked Health Information Environment** (April 2006) — which describes a set of fair information practices that the Common Framework has endorsed to guide systems that support the exchange of personal health information. These principles are:
 - **Openness and transparency:** Consumers should be able to know what information exists about them, the purpose of its use, who can access and use it, and where it resides. They should also be informed about policies and laws designed to ensure transparency on how privacy is assured.
 - **Purpose specification and minimization:** The purposes for which personal data are collected should be specified at the time of collection, and the subsequent use should be limited to those purposes or others that are specified on each occasion of change of purpose.
 - **Collection limitation:** Personal health information should only be collected for specified purposes and should be obtained by lawful and fair means. Where possible, consumers should have the knowledge of or provide consent for collection of their personal health information.
 - **Use limitation:** Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified.
 - **Individual participation and control:** Consumers should be able to control access to their personal information. They should know who is storing what information on them, and how that information is being used. They should also be able to review the way their information is being used or stored.

¹³ Available online at: http://www.connectingforhealth.org/assets/reports/linking_report_2_2005.pdf.

¹⁴ Available online at: <http://www.connectingforhealth.org/commonframework/index.html>.

- **Data quality and integrity:** All personal data collected should be relevant to the purposes for which they are to be used and should be accurate, complete, and current.
 - **Security safeguards and controls:** Personal data should be protected by reasonable safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure.
 - **Accountability and oversight:** Entities in control of personal health information must be held accountable for implementing these principles.
 - **Remedies:** Legal and financial remedies must exist to address any security breaches or privacy violations.
-
- ***Connecting Americans to Their Health Care: A Common Framework for Networked Personal Health Information*** (December 2006) — which envisions a consumer-accessible data stream, consisting of electronic copies of personal health data that have been captured at various points on a network (e.g., doctor’s offices, hospital systems, pharmacies and pharmacy benefit managers, labs, diagnostic imaging services, etc.).¹⁵

¹⁵ Available online at:
http://www.connectingforhealth.org/commonframework/docs/P9_NetworkedPHRs.pdf.

APPENDIX D: OTHER GROUPS WORKING ON AUTHENTICATION

The following paragraphs list several authentication projects that currently exist. This list is based on input from Authentication Work Group members and is not comprehensive.

Electronic Authentication Partnership (EAP)

Building off the work of the E-Authentication Federation (see below) and other authentication federations, EAP has developed as a "multi-industry partnership working on the vital task of enabling interoperability for electronic authentication among public and private sector organizations." It is sort of a federation of federations. This group is creating a framework for accrediting and compliance testing of participating Credential Service Providers (CSPs) and Relying Parties (RPs). EAP also addresses the issue of liability.

See: <http://eapartnership.org/>

See Trust Framework web site: http://www.eapartnership.org/docs/Trust_Framework_010605_final.pdf

E-Authentication Federation

The E-Authentication E-Government Initiative is one of the President's 24 cross-agency E-Government Initiatives. Its mission is to put in place the necessary infrastructure to support common, unified processes and systems for government-wide use. E-Authentication recently launched the E-Authentication Federation (EAF), "a public-private partnership that enables citizens, businesses, and government employees to access online government services using log-in IDs issued by trusted third parties, both within and outside the government." Currently 13 different agency web applications are using the service. EAF has focused on the creation of policies, systems, and relationships that reuse existing credentials to meet the needs of mostly federal government-relying parties. EAF has created a framework by which a variety of Credential Service Providers — currently including federal, state, and private sector

organizations — issue credentials to be trusted by Relying Parties in the federal government.

(Quotations taken from E-Authentication web site: <http://www.cio.gov/eauthentication/>)

Privacy:

<http://www.cio.gov/eauthentication/documents/EAPrivacy.htm>

E-Authentication Guidance for Federal Agencies (M-04-04):

<http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>

NIST 800-63: E-Authentication Technical Guidelines:

http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

NIST 800-53: Recommended Security Controls for Federal Information Systems

<http://csrc.nist.gov/publications/drafts/draft-SP800-53.pdf>

Liberty Alliance Project

In 2001, a consortium of 30 organizations formed the Liberty Alliance Project. The project's stated mission is: "to establish an open standard for federated network identity through open technical specifications." Over the past few years, they have published an "open framework for deploying and managing a variety of identity-enabled Web Services." Liberty Alliance is currently working on a framework for "deploying and managing interoperable strong authentication."

Liberty Alliance is a standards group. Liberty Alliance is represented on the EAP and involved either directly, or through efforts of members and the products and services they provide, with the other efforts.

(Quotations taken from Liberty Alliance Project web site: <http://www.projectliberty.org/>)

eC3

eC3 is an alliance of state and local governmental associations. Their mission is to advance the use of electronic commerce by governmental organizations. As part of this

mission, they have published several white papers concerning identity management.

See: <http://www.ec3.org/index.htm>

SAFE-Biopharma Association

This identity management organization maintains and enforces the SAFE framework, which permits bio-pharmaceutical companies to digitally sign business-to-business and business-to-regulator transactions.

SAFE is a successfully operating federation which has solved a number of important cross-boundary issues including those of private-public sector and international boundaries. Based in the health industry, it is familiar with health issues and familiar to current industry participants. Representatives of SAFE participate in EAP.

See: <http://www.safe-biopharma.org/>

HSPD-12 / FIPS 201 / PIV

On August 17, 2004, President Bush issued Homeland Security Presidential Directive - 12 (HSPD-12). This directive called for a common identification standard for all federal employees and contractors. Given this directive, the National Institutes for Standards and Technology developed the Federal Information Processing Standards Publication 201 (FIPS 201), entitled Personal Identity Verification of Federal Employees and Contractors (PIV). This project will provide credentials to 10 to 12 million people at a relatively high level of verification and authentication and could be rolled out to many others through various extensions.

See: <http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html>

See Personal Identity Verification web site: <http://csrc.nist.gov/piv-program/index.html>

Real ID Act

The Real ID Act was passed in 2005 by Congress. The Act is intended to deter terrorism. Among other things, the law states that after May 11, 2008, no Federal agency may accept, for official purposes, a state driver's license as

proof of identity unless that state's driver's license meets certain requirements defined by the Real ID Act. There is a debate as to whether the Act creates a national ID. The debate aside, unless the law is repealed, it will likely have a significant impact on how individuals in America manage their identities.

Real ID requires issuance of a machine readable credential based upon enhanced identity verification as well as improved security practice and technology. Many people are working diligently to ensure that it becomes a widely usable component of an identity infrastructure. There will likely be many different ways to use the Real ID credentials as functions are built to extend the systems or use of the credentials and as States and/or the Federal Government extend the infrastructure. It is possible that one or more States could choose to issue further electronic credentials, PIN's, passwords, PKI certificates, etc., in conjunction with Real ID and/or join EAF or EAP to provide a channel for citizens to use the credentials across a broader range of our society.

Shibboleth

According to its web site, Shibboleth is "standards-based, open source middleware software which provides Web Single SignOn (SSO) across or within organizational boundaries." As part of the Internet2 project, Shibboleth "is developing architectures, policy structures, practical technologies, and an open source implementation to support inter-institutional sharing of web resources subject to access controls. In addition, Shibboleth will develop a policy framework that will allow inter-operation within the higher education community." The Shibboleth federation approach is being widely adopted in this country by educational institutions and internationally by government and private sector organizations. It is working to align its policies and practices to allow interoperability with EAF, EAP and others. Examples of initiatives that have adopted Shibboleth technology include: InCommon, EduCause, and LionShare. InCommon has set up InQueue as a learning environment for participating organizations.

See: <http://shibboleth.internet2.edu/>

Bylaws:

http://www.incommonfederation.org/docs/policies/InC_SCbylaws.html

Participant Operational Practices:

<http://www.incommonfederation.org/docs/policies/incommonpop.html>

Federation Operating Practices and Procedures:

<http://www.incommonfederation.org/docs/policies/incommonfopp.html>

Trust Service (WebTrust/SysTrust)

The American Institute of Certified Public Accountants initiated the WebTrust/SysTrust project. The AICPA's Trust Services are defined as "a set of professional assurance and advisory services based on a common framework (i.e., a core set of principles and criteria) to address the risks and opportunities of IT." Essentially, the project enables CPAs to offer a new service to clients: evaluating web sites that involve data transmission (e.g., personal information such as credit card numbers, birth date, health information, etc.). Web sites that meet the WebTrust/SysTrust requirements can post a "seal of approval" logo on their web sites.

See: <http://www.webtrust.org/>

JA-SIG Central Authentication Service (CAS)

CAS is a single sign on service offered by JA-SIG (Java Architectures). It is an open protocol that appears to be used primarily by the academic community. (It was originally created at Yale University.)

See: <http://www.ja-sig.org/products/cas/>

OATH

As described on its web site, OATH is "an industry-wide collaboration to develop an open reference architecture by leveraging existing open standards for the universal adoption of strong authentication." Its vision is to provide "a reference architecture for universal strong authentication across all users and all devices over all networks."

See: <http://www.openauthentication.org/>

American Health Information Community (AHIC) Confidentiality, Privacy & Security Work Group

The American Health Information Community (AHIC), a health IT advisory panel of the U.S. Department of Health and Human Services, in May 2006 established a cross-cutting work group on confidentiality, privacy and security. The Work Group's charge is to "make actionable confidentiality, privacy, and security recommendations to the Community on specific policies that best balance the needs between appropriate information protection and access to support, and accelerate the implementation of the consumer empowerment, chronic care, and electronic health record related breakthroughs."

See:

<http://www.hhs.gov/healthit/ahic/confidentiality>

Healthcare Information Technology Standards Panel (HITSP)

HITSP will assist in the development of the U.S. Nationwide Health Information Network (NHIN) by selecting standards and publishing specifications to support use cases developed by AHIC and the Office of the National Coordinator for Health Information Technology (ONC). The Panel is sponsored by the American National Standards Institute (ANSI) in cooperation with strategic partners such as the Healthcare Information and Management Systems Society (HIMSS), the Advanced Technology Institute (ATI), and Booz Allen Hamilton.

See: <http://www.hitsp.org>

Center for Democracy and Technology (CDT)

In March 2007, the Center for Democracy and Technology released draft principles for identity in the Digital Age.

See:

<http://www.cdt.org/security/20070327idprinciples.pdf>

PCI Security Standards Council

The PCI Security Standards Council is an open global forum for the ongoing development, enhancement, storage, dissemination, and

implementation of security standards for account data protection. The PCI Security Standards Council's mission is to enhance payment account data security by fostering broad adoption of the PCI Security Standards. The organization was founded by American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International.

See: <https://www.pcisecuritystandards.org/>

Information Technology Association of America (ITAA)

ITAA provides global public policy, business networking, and national leadership to promote the continued rapid growth of the IT industry. The Association represents over 325 information technology companies. ITAA has an Identity Management Committee that was created to provide a forum for industry to work with federal, state, and global governments to develop best practices for the authentication and verification of identity, as well as to promote the use of technology to increase the security of our credentialing and access systems. Members include companies producing driver's licenses, national identity credentials, and other identity cards; managing federal, state, and local smart card and identity credentialing programs; providing biometric devices, radio frequency identification technologies, and middleware solutions; as well as performing background checks and other identity proofing services.

See: <http://www.ita.org>

APPENDIX E: EAF/EAP LEVELS

The following is a very brief description of the E-Authentication Federation (EAF) among U.S. government agencies and its companion organization for private sector organizations, the E-Authentication Partnership (EAP). Please refer to the EAF home page (<http://www.cio.gov/eauthentication/>) for comprehensive documents and updates.

The National Institute for Standards and Technology (NIST) has documented EAF policies, standards, practices, and technology.

The EAF is designed to create a trust infrastructure for authenticating individuals who wish to connect to Internet-based services from federal agencies. The EAP, which licenses EAF standards, is a partnership attempting to enable interoperability for electronic authentication among public and private sector organizations. The EAF is further developed than the EAP, and for simplicity, we will refer to EAF for the rest of this discussion.

Joining the EAF requires Credential Service Providers and Relying Parties to agree to use the components of the infrastructure, and to abide by the Business Rules and Operating Rules and comply with the requirements of the appropriate documents such as NIST SP 800-53 or NIST SP 800-63.

Credential Service Provider — An organization that offers one or more credential services (i.e., proofs and provides credential to individuals).

Relying Party — A person or agency that relies on the credentials issued by a Credential Service Provider.

There are many technology, security, privacy, business, and operating requirements for all participating organizations covered by the suite of documents and components used to guide the implementation of the EAF. The following discussion will focus on those specific to identity proofing and credentials of individual users.

Relying parties within the EAF self-assess the risk associated with reliance upon e-

authentication credentials.¹⁶ Based upon this risk assessment, the relying party chooses which of four designated levels of authentication stringency will be required for accessing one or more of its online resources such as web sites, applications, or information.

Level 1 has no level-specific requirements for proofing or issuance (and thus does not have a section in the chart below). This level can be employed when the Relying Party does not have a need to ascertain the identity of the person accessing a resource. The consumer employs self-assertion, and she may employ a pseudonym. Due to the lack of identity proofing, the low level of security provided by Level 1 authentication is inappropriate for use in facilitating access to personal health information.

¹⁶ See *Electronic Risk and Requirements Assessment (e-RA)*. Accessed online May 9, 2007, at: <http://www.cio.gov/eauthentication/era.htm>.

Proofing Requirements Under EAF

The table below¹⁷ summarizes the requirements of Levels 2-4. Both in-person and remote identity proofing methods are permitted for Levels 2 and 3. Explicit requirements are specified for each scenario in Levels 2 and 3. Only in-person initial proofing is permitted at Level 4.

LEVEL 2		
	In-Person	Remote
Basis for issuing credentials	Possession of a valid current primary Government Photo-ID that contains applicant's picture and either address of record or nationality (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 account number (e.g., checking account, savings account, loan, or credit card) with confirmation via records of either number.
Registration Authority Actions (Proofing)	<p>Inspects Photo-ID, compares picture to applicant, records ID number, address, and DoB. If ID appears valid and photo matches, applicant then:</p> <p>a) If ID confirms address of record, authorizes or issues credentials and sends notice to address of record, or;</p> <p>b) If ID does not confirm address of record, issues credentials in a manner that confirms the address of record.</p>	<p>Inspects both ID number and account number supplied by applicant. 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, other personal information in records are on balance consistent with the application and sufficient to identify a unique individual.</p> <p>Address confirmation and notification:</p> <p>a. Sends notice to an address of record confirmed in the records check or;</p> <p>b. Issues credentials in a manner that confirms the address of record supplied by the applicant; or</p> <p>c. Issues credentials in a manner that confirms the ability of the applicant to receive telephone communications or e-mail at number or e-mail address associated with the applicant in records.</p>

¹⁷ Table is adapted from *NIST Special Publication 800-63, Version 1.0.2, Electronic Authentication Guideline*. (April 2006). Accessed online May 9, 2007, at: 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 Photo-ID that contains applicant's picture and either address of record or nationality (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 account number (e.g., checking account, savings account, loan, or credit card) with confirmation via records of both numbers.
Registration Authority Actions (Proofing)	<p>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, records ID number, address, and DoB. If ID is valid and photo matches applicant then:</p> <p>a) If ID confirms address of record, authorizes or issues credentials and sends notice to address of record, or;</p> <p>b) If ID does not confirm address of record, issues credentials in a manner that confirms address of record</p>	<p>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. Address confirmation:</p> <p>a. Issues credentials in a manner that confirms the address of record supplied by the applicant; or</p> <p>b. 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.</p>

LEVEL 4		
	In-Person	Remote
Basis for issuing credentials	In person appearance and verification of two independent ID documents or accounts, meeting the requirements of Level 3 (in person and remote), one of which must be current primary Government Photo-ID that contains applicant's picture and either address of record or nationality (e.g., driver's license or passport), and a new recording of a biometric of the applicant at the time of application	Not applicable
Registration Authority Actions (Proofing)	<ul style="list-style-type: none"> • <i>Primary Photo-ID</i>: Inspects Photo-ID and verifies via the issuing government agency, compares picture to applicant, records ID number, address, and DoB. • <i>Secondary Government ID or financial account</i> <ol style="list-style-type: none"> a. Inspects Photo-ID and if apparently valid, compares picture to applicant, record ID number, address, and DoB, or; b. Verifies financial account number supplied by applicant through record checks or through credit bureaus or similar databases, and confirms that: name, DoB, address, other personal information in records are on balance consistent with the application and sufficient to identify a unique individual. • <i>Records Current Biometric Record</i> - a current biometric (e.g., photograph or fingerprints to ensure that applicant cannot repudiate application). • <i>Confirms Address</i> - Issues credentials in a manner that confirms address of record. 	Not applicable

Ongoing Tokens Under EAF

The following tables describe the allowable uses of tokens under EAF levels 2-4. Table 2 shows the types of tokens that may be used at each authentication assurance level. Table 3 identifies the protections that are required at each level. Protections are defined in section 8.1.2 above. Table 4 summarizes the requirements for the resistance of passwords to online password guessing attacks. Table 5 identifies the types of authentication protocols that are applicable to each assurance level. Table 6 identifies additional required protocol and system properties at each level. (NIST 800-63; page 38, section 9.)

Table 2. Token Types Allowed at Each Assurance Level

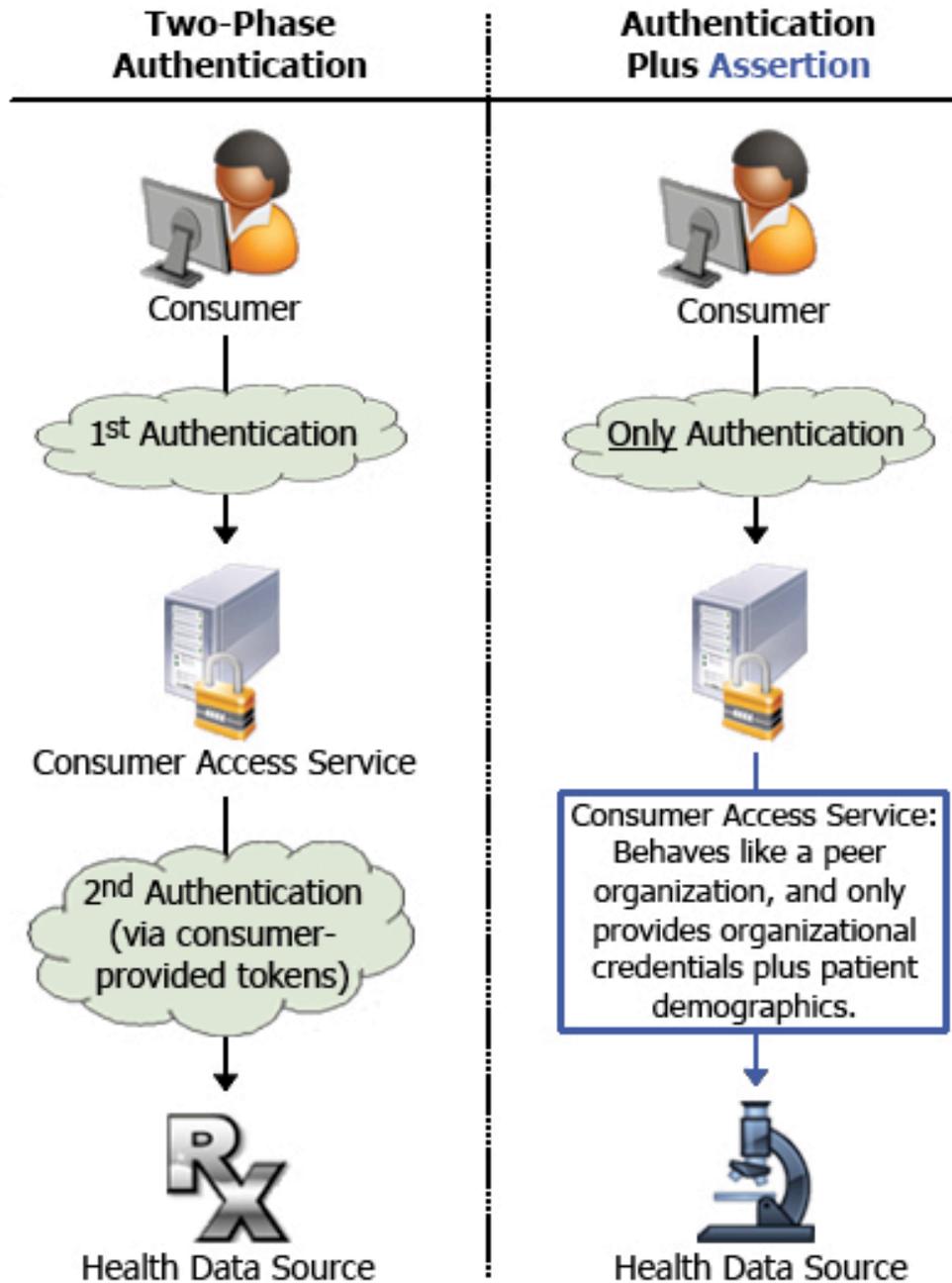
<i>Token type</i>	Level 1	Level 2	Level 3	Level 4
Hard crypto token	√	√	√	√
One-time password device	√	√	√	
Soft crypto token	√	√	√	
Passwords & PINs	√	√		

Table 3. Required Protections

<i>Protect against</i>	Level 1	Level 2	Level 3	Level 4
Online guessing	√	√	√	√
Replay	√	√	√	√
Eavesdropper		√	√	√
Verifier impersonation			√	√
Man-in-the-middle			√	√
Session hijacking				√

APPENDIX F: TWO MODELS OF REMOTE AUTHENTICATION

There are at least two possible architectural solutions to the question of allowing a Health Data Source to accept a Consumer Access Services' request for copies of a consumer's health data. First, the Health Data Source could re-authenticate the consumer. Collectively, we will call this repeated authentication process a **two-phase authentication** (not to be confused with two-factor authentication). Second, in lieu of re-authenticating the consumer, the remote data source could accept an identity assertion from the Consumer Access Service. Collectively, we will call this scenario **authentication plus assertion**. The diagram, text, and table below will elaborate on the differences between these two processes.



In **authentication plus assertion** (right hand model), the consumer only authenticates to the Consumer Access Service, which then transmits an assertion to the remote source indicating that the consumer is requesting data. In addition to this assertion, the Consumer Access Service passes along its own organizational credentials. The Consumer Access Service authenticates the consumer, but asserts to the remote data source that it is acting on the consumer's behalf by presenting the demographic information necessary to match the consumer to data held by the remote data source. Therefore, authentication plus assertion assumes that a data owner trusts another entity (i.e., the local application) to authenticate the consumer.

In **two-phase authentication** (left hand model), the consumer has two separate sets of authentication credentials and procedures. Both the Consumer Access Service and the remote data source maintain separate authentication information on the consumer. Each has gone through a process that initially proves the consumer's identity, and each has an associated method for authenticating the consumer on an ongoing basis. The role of the Consumer Access Service is to both locally authenticate the consumer and to transmit the consumer's information that is required by the remote data source to perform its authentication process. In this second step, the Consumer Access Service acts only as a proxy.

Let's consider an example that illustrates **two-phase authentication**. Programs such as Quicken allow users to download data from remote sources (banks, brokerage firms, etc.) into the local application. When a user wishes to download data from her bank into her Quicken application, she must first authenticate locally (i.e., log into the Quicken software). Then, when she requests a data download, Quicken sends the login-name/password combination that corresponds to her bank's online banking service. (For convenience, the user has already stored her login-name and password within Quicken.) Thus, Quicken acts as the user's proxy during the remote data source authentication process. In the case that the local application is a web-based service, such as the Consumer Access Service, the local application can use mechanisms such as SAML to transmit the user's credentials.

This two-phase authentication model puts the burden of authentication on the consumer and the data sources. The individual must log in to multiple data sources before accessing data through the Consumer Access Service. Data gathering and authentication choices are handled by proximate data sources. Consumer access authentication choices are handled by the Consumer Access Service. This model is the safe deposit model — the consumer's authentication with the Consumer Access Service is unrelated to her authentication with the proximate data sources. There is also nothing specific to health care governing the collection of usernames and logins for remote services, increasing the risk.

However, having established that the consumer has authenticated both at the Consumer Access Service and at a data source, the Consumer Access Service and a data source could set up a business relationship such that all subsequent logins would be treated as the same person. This would make it possible to rely on the clinical data source's proofing mechanism, but the Consumer Access Service's authentication method. The weak link in this system is the Consumer Access Service authentication mechanism. The Consumer Access Service and the clinical data source would have to agree on the stringency of the Consumer Access Service authentication requirements, and have mechanisms for audit and redress.

In **authentication plus assertion**, the consumer only authenticates to the Consumer Access Service, which then transmits an assertion to the remote source indicating that the consumer is requesting data. In addition to this assertion, the Consumer Access Service passes along its own organizational credentials. The Consumer Access Service authenticates the consumer, but asserts to the remote data source that it is acting on the consumer's behalf by presenting the demographic information necessary to match the consumer to data held by the remote data source. Therefore, authentication plus

assertion assumes that a data owner trusts another entity (i.e., the local application) to authenticate the consumer.

The table below compares these two processes based on a list of issues:

Issue	Two-phase Authentication	Authentication plus Assertion
Ease of use for consumer		Advantage
Technical work for implementing authentication		Advantage
Number of proofing/token problems per remote access	2	1
Susceptibility to man-in-the-middle attacks		Advantage against browser hacks (but open to attacks between Consumer Access Service/data sources)
Susceptibility to error/abuse by human authorizer	Advantage	
Legal risk for remote data source	Advantage	
Scales well for establishing relationships from data source to Consumer Access Service	Advantage	
Cost to Consumer Access Service to implement	Low	High
Cost to individual data sources	High	Low

Authentication plus assertion requires data owners to be willing to delegate authentication to another entity. Unless a data source has developed appropriate legal agreements that cover mistakes made by delegates (e.g., releases of data to the wrong person), the data owner (and its insurance carrier) may be unwilling to delegate its authentication process to others.

Authentication plus assertion does not scale well from the standpoint of industry since every local application must have agreements with all remote data sources. As the number of local applications and remote data sources increases, the total number of agreements rises exponentially. Therefore, this model is only practical if one of the following conditions is true:

1. There are a limited number of both data sources and local applications or intermediaries (i.e., if there were only a handful of Consumer Access Service providers.)
2. There are a limited number of data sources.
3. There are a limited number of local applications or intermediaries.

It is not the purpose of our Work Group to endorse one model over another. We believe it important to note that both models will likely be offered in the marketplace for some time to come.