MARKLE

CONNECTING FOR HEALTH

COMMON FRAMEWORK FOR NETWORKED PERSONAL HEALTH INFORMATION

POLICIES IN PRACTICE

The Download Capability

August 2010

MARKLE
Advancing Health in a Connected World

Policies in Practice 1:
The Download Capability

I. Introduction

A Vision for the Download Capability

Health information technology (health IT) provisions of the American Recovery and Reinvestment Act of 2009[1] (Recovery Act) set the expectation that individuals will be able to get electronic copies of pertinent health information about themselves.

The federal government and the private sector are investing billions of dollars in health IT to improve health care quality and efficiency, enhance safety, promote patient engagement, and protect privacy. A simple and efficient way for individuals to get their own health information electronically must be a priority of these efforts.

Markle Connecting for Health, a public-private collaborative established to improve health by accelerating the full potential of information technology, has long considered patients and their families to be information partners with health care professionals. They are knowledge contributors, shared decision makers, personal and family care advocates, and care plan collaborators. The Markle Connecting for Health Common Framework for Networked Personal Health Information (Markle Common Framework),[2] developed and endorsed by 58 diverse organizations, details policies and practices to enhance individual access to personal health information and protect privacy.

Information is a foundation for individuals to be active participants in achieving health-improvement and efficiency goals targeted by taxpayer subsidies of health IT.

Delivering personal health information to an individual's desktop or device is only a small step. But this initial step represents a big change in current practice and it can enable a whole host of innovations and services that can add significant value for individuals over time.

Current Opportunity

As public and private sector organizations, we are working together to make it commonplace for individuals to be able to routinely download their pertinent health information from providers and other entities that generate and collect it.

There are several things we can do to make this possible:

- **Make the download capability a common practice.** We call on organizations that display personal health information electronically to individuals in Web browsers to include an option for individuals to download the information under Markle Common Framework Policies in Practice outlined below.

- **Implement sound policies and practices to protect individuals and their information.** We are mindful that added convenience and increased data liquidity must come with a carefully considered policy framework to prevent abuse and consumer mistrust. We believe that a necessary step is implementing the Markle Common Framework for Networked Personal Health Information, as well as *Policies in Practice—PP1: The Download Capability*.

- **Collaborate on sample data sets.** The Centers for Medicare & Medicaid Services and the U.S. Department of Veterans Affairs are leading

[1] American Recovery and Reinvestment Act of 2009. Pub. L. No. 111–5 *(Feb. 17, 2009)*.

[2] *Markle Common Framework for Networked Personal Health Information*. Available at www.connectingforhealth.org/phti/index.html.

the way in making publicly available sample data sets for demonstrations. We call on other private sector custodians of health information to join the effort by contributing additional sample data sets and joining in problem-solving.

- **Support the download capability as part of Meaningful Use and qualified or certified health IT.** A diverse collaborative of more than 50 organizations used the public comment period to recommend the download capability as an option for providers and hospitals to achieve the Stage 1 patient-engagement requirements of Meaningful Use of health IT under the Recovery Act.[3] We urge the U.S. Department of Health and Human Services (HHS) to specify the download capability as an allowable means for providers to deliver electronic copies to individual patients. We recommend that the download capability be a requirement of qualified health IT so that providers using qualified systems will have this capability.[4]

- **Include the download capability in procurement requirements.** We encourage making the download capability a core procurement requirement for federal- and state-sponsored health IT grants and projects, as well as a priority in health information exchanges (HIEs) and private-sector purchasing initiatives for personal health information services. Our diverse group of organizations can implement the download capability as a procurement requirement in a variety of ways.

RATIONALE

Individual access to information is rooted in fair information principles and law. The ability to access information about oneself is a core component of Fair Information Practices, as articulated by the Federal Trade Commission for more than a quarter century. Federal law firmly establishes this expectation for personal health information. The Health Insurance Portability and Accountability Act (HIPAA) codifies the individual's right to request and receive personal health information from health care entities. Section 13405 (e) of the Health Information Technology for Economic and Clinical Health Act (HITECH), part of the economic stimulus Recovery Act, establishes an individual's ability to request certain information in electronic format from electronic health records (EHRs) and have it sent to a service of the individual's choosing.[5]

Patients need and want the information. Empowering patients and their families by placing information directly in their hands can help fill information gaps in health care and enhance communication between patients and medical professionals. Patients are often in the best position to gather and share information with their different providers. For example, a physician might know that a medication has been prescribed for a patient. But without asking the patient, the doctor does not know whether the patient actually took the medication, how well it worked, what other remedies the patient is taking, or whether there have been side effects.

---

3 *Collaborative Comments on the Centers for Medicare and Medicaid Services' Notice of Proposed Rulemaking for the Electronic Health Record Incentive Program (CMS-0033-P).* Available at www.markle.org/downloadable_assets/20100315_ehrincent_cms0033p.pdf.

4 *Collaborative Comments on the Office of the National Coordinator's Interim Final Rule on the Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology,* March 15, 2010. Available at www.markle.org/downloadable_assets/20100315_ehrtechifrrule.pdf.

5 Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5 (Feb. 17, 2009), §13405(e).

Four out of five Americans believe that using an online personal health record (PHR) that includes electronic copies of health information would provide major benefits to individuals in managing their health and health care services.[6] At least 86 percent of respondents say that PHRs could help them avoid duplicated tests, keep doctors informed, move more easily from doctor to doctor, check the accuracy of their medical records, and track personal health expenses.[7]

The download capability would encourage innovation. In a powerful new opportunity for innovation, the individual's secure access to personal health information can enable new platforms, applications and services to provide value in a rich variety of ways. The explosion of iPhone applications is a particularly salient example. Application developers make use of the iPhone platform, and pull together a rich variety of data sets, including information contributed by iPhone users themselves, to create a wide array of offerings.

While experimentation and failure are a part of all innovation cycles, the potential is great to learn how health information can be used in helping people better manage their health and health care.

Initially, even if only a small percentage of people download copies of their information online, those who do can help drive improvements in service that eventually benefit everyone. The key is to make the data available to individuals, beginning with the most basic means possible.

A download capability frees data sources from having to make many decisions about the user interface. Although the Recovery Act includes a provision requiring that individuals be able to request and receive copies of their health information electronically, not every vendor and provider is suited to or capable of supporting patient portals, developing high-value applications for patients to use, or of dealing with implementation and adoption challenges. In fact, it is not realistic or desirable to expect every holder of a patient's data to also be the purveyor of patient-facing portals or applications. This may be untenable for patients and providers alike. We recommend instead the use of federal levers in the form of standards or incentives to encourage and support the development of services that allow individuals to compile copies of their health information from multiple providers and sources. A recent program at Kaiser Permanente Colorado to help patients manage blood pressure control provides one example of this.[8] Patients used at-home blood pressure monitors and Web-based reporting tools to connect with their clinicians. In addition to working with their clinicians, patients were able to access their home blood pressure readings directly through a secure Web-based personal health data storage service. There, they could manage their data using a wide variety of applications that could also pull information from other data sources, including medical information from other providers and from home monitoring equipment. For example, patients were able to use Heart360, a free online tool provided by the American Heart Association, to track and manage their cardiac health.

---

6 *Americans Overwhelmingly Believe Electronic Personal Health Records Could Improve Their Health,* Markle Foundation survey conducted by Knowledge Networks, June 25, 2008. Available at www.connectingforhealth.org/resources/ResearchBrief-200806.pdf.

7 Ibid.

8 *Home Health Monitoring May Significantly Improve Blood Pressure Control, Kaiser Permanente Study Finds,* PR Newswire, May 21, 2010. Available at www.prnewswire.com/news-releases/home-health-monitoring-may-significantly-improve-blood-pressure-control-kaiser-permanente-study-finds-94576164.html.

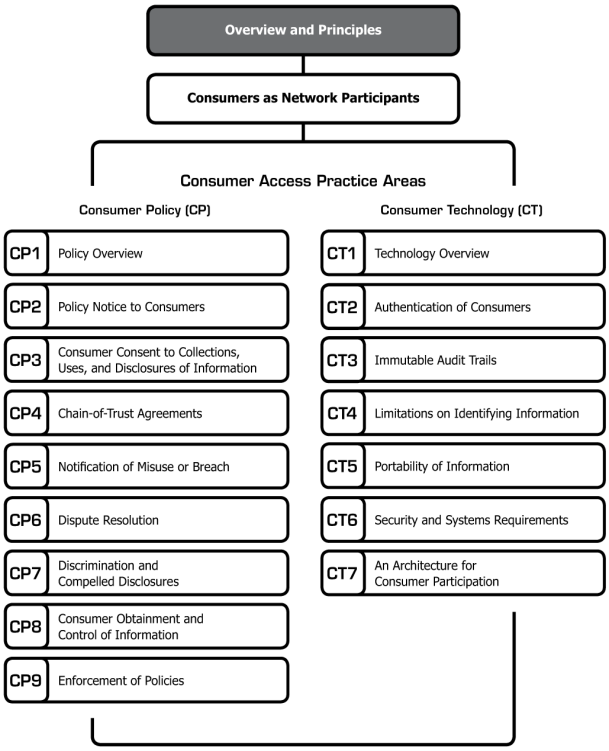
A download capability would likely hasten the path to standards and interoperability. The download feature clearly separates data from applications (i.e., the patient can access and keep copies of the information without being locked into a particular portal or application). This critical separation makes it technically easier for various services of the patient's choosing to parse and use the downloaded information. Ultimately, commonly structured and codified data can be a dramatic accelerator for the development of more sophisticated applications or services that may help people benefit from and further use their information. The consumer finance and online banking sectors demonstrate that making personal information directly accessible to individuals increases demands for standards to improve efficiency and meet market expectations.

II. Policies in Practice 1 (PP1)

Overview of the Download Capability

As with any health IT feature or service, the download capability must be implemented with attention to sound information policies and privacy protections. Although regulations apply unevenly across the spectrum of organizations that offer electronic personal health records and similar services, there is a broadly endorsed framework[9] that applies specifically to this area.

When taken together, the practices described in the Markle Common Framework enhance individual participation and protect privacy. All organizations that offer the download capability to individuals—whether they are HIPAA-covered entities, business associates of HIPAA-covered entities, or not at all covered by HIPAA—must address each of the practices in the framework in a sound and public way. Therefore, any service that offers the download capability to individuals, and any service that seeks to make use of the downloaded information on the individual's behalf, should abide by each of the policies and practices in the Markle Common Framework:



[9] *Fifty-eight diverse organizations have endorsed the Markle Connecting for Health Common Framework for Networked Personal Health Information.* See the endorsement statements at www.connectingforhealth.org/resources/CCEndorser.pdf.

The Markle Common Framework is a general set of policies and practices for a wide array of networked personal health information services, including the download capability; we encourage entities who offer the download capability to apply the full spectrum of policies and practices described by it.

In considering how the Markle Common Framework applies to the narrower context of the download capability, several requirements are self-evident, such as adopting best industry practices for data transaction security when information is downloaded. In addition, CT5: Portability of Information[10] of the Markle Common Framework states that PHR services should provide an easy-to-use mechanism for individuals to export the information in their accounts for personal use. It details that such mechanisms should:

- Provide information in human-readable form.
- Log each transaction (e.g., download) in an immutable audit trail.
- Include time-, date-, and source-stamps for key data entries (e.g., diagnoses) within the downloaded information itself.
- Include a printer-friendly format.
- Enable data to be exported into commonly used software formats, such as spreadsheets, PDFs, or text files. Conform to industry standards for health data subsets as they become available and broadly implemented.

As applied to Meaningful Use, this final item necessitates standardized clinical summary formats adopted by HHS in 45 CFR Part 170.205(a), i.e., CCD or CCR.[11] The value of the download capability will be substantially enhanced when the downloadable data are commonly structured. The value increases dramatically when specific data elements, such as laboratory results or medication lists, are commonly codified for computability, which can enable a wide variety of value-added services and decision support.

Specific Markle Common Framework Policies in Practice

In our assessment of the Markle Common Framework's applicability to the specific context of the download capability, we determined that there were some practice areas that should be further detailed to be very specific about the practices required of entities that offer this capability. Together, we defined a subset of more detailed practices that would fulfill the Markle Common Framework requirements. We have drafted these as *Policies in Practice—PP1: The Download Capability*:

- PP1a: Helping Individuals Make Informed Choices
- PP1b: Making the Download Capability Available to the Right Person (and the Right Machines)

[10] *Markle Common Framework for Networked Personal Health Information, CT5: Portability of Information, June 2008*. Available at www.connectingforhealth.org/phti/reports/ct5.html.

[11] Title 45, CFR Part 170.205(a) adopts the Health Level Seven Clinical Document Architecture (CDA) Release 2, Level 2 Continuity of Care Document (CCD) and ASTM E2369 Standard Specification for Continuity of Care Record (CCR) and Adjunct to ASTM E2369 (as of August 24, 2010).

PP1a: Helping Individuals Make Informed Choices

Simplicity is one of the biggest strengths of the download button. No matter how simple this concept, however, individuals need to be made aware of how it works.

The implications of downloading sensitive information to a computer or device may not be fully apparent to large numbers of people. For example, an unaware individual may download personal files and leave them unsecured on a shared computer at work or a public library. The interface must enable individuals to make informed choices. The options should be depicted as clearly as possible, with prominent and accurate information about the risks as well as the opportunities.

A goal of the download capability is to reduce the barriers for individuals to access their data. It will be counterproductive if attempts to educate people about the risks of the download capability are unnecessarily alarming or laden with legalese. Sound practices to help individuals make informed choices should prevent either of these bad outcomes:

- Individuals clicking the download button are unaware of the privacy and security implications.
- Individuals are frightened away from clicking the download button due to too many warnings.

The Markle Common Framework for Networked Personal Health Information has detailed recommendations on providing notice (appropriately posting statements of policies, practices, protections, and risks) and obtaining consent (confirming the individual's permission for collections, uses, and disclosures of information).

CP2: Policy Notice to Consumers[12] and CP3: Consumer Consent to Collections, Uses and Disclosures of Information[13] offer general guideposts for providing individuals with easy-to-understand and contextually appropriate information for them to make informed choices, even if the term "confirmation" may be better than "consent" in this context of individuals downloading copies of information about themselves to a computer or device that they are using.

We assume that any organization providing online access to personal health information is addressing all of the policies of the Markle Common Framework, including the policy notice requirements outlined in CP2: Policy Notice to Consumers[14], which says that notices must be clearly written, summarized, comprehensive, easily accessible, updated, and focused on consumer protections provided (i.e., not focused predominantly on what the service may do, or on limitations of its liability). The policies of the

---

12 *Markle Common Framework for Networked Personal Health Information, CP2: Policy Notice to Consumers, June 2008*. Available at www.connectingforhealth.org/phti/reports/cp2.html.

13 *Markle Common Framework for Networked Personal Health Information, CP3: Consumer Consent to Collections, Uses and Disclosures of Information, June 2008*. Available at www.connectingforhealth.org/phti/reports/cp3.html.

14 *Markle Common Framework for Networked Personal Health Information, CP2: Policy Notice to Consumers, June 2008*. Available at www.connectingforhealth.org/phti/reports/cp2.html.

Markle Common Framework also require detailed consent practices[15], including the need to specifically obtain consent that distinguishes between:

- **general consent** (i.e., when one agrees to use a service after exposure to the marketing materials, privacy policies, terms of services, and similar information)

- **independent consent** (i.e., permissions that should be obtained specifically for collections, uses, or disclosures of information that may be unexpected by a reasonable person, or when personal data are to be exchanged with a third party that may have different policies or practices)

Under the Markle Common Framework, the general standard for independent consent centers on a reasonable person's expectations and is rooted in the principle that choices be proportional (i.e., the more sensitive, personally exposing, or inscrutable the activity, the more specific and discrete the consent required).

Fundamentally, any organization offering the download button should **inform** individuals about the choice to download information and **confirm** that the individual really wants to do it. That means providing a simple explanation at the point of decision, as recommended below.

Specific Practices For Organizations that Provide the Download Capability

When an individual is downloading from a secure online service to a computer or a device, the provider of the download button should do the following:

- Provide a clear, concise explanation of the download function and its most fundamental implications for the individual.

- Provide prominent links that enable individuals to view more details about the download process, including what basic security precautions they can take on their own, how the service answers questions (e.g., through direct communication, FAQ page, or other means), and who they should contact if they believe some of the downloaded information is in error).

- Obtain independent confirmation from the individual (i.e., such as a "yes" response to a question) that the individual wants to download a copy of personal health information. Such independent confirmation should be obtained after presenting the individual with, at minimum, the following clearly stated information:

  Health records can contain sensitive information.

  If you download sensitive information to a shared or unsecured computer or device, others might see it.

  You are responsible for protecting the information that you download, and for deciding with whom to share it.

  Are you sure you want to download a copy of your personal health information to the computer or device you are using?

[15] *Markle Common Framework for Networked Personal Health Information, CP3: Consumer Consent to Collections, Uses and Disclosures of Information, June 2008*. Available at www.connectingforhealth.org/phti/reports/cp3.html.

- Present the individual with a conspicuous means to cancel the download at every step up to the final confirmation step (e.g., when the individual answers "yes" to the above question). It is good practice to include not only a "yes" and a "no" option, but also a "tell me more" option, which enables the individual to get a more detailed explanation.

People may be provided this information in a variety of ways, including bulleted text, animations, video, interactive dialog boxes, etc. It is good practice to user-test the effectiveness of various messages and means of communication to optimize the level of detail needed for individuals to make informed choices.

RATIONALE

It is a basic fair information practice to help people know what they are agreeing to and doing. Not all individuals understand the security implications of downloading information to a device or desktop. Distinctions between Web-based services and a computer desktop are increasingly blurred as well, as more online services interact with desktop applications and vice versa.

The essential point is that when an individual clicks a download button, it opens up a new data stream carrying new copies of personal information, with new opportunities and new risks. For this reason, the download button should require contextual explanations and an independent step for confirmation, most essentially upon the initial time that the individual opts to click it. It is good practice to remind individuals about what they are downloading, where it will go, and who will be responsible for its security and subsequent sharing.

Notice, consent, education, and confirmation are linked concepts that are most effective when presented to the individual in a logical, user-friendly flow. For example, good e-commerce sites provide a simple and assuring checkout sequence in which individuals can always see where they are in the process, cancel or modify their requests at any time, and finally, easily review all essential terms of the transaction before pressing a conspicuous button to process their order.

This information is best presented at the point that users are ready to initiate a request or complete a transaction, when individuals are likely to be most attentive.

NOTE: The above scenario (i.e., an individual downloading information to a computer or device) is only one possibility by which individuals may obtain electronic copies of their health information. There will be other scenarios in which an individual is asked to authorize regular, automated downloads of personal health information by a service acting as the individual's proxy. The Markle Common Framework for Networked Personal Health Information provides a comprehensive set of recommendations for such environments, including those practices required in CP2: Policy Notice to Consumers[16] and CP3: Consumer Consent to Collections, Uses and Disclosures of Information[17].

[16] *Markle Common Framework for Networked Personal Health Information, CP2: Policy Notice to Consumers, June 2008*. Available at www.connectingforhealth.org/phti/reports/cp2.html.

[17] *Markle Common Framework for Networked Personal Health Information, CP3: Consumer Consent to Collections, Uses and Disclosures of Information, June 2008*. Available at www.connectingforhealth.org/phti/reports/cp3.html.

PP1b: Making the Download Capability Available to the Right Person (and the Right Machines)

Any online download capability for personal health information must be provided via secure access. That means the identity of each individual given credentials to access their own data must be proofed to an acceptable level of accuracy, and the individual must present those credentials or some acceptable token of those credentials upon login in order to get access to the data for download.

However, such download capabilities present challenges beyond making sure that the authorized individual is getting access. If the download capability becomes a common feature on patient portals and other personal health information services, as we believe it should, it would make structured health data more accessible to the right individuals and authorized third parties, and more easily harvestable by automated processes, whether acting as legitimate proxies or as impostors. Therefore, it is important to distinguish accurately between requests made by humans and those by machines.

Specifically, an individual may want to authorize a service to aggregate personal health information on the individual's behalf. Clearly, the most efficient way to perform such aggregation is through automated downloads of the individual's personal health information. The challenge is, therefore, not to distinguish between a human and a machine, but to be able to detect an individual-authorized machine versus a non-authorized machine.

To preserve the security of authentication tokens, the solution must enable individuals to authorize automated downloads by proxy services without giving those proxies the secure user names and passwords they maintain at each health data collection point (e.g., at each medical provider they visit).

Balanced against each of these challenges is an imperative for solutions to raise as few additional technical barriers as possible, because an individual's health information may be scattered across several organizations, including some with limited technical capabilities. For example, there are multiple approaches to conducting machine-to-machine authentication, but not all of them are feasible across all provider settings.

Recommendation: NIST should provide guidance on identity proofing and authentication of individuals.

The Federal Government, through the expertise of the National Institute for Standards and Technology (NIST) and other appropriate agencies, should recommend a framework for acceptable methods and accuracy thresholds for the initial identity proofing and authentication for individuals accessing copies of their personal health information online.

RATIONALE

Congress and the current administration have made increasing accessibility of electronic health records to providers and citizens a national goal. One hurdle to this goal is the lack of well-understood and generally agreed-to methods to manage the identity of individuals online, a challenge that is not unique to health care.

Given that patient engagement is a federal health IT priority, and that federal laws and regulations support the expectation that individuals should have electronic access to their personal health information,

there is a need for federal guidance on acceptable thresholds for identity proofing and authentication of individuals. This is particularly important within the context of requirements for health care providers giving their patients electronic copies of personal health information to meet the patient-engagement components of Meaningful Use in order to qualify for health IT subsidies under the Recovery Act.

To be clear, this is not a request for a common identifier, or identification methodology, but rather for a required level of accuracy to be used in determining that the correct individual gets authorized access to their records. There is no one-size-fits-all answer to this issue. We believe that the E-Authentication Federation (EAF) and Electronic Authentication Partnership (EAP), as well as the Department of Homeland Security's recently drafted National Strategy for Trusted Identities in Cyberspace,[18] provide a good framework for discussion on finding an acceptable degree of authentication certainty and policy enforcement for the use case of individuals accessing their health information online. Based on practicality and current experience, we presume that EAP Level 2 or 3[19] is generally the right range of requirements for a spectrum of contexts. Further guidance from the government through NIST could be highly beneficial to the overall environment.

There are many ongoing collaborative groups working on this problem. It is important for the government to recommend the best options for critical use cases such as the patient engagement requirements of Meaningful Use.

Specific Practices for Organizations that Offer the Download Capability

We assume that any organization providing online access to personal health information is addressing all of the policies of the Markle Common Framework for Networked Personal Health Information, including the identity management practices outlined in CT2: Authentication of Consumers,[20] which contains guidance on identity proofing (including face-to-face and remote procedures), issuance of tokens or identifiers, ongoing activity monitoring to detect fraud, and reliance on third parties or federations for each of these activities.

We recommend the following specific practices for the download button:

- **Deploy separate pathways for download requests from the individual, and download requests via automated processes acting on the individual's behalf.** Services offering download capabilities should create one URL for the individual to request downloads, and a separate URL to be accessed by machines. This separation of access points for the data is designed to discourage third-party services from asking for or operating with the individual's passwords or other digital tokens to collect the individual's information (even when the individual has authorized such third-party services to receive automated

[18] *National Strategy for Trusted Identities in Cyberspace: Creating Options for Trusted Online Security and Privacy,* Department of Homeland Security, June 10, 2010. Available at www.dhs.gov/xlibrary/assets/ns_tic.pdf.

[19] For an explanation of EAP levels 2 and 3, see Appendix E: EAF/EAP Levels, Markle Common Framework document *CT2: Authentication of Consumers,* available at www.connectingforhealth.org/phti/reports/ct2-7.html.

[20] *Markle Common Framework for Networked Personal Health Information, CT2: Authentication of Consumers, June 2008*. Available at www.connectingforhealth.org/phti/reports/ct2.html.

downloads). Further, the separation of access points as a matter of policy should encourage the adoption of standards that let the patient link data sources and PHR services securely without making such password or token disclosures. To set this up, the individual logs in separately at each entity, using different user names and passwords at each, and then authorizes data exchange between the two entities for a given time period or under other constraints. We recommend that organizations providing the download button implement such a standard to handle automated requests from individual-authorized services.

- **On human-accessible download pages, deploy an effective means to determine whether a human is requesting the download.** Although there is no perfect device to determine whether a human is accessing the contents of a URL, CAPTCHAs (challenge-response tests designed to be solvable by a human but not by a computer) are commonly deployed and considered effective. Whether or not a machine-accessible URL is available, we recommend that human-accessible URLs offering downloads use a CAPTCHA or another effective means of ascertaining that a human is indeed requesting the download.

- **Keep a record of download events in immutable audit logs.** As recommended in CT3: Immutable Audit Trails[21] of the Markle Common Framework, all imports and exports of information should be tracked in a running log that the individual is able to view at any time. The provider of the download button should capture as much information as practical from all requesters of downloads (human or machine), such as the IP address. This information can be important for monitoring activity and investigating suspected fraud.

- **Consider enabling individuals to set up automated notifications for each time their information is downloaded.** It is a common protection in online banking for individuals to be able to set up an automated email notification for major transactions or changes to their account. It is designed to help individuals monitor whether there is any unexpected activity related to their accounts. It is considered a good practice to provide such notification options for individuals in conjunction with the download capability for obtaining personal health information, particularly an automated email to provide notice after the initial download event.

- **Include source and time stamps for data entries in the information downloads.** CT3: Immutable Audit Trails[22] and CT5: Portability of Information[23] of the Markle Common Framework call for key data elements (e.g., diagnoses, procedures, and prescriptions) to be displayed with information about the time, date, and source, and for imports and exports of information to carry these time, date, and source stamps. As applied to the download, these stamps should be included in the information download itself, as well as information on contacting the source. For example, if a patient downloads an

[21] *Markle Common Framework for Networked Personal Health Information, CT3: Immutable Audit Trails, June 2008*. Available at www.connectingforhealth.org/phti/reports/ct3.html.

[22] *Markle Common Framework for Networked Personal Health Information, CT3: Immutable Audit Trails, June 2008*. Available at www.connectingforhealth.org/phti/reports/ct3.html.

[23] *Markle Common Framework for Networked Personal Health Information, CT5: Portability of Information, June 2008*. Available at www.connectingforhealth.org/phti/reports/ct5.html.

electronic copy of personal health information and shares that copy with her physician, it will be helpful for the physician to be able to view the recorded sources and dates associated with the information. Similarly, if an individual downloads information that she believes is in error, it should be easy for her to see the source and an explanation of how she may contact the source to request a correction or clarification. Digital signatures to validate information sources will likely be a necessary component of the download capability in the future, but this should not hold up progress today.

RATIONALE

The practices described here are intended to anticipate the environment if a personal health information download capability becomes ubiquitous, or even if it is offered by a few organizations that maintain tens of millions of records. Assuming that health data is made available for secure-access download, and that it is structured in ways that make it more amenable to automated harvesters, it will be important to do the following:

- Accurately establish the identity of individuals and issue appropriate tokens, with guidance from appropriate federal agencies for the context of online access by individuals to copies of their personal health information.

- Create a separate pathway for the automated harvesting of personal health information downloads. The best way to do this is through the implementation of a standard to separate download requests by humans from download requests from a known partner that is authorized by the individual. Note that the point of the CAPTCHA is not security but differentiation. The CAPTCHA is not to prevent unauthorized parties from accessing the data (the goal of security), but to encourage individual-authorized parties to avoid undesirable practices such as recording or reusing the passwords or tokens that the individual uses at various sites offering the download capability.

- Track and immutably log source information from requesting parties (such as IP addresses) as a means of monitoring and/or investigating potential fraud.

- Provide key time, date, and source information to aid the usefulness of the downloaded information for all authorized downstream users.

Acknowledgements

This set of policies and practices is a collaborative work of the **Markle Work Group on Consumer Engagement**, a public-private collaboration operated and financed by the Markle Foundation. Markle thanks the members of the Work Group for reviewing several drafts of these documents and improving them invaluably each time. We thank our federal partners at the US Department of Health and Human Services and the US Department of Veterans Affairs for their outstanding leadership and important contributions. We also thank Josh Lemieux, Markle Foundation, for drafting and editing the documents, and Clay Shirky, Adjunct Professor, New York University Graduate Interactive Telecommunications Program and the Technical Lead for Markle Connecting for Health, for his continued leadership and his skillful moderation of our Work Group discussions.

MARKLE WORK GROUP ON CONSUMER ENGAGEMENT

Rick Altinger
Intuit Health

Christine Bechtel
National Partnership for Women & Families

Adam Bosworth
Keas, Inc.

Mary Cain
LifeMasters-StayWell Health Management

Brian L. DeVore
Intel Corporation

Marc Donner
Google

Joyce Dubow
AARP

Colin Evans
Dossia Consortium

Steven Findlay, MPH
Consumers Union

Mark Gorman
National Coalition for Cancer Survivorship

Adrian Gropper, MD
MedCommons

James Heywood
PatientsLikeMe

Scott Heimes
WebMD Health

Joseph Kvedar, MD
Center for Connected Health, Partners HealthCare System, Inc.

David Lansky, PhD
Pacific Business Group on Health

Peter L. Levin, PhD*
US Department of Veterans Affairs

Deven McGraw, JD, MPH
Center for Democracy and Technology

John Moore
Chilmark Research

Tom Morrison
NaviNet

David Nace
McKesson Technology Solutions

Sean Nolan
Microsoft Corporation

Marcus Osborne
Wal-Mart Stores, Inc.

Raymond Scott
Axolotl

Clay Shirky
New York University Graduate Interactive Telecommunications Program

Kenneth Tarkoff
RelayHealth

Robert Tennant, MA
Medical Group Management Association

Steven Waldren, MD
American Academy of Family Physician

Matthew Wynia, MD, MPH
American Medical Association

** Federal, state and city employees collaborate but make no endorsement.*

MARKLE CONNECTING FOR HEALTH COLLABORATORS WHO SUPPORT THIS DOCUMENT

Hunt Blair*
Office of Vermont Health Access

William Braithwaite, MD, PhD
Anakam Inc.

Neil S. Calman, MD
The Institute for Family Health

Janet Corrigan, PhD, MBA
National Quality Forum

Rex Cowdry, MD*
Maryland Health Care Commission

Mike Cummins
VHA, Inc.

Alan F. Dowling, PhD
American Health Information Management Association

Mark Frisse, MD, MBA, MSc
Vanderbilt Center for Better Health

Daniel Garrett
PricewaterhouseCoopers LLP

Douglas A. Gentile, MD, MBA
Allscripts Healthcare Solutions

Joseph M. Heyman, MD
Whittier Independent Practice Association, Wellport;
Lower Merrimac Valley Physician Hospital Organization

Gerry Hinkley, JD
Pillsbury Winthrop Shaw Pittman LLP

Kevin Hutchinson
Prematics, Inc.

Brian F. Keaton, MD
American College of Emergency Physicians

Allan M. Korn, MD, FACP
Blue Cross Blue Shield Association

Arthur Levin
Center for Medical Consumers

Jack Lewin, MD
American College of Cardiology

Philip Marshall, MD, MPH
Press Ganey

Howard Messing
Meditech

Margaret E. O'Kane
National Committee for Quality Assurance

Amanda Heron Parsons, MD, MBA*
Primary Care Information Project

Carol Raphael, MPH
Visiting Nurse Service of New York

Stephanie Reel
Johns Hopkins Medicine

Peter A. Schad, PhD
RTI International

Scott Schumacher, PhD
Initiate, an IBM Company

Terri Shaw
The Children's Partnership

Ramesh Srinivasan
MedicAlert Foundation

Thomas E. Sullivan, MD
DrFirst

Robert Wah, MD
Computer Sciences Corporation

Jeb Weisman, PhD
Children's Health Fund

Markle Foundation

Zoë Baird
President

Carol C. Diamond, MD, MPH
Chair, Markle Connecting for Health

** Federal, state and city employees collaborate but make no endorsement.*