An Information-Rich Health Care Ecosystem

Response to the Office of the National Coordinator's Request for Information Regarding the PCAST Report on Realizing the Full Potential of Health Information Technology to Improve Health Care for Americans

This comment represents a collective view informed by the many and diverse collaborators of Markle Connecting for Health.

Executive Summary

Markle Connecting for Health, a public-private collaborative, supports the President's Council of Advisors on Science and Technology (PCAST) vision for an information-rich health ecosystem to improve health outcomes, increase the cost-effectiveness of care, encourage innovation, and protect privacy. We share PCAST's sense of urgency to catalyze broad-scale implementation of health information technology to transform health care.

Our comments emphasize the importance of clear goals and a policy framework, and consider the implications of implementing novel technology approaches in a heterogeneous environment such as the US health care system. Lastly, we provide a set of forward-looking recommendations.

We support the PCAST vision for the following:

- A nationwide capability of secure health information exchange using the Internet, not a new network.
- A distributed network for information-sharing, and not a national database.
- A model for linking patient information across sites of care using *existing* identifiers, and not a single national health identifier.
- An approach to technology that emphasizes innovation and a diversity of solutions to support broad participation and new entrants.
- A comprehensive set of privacy and security practices to support trust in information sharing.
- A universal exchange language for exchanging health information securely over the Internet.
- Population health improvement and analysis using distributed networks.

However, we also identify areas for further development and analysis based on our experience with three foundational principles. These principles, which have guided our work for nearly a decade, most notably the Markle Connecting for Health Common Framework, offer grounding for our comments on the PCAST report. These principles with related key findings and commentary are summarized below.

A. Adopt a trust framework based on Fair Information Practices (FIPs).

- Any information-sharing effort should adopt a trust framework that includes a full complement of protections, including clear and transparent policies and practices, limitations on data collections and uses, individual consent and controls, oversight, accountability, remedies, and enforcement, in addition to technical and security protections.
- Trust cannot be achieved with technology alone. We recommend that the approach taken develop information policies alongside the technical system requirements. The challenge is to find the right mix of policies, practices, technologies, and standards that can protect health information while allowing it to be shared with authorized parties, who will inherently be at different stages of technology adoption and sophistication.
- Consent, if used as the sole mechanism to protect privacy, can unintentionally result in weak protections for consumers. Consent is an important element of a full complement of both policy and technology protections, but it must be balanced and applied together with others. It may not be possible for individuals to make informed consent decisions about all of the granular data elements in an environment as complex as health care; therefore, the buttress created by a full array of protections is vital.

B. Protect privacy while enabling greater information sharing through simple, progressive steps using well-tested standards and technology.

- We believe the path toward this goal starts with the imperfect data of today, and takes into account the varying capabilities of a wide array of health care settings, ranging from sophisticated environments in large integrated delivery systems to small office practices.
- In order to move in this direction, the Office of the National Coordinator for Health Information Technology (ONC) should focus on deploying well-tested and widely used standards and technology that can be implemented within a comprehensive privacy and security framework of policies and practices.
- Because trust is primarily an attribute of entities or participants, rather than of software or data, progress will be made primarily through an expanding network of trusted participants, rather than being driven through novel networks or infrastructures.
- ONC should consider the following observations while evaluating the report's recommendations for using granular metadata and granular permissions controls, catalogued and moderated by a few national Data Element Access Services (DEAS):

- Experience has shown that large IT upgrades or novel national infrastructures have a high risk of implementation failure.
- Improving the reasons to share data, namely achieving quality and safety goals, creates an incentive to improve data quality and adopt more standardization—something the mere specification of standards can never achieve on its own.
- Experience with digital rights management (DRM) and the Platform for Privacy Preferences (P3P) also offer important insights whose implications must be further understood in efforts to tether privacy permissions to data in health care or to entirely rely on novel technology to solve a complex policy problem. The successful use of technologies that tether rules to data remains elusive, particularly in instances in which the technology was used to enforce a set of rights and obligations.
- The PCAST proposal requires services that can locate patient records. These services take information from patient records and store metadata about them in a small number of encrypted indices, queriable at the national level. While encryption is one key part of an approach to protect this metadata, it is not sufficient against some forms of breach, such as attacks by authorized actors, a common source in health care as well as other sectors (e.g. Equifax and SIPRnet). Restricting clinical information from indices can mitigate the risks posed by other vulnerabilities and wide-scale implementation challenges in the current environment.

C. Focus on rapid learning and better decision making by many.

- Our goal is an information-driven health care ecosystem, where analysis can be accomplished in a timely way to show what works, to alert decision makers about emerging trends, and to help clinicians make the best decisions possible to improve care while protecting privacy.
- One of the greatest strengths of the PCAST report is its vision for robust distributed population-level analysis and quality measurement that leverages digitized and networked health information.
- ONC is in a good position to take steps toward this vision today by encouraging the adoption of research methods and tools that enable distributed analysis of aggregate clinical data where data are cleaned and analyzed in a common way at the source before being sent in a standardized summary format. Stage 1 Meaningful Use is a good example, and we applaud its reporting requirements utilizing only de-identified aggregate summary results.
- We agree with PCAST that there is enormous potential for innovation in this area to help drive toward a more nimble and effective quality improvement ecosystem. To accelerate population health analysis, further investments in methodologies and best practices should be made.

Recommendations

1. Set clear health objectives to guide health IT investments.

- Government leadership is needed to focus the health sector on encouraging the effective use of information to reach specific health objectives. ONC and the Centers for Medicare & Medicaid Services (CMS) have laid a promising foundation with the Meaningful Use Rule.
- Government has the opportunity to add crucial visibility to key health objectives for the nation. For example, a declaration of specific targets—such as preventing one million heart attacks and strokes, cutting medication errors, and reducing administrative burdens by half—could add visibility and focus to future stages of Meaningful Use.
- The deliberate and strategic alignment of current Health Information Technology for Economic and Clinical Health Act (HITECH) and health reform opportunities is critical to create a more optimal environment for doctors and patients to share and use the best available information for high-quality and cost-effective health decisions. The Department of Health and Human Services' (HHS) emerging national strategy for quality improvement offers an opportunity to align health IT efforts with the nation's health priorities.

2. Implement a trust framework that addresses a full complement of protections based on FIPs and that is implemented through both policy and technology.

- The starting place is a broad framework of privacy principles based on FIPs and adopted by ONC. It must be used holistically to develop more detailed policies, practices, and technical approaches to achieve the PCAST vision for an information-rich health ecosystem.

3. Accelerate standards adoption through bottom-up and top-down approaches.

- Most health care is local, and many multi-institution systems that serve particular localities already exist. However, to ensure interoperability among those regional systems as they grow, some national standards must be adopted in the market. We agree with PCAST's desire to accelerate the nation's use of common exchange standards.
- The path toward this goal starts with the imperfect data of today, and takes into account the varying capabilities of a wide array of health care settings, ranging from sophisticated environments in large integrated delivery systems to small office practices. The challenge is to build from the simplest and most widely adopted solutions that can work in the real world.
- The question is not whether to work from top up or bottom down; both are necessary. The question is which problems are most amenable to which type of solution.

- As the Direct Project has correctly prioritized, a critical starting point is to identify and specify common and implementable standards for secure transport.
- The government's initiative to provide a blue button has provided an example of how giving patients access to downloads of their information available now in the most basic but readable form as a text file, is a building block for individual participation and private-sector innovation.
- Necessary accelerants for greater standardization and adoption will benefit from coordinated efforts to promote and incentivize the sharing of data in its existing forms to improve a patient's care. The standards chosen under Stage 1 Meaningful Use provide a solid foundation.

4. Create pilot projects and prototypes to test some of the innovative elements of the PCAST report and to facilitate rapid standards adoption.

- ONC can support progress by developing pilot projects and prototypes with existing grantees, particularly the Beacon communities and State HIE efforts, and in coordination with other government partners, such as the Center for Medicare and Medicaid Innovation. Promising areas for exploration include the following:
  - Evaluating the potential opportunities and criteria for using metadata in direct communications for sharing information about permissions or other categories of information.
  - Exploring how distributed models for quality reporting and quality improvement that enable the sharing of aggregate data could be used to make progress towards specific health objectives.

5. Commit to further evaluation of the PCAST proposal in the context of the lessons we have learned from past efforts.

- Based on past lessons learned and the vast heterogeneity and asymmetry of US health care, we believe that an optimal approach will include the following:
  - Ensure that policy goals shape technology choices, including standards and architecture, and not vice versa.
  - Work in a series of simple, progressive steps that create value for participants.
  - Design for the simplest sites of care.
  - Always default to sharing what information is available, in the form it is available if it can improve the care of a patient, with a preference, but not a requirement, for improved structure in exchange.
  - Adopt well-tested standards and mechanisms.
  - Keep data as close as possible to where it is captured, and share only as needed.

    - Assume that information need not be centralized in order to be shared.

- In addition, many past experiences offer important lessons learned, which should be addressed by ONC in evaluating the report's recommendations for granular metadata, and permissions controls catalogued and moderated by a few national DEAS. Questions to consider in this analysis include the following:
    - To what extent has a DEAS-like model been implemented in other heterogeneous industries?
    - How can consumers be given the tools and insight necessary to make granular privacy decisions beyond the default settings without potentially unleashing unwanted disclosure? How would this be implemented in provider care settings?
    - What approaches could be used to audit the implementation of granular privacy settings in a manner that is scalable?
    - What guidelines should be in place to inform efforts to implement granular controls so that they provide individuals with greater control over their information? How can these controls be implemented by providers in a wide variety of care settings?
    - Who is in the best position to manage consumer expectations and understanding of their rights and responsibilities with regard to managing privacy settings?
    - What are the risks of establishing a limited number of access points for national health information? Are these risks different than those for a limited number of repositories of health information?
    - Would a DEAS-like model require a single authority to monitor the attributes of all users?
    - Who would maintain the infrastructure needed to support the DEAS? How would the rules of the road be determined and who would determine them?
    - What are the privacy and security risks of the DEAS model and how can they be minimized?
    - How would requirements for tethering permissions directly to data elements impact innovation?

I. Introduction

The President's Council of Advisors on Science and Technology (PCAST) report *Realizing the Full Potential of Health Information Technology to Improve Healthcare for Americans*[1] envisions an information-rich health ecosystem. Like PCAST, we seek to accelerate the use of modern information tools to improve health outcomes, increase the cost-effectiveness of care, and encourage innovation while protecting privacy.

Markle Connecting for Health, a public-private collaborative of more than 100 organizations across the spectrum of health care and information technology, appreciates the opportunity the Office of the National Coordinator for Health Information Technology (ONC)[2] has provided for commentary on this very important report.

Our comments fall into three parts: We start by addressing the basic parameters of the PCAST vision, one that has many parallels to the Markle Connecting for Health Common Framework (Markle Common Framework). Next we provide input on some of the specific recommendations of the report, and here our comments fall into two categories: As in all of our past work, we emphasize the importance of starting with clear goals and a policy framework to guide technology choices and solutions, and we consider some of the novel technology approaches that PCAST proposes and their implications for the vast, heterogeneous environment that characterizes US health care today. Lastly, based on the collective experience of our broad collaboration, which has worked together on solutions to health IT challenges for nearly a decade, we provide ONC a set of forward-looking recommendations that we believe can accelerate the use of health IT to improve health outcomes and cost effectiveness while protecting privacy.

---

1 President's Council of Advisors on Science and Technology. "Realizing the Full Potential of Health Information Technology to Improve Healthcare for Americans: The Path Forward," December 2010. Accessed on the Web January 8, 2011: http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-health-it-report.pdf.

2 Office of the National Coordinator for Health Information Technology; Health Information Technology; Request for Information Regarding the President's Council of Advisors on Science and Technology (PCAST) Report Entitled "Realizing the Full Potential of Health Information Technology To Improve Healthcare for Americans: The Path Forward." 75 Federal Register 237 (December 10, 2010), pp. 76,986–76,987.

A Vision Supported by the Markle Connecting for Health Common Framework

The PCAST report offers a compelling vision for an information-rich health care system that we support. The Markle Common Framework is aligned with and supportive of the PCAST vision for:

- **A nationwide capability for secure health information exchange using the Internet, not a new network.** We agree with the PCAST report that health information exchange should be accomplished without ripping and replacing existing structures. We believe that information sharing can be accomplished by using Internet protocols without a need for a novel national infrastructure. Any proposed model for health information exchange to be used in the near term should rely on the current capabilities for ensuring the secure transfer of information.
- **A distributed network for information-sharing.** The PCAST vision for a distributed network is supported and shared by the Markle Connecting for Health Common Framework.[3] Local providers who have relationships with patients are in the best position to carry out their patients' wishes for the information to be shared or kept private. A distributed approach leaves clinical data in the control of the providers or entities that have this direct relationship with the patient, and leaves judgments about who should and should not see patient data in their hands.
- **A model for linking patient information across sites of care using *existing identifiers***. The PCAST report proposes information sharing without the use of a national health identifier to link patient records across sites of care. We support this conclusion and similarly support the use of distributed networks enabled by indices to locate patient information across sites of care using existing identifiers.
- **An approach to technology that emphasizes innovation and a diversity of solutions to support broad participation and new entrants.** PCAST's emphasis on innovation is well placed and critically important. The goal of creating a viable platform for innovation and broad participation is critical to the rapid adoption and evolution of IT. We emphasize that standards requirements and protocols be limited to those essential for widespread exchange of health information in an asymmetric environment. This approach creates low barriers to entry, encourages innovation, reduces costs, and maximizes competition for privacy and security protections.

---

3 Markle Connecting for Health. "Common Framework for Private and Secure Information Exchange," 2005. Accessed on the Web January 15, 2011: http://www.markle.org/health/markle-common-framework/connecting-professionals.

Markle Connecting for Health. "Common Framework for Networked Personal Health Information," 2007. Accessed on the Web January 15, 2011: http://www.markle.org/health/markle-common-framework/connecting-consumers.

- **A comprehensive set of privacy and security practices to support trust in information sharing.** PCAST's explicit recognition for the need to have a complete privacy and security framework[4] is vitally important, and one that we strongly support.
- **A universal exchange language for exchanging health information securely over the Internet.** The need for standards for using Internet protocols for secure exchange of health information is a foundational requirement, and one that we have long supported.
- **Population health improvement and analysis using distributed networks.** We support PCAST's vision for a distributed approach to population health analysis to improve health and health care. A cutting-edge health information environment should be comprised of and leverage a large network of distributed data sources that enables analysis while protecting privacy and security, without requiring the creation of large national central repositories of identifiable health information.

The Markle Connecting for Health collaborative has described these attributes in greater detail in the Common Framework for Private and Secure Information Exchange (2006), the Common Framework for Networked Personal Health Information (2008), and Decision-Making for Population Health "First Principles" (2007).[5]

The Path Forward: Moving from Vision to Implementation

The potential of networked information to achieve measurable health improvement is enormous. Access to and use of critical information—recent lab values, home monitoring results, discharge summaries, medication fill histories—is the lifeblood of health improvement.

But we know that this critical information is often not available when and where it is needed. For instance, primary care physicians only have hospital care summaries one third of the time when they first see recently discharged patients.[6] Also, there is inconsistent delivery of proven care, with adults estimated to receive on average only 55 percent of the care recommended by

---

4 The report states, "To build and maintain the public's trust in health IT requires comprehensive privacy and security protections that are based on Fair Information Practices and [that] set clear rules on how patient data can be accessed, used and disclosed, and that are adequately enforced." President's Council of Advisors on Science and Technology. "Realizing the Full Potential of Health Information Technology to Improve Healthcare for Americans: The Path Forward," December 2010: p. 4.

5 Available at http://www.markle.org/health/markle-common-framework.

6 A review of studies found that in the first visit after discharge, summaries of hospital care were only available to primary care physicians 12 to 34 percent of the time. See Kripalani, S., F. LeFevre, et al. "Deficits in Communication and Information Transfer Between Hospital-Based and Primary Care Physicians." 2007. JAMA 297:831-841.

evidence-based best practices.[7] In addition to these information gaps, basic privacy and security protections have not been met. A recent survey found that 33 percent of health care organizations had at least one known case of medical identity theft.[8] And even when gaps are identified, 43 percent of organizations said that it took up to six months to rectify, and 33 percent said it took them between six months and one year to correct.[9]

We share PCAST's sense of urgency and desire to catalyze improvements in health care quality, safety, and cost-effectiveness with broad-scale implementation of health information technology.

7 McGlynn, E., S. Asch, J. Adams, J. Keesey, J. Hicks, A. DeCristofaro, and E. Kerr. "The Quality of Health Care Delivered to Adults in the United States," 2003. *The New England Journal of Medicine,* 348 (26):2635-2645.

8 Healthcare Information and Management Systems Society. "2010 HIMSS Security Survey." November 3, 2010. Accessed on the Web January 5, 2011: http://www.himss.org/content/files/2010_HIMSS_SecuritySurvey.pdf.

9 Ibid.

II. Key Findings and Commentary

In the following section, we identify areas ONC may want to consider for further development and analysis. These findings are based on three foundational principles that have guided our work for nearly a decade and offer grounding for our understanding of many of PCAST's proposals:

A. Adopt a trust framework based on Fair Information Practices (FIPs).

B. Protect privacy while enabling greater information sharing through simple, progressive steps using well-tested standards and technology.

C. Focus on rapid learning and better decision making by many.

A. Adopt a trust framework based on Fair Information Practices (FIPs).

Both the public and doctors agree on the importance of privacy and security practices as a priority of health IT. A 2010 Markle survey found that more than 80 percent of the public and doctors consider privacy safeguards an important requirement for health IT incentives.[10]

Our surveys also have made clear that Americans expect benefits of health IT if appropriate safeguards are in place to protect their personal information. We need to earn and keep the public's trust that personal health information will be protected as it is shared so we can move toward the nation's goals for better quality health care.

Critically, however, trust cannot be achieved with technology alone.

Sharing information is mostly about trusting relationships between entities and institutions, not machines. Interoperable standards by themselves do not move information. Pushing the SEND button requires that the people who need to share information trust each other, understand and implement the necessary protections for the information they hold, and know that the information policies in place will be upheld and enforced in the event of a breach.

Our experience suggests that a path forward to meet these goals is through the adoption of a trust framework that couples strong policies and privacy practices with technology.

---

[10] Markle Foundation. *New Markle Survey Finds US Public and Doctors Alike Support 'Blue Button' for Downloading Health Information*. October 7, 2010. Accessed on the Web January 15, 2010: http://www.markle.org/news-events/media-releases/new-markle-survey-finds-us-public-and-doctors-alike-support-blue-button-d.

Any information sharing effort should adopt a trust framework and then translate it into practice by specifying the necessary policies, practices, and technology choices that will implement it.

A framework for trust must manifest in a multifaceted approach that addresses a full complement of protections based on Fair Information Practices (FIPs) and be implemented through both policy and technology. In our experience, the specific privacy policies and practices articulated in the Markle Common Framework benefited greatly by being deeply rooted in nine privacy principles based on FIPs (See Appendix). These foundational principles include openness and transparency, purpose specification, collection limitation and minimization, use limitation, individual participation and control, data integrity and quality, security safeguards and controls, accountability and oversight, and remedies.[11] Government initiatives have also used the FIPs to guide information sharing efforts for almost 40 years, and the Department of Commerce recently recommended that they be used to protect online consumers.[12] When applied together, these principles yield a set of privacy practices and technology approaches that add up to an integrated and comprehensive framework of protections. Elevating certain principles over others, however, will simply weaken the overall trust framework. We believe it is essential to apply them upfront, in a thorough and comprehensive manner and not as an afterthought, when contemplating any new information sharing.

For example, a policy-driven approach means that when data are needed for public health, research, quality, or some other authorized use, the purpose must be specified and only the data necessary for achieving that purpose is shared. Data use and sharing are made transparent through immutable audit logs. Data stay as close as possible to where they are captured, and are shared according to specific needs and with specific purpose and authorizations. Without a policy framework in place, technology-driven approaches inevitably result in de-facto policies, often misaligned with or inadaptable to policy goals that are established after the fact.

We suggest balancing consent mechanisms with other comprehensive policy and technology protections to support privacy, including oversight and accountability.

The objective to give consumers greater control over their information is the right one, and one that we support. But a privacy approach that rests predominately on obtaining consumer consent can unintentionally result in weak protection for consumers if it overlooks the importance of systems, rules, and processes to protect personal health information. While

---

[11] Markle Connecting for Health. "Common Framework: The Architecture for Privacy in a Networked Health Information Environment." 2005. Accessed on the Web January 15, 2011: http://www.markle.org/sites/default/files/P1_CFH_Architecture.pdf.

[12] Department of Commerce Internet Policy Task Force. "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework." 2010. Accessed on the Web January 10, 2011: http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf.

consent is an important element of a complete package of privacy protections, it is inadequate if relied upon as the singular privacy pillar for networked health information.[13] An over-reliance on consent can have unintended consequences and place undue burden on consumers.

One reason that consent should be bolstered by other protections is that it may not be possible for patients to make informed consent decisions about all of the granular data elements across all of the entities that hold their data in an environment as complex as health care. Health information streams are highly complex and involve an ever-growing number of people. Almost 150 different people (including doctors, nursing staff, X-ray technicians, and billing clerks) access at least part of a patient's health record during a single hospital visit,[14] and that there are roughly 600,000 entities with the ability to access at least some part of a patient's information.[15] It is unlikely that most medical professionals understand the role of each of these actors, and even less likely that consumers can understand. To add complexity, this cast of actors is likely to change over time, and a patient's privacy preferences will likely change as well. In fact, many of the factors that determine a patient's preferences— including their health status, trust relationships, family situation, and geographic location—shift with the regular ebb and flow of a person's life; moreover, they are unpredictable and will likely not be taken into consideration when making initial decisions about privacy preferences. For the foreseeable future, it is hard to imagine how most consumers could provide meaningful fine-grained consent about all of their data because it is too difficult to be fully informed about exactly what data is being collected, under what circumstances it will be shared, and how it will be protected, both currently and in future uses. This reality makes all the more important to have in place a complete set of privacy and security policies and practices.

B. Protect privacy while enabling greater information sharing through simple, progressive steps using well-tested standards and technology.

We share the goal of wanting to make rapid progress toward a health care system where information is more commonly used to drive better care, and privacy and security are protected. However, we believe the path toward this goal starts with the imperfect data of today, and takes into account the varying capabilities of a wide array of health care settings, ranging from sophisticated environments in large integrated delivery systems to small office practices. The

---

[13] Markle Connecting for Health. Common Framework: The Architecture for Privacy in a Networked Health Information Environment," 2005. Accessed on the Web January 15, 2011: http://www.markle.org/sites/default/files/P1_CFH_Architecture.pdf.

[14] "Standards for Privacy of Individually Identifiable Health Information." 65 Federal Register 250 (December 28, 2000). pp. 82461-82510.

[15] Los Angeles Times. "At risk of exposure: In the push for electronic medical records, concern is growing about how well privacy can be safeguarded." June 26, 2005. Accessed on the Web January 8, 2011: http://articles.latimes.com/2006/jun/26/health/he-privacy26.

challenge is to build from the simplest and most widely adopted solutions that can work in the real world.

The goal of developing a universal exchange language for secure exchange using the Internet is foundational to these efforts. In order to move in this direction, ONC should focus on deploying well-tested and widely used standards and technology that can be implemented within a comprehensive privacy and security framework of policies and practices. The standards chosen under Stage 1 Meaningful Use provide a solid foundation. Yet because trust is primarily an attribute of entities or participants, rather than of software or data, progress will be made primarily through an expanding network of trusted participants, rather than being driven through novel networks or infrastructures.

Moreover, improving the reasons to share data, namely achieving quality and safety goals, can help create an incentive to improve data quality and adopt more standardization—something the mere specification of standards can never achieve on its own. Necessary accelerants for greater standardization and adoption will benefit from coordinated efforts to promote and incentivize the sharing of data in its existing forms to improve a patient's care.

Lessons Learned: History Offers a Cautionary Tale

As ONC evaluates how best to move forward, there are important lessons to learn from past efforts to use IT to improve information sharing and increase data protections. First, large scale IT upgrades and novel standards, even when mandated, run significant risk of failure. Projects like the FBI's Virtual Case File,[16] the FAA's Air Traffic Control modernization,[17] or the IRS's Electronic Fraud Detection System[18] show that attempts to provision sudden, massive upgrades are high-risk ventures that often fail to deliver any of the imagined benefits. A particularly relevant example is the Government Open Systems Interconnection Profile (GOSIP) effort of 1986,[19] which mandated the adoption of a particular form of networking technology that would replace core Internet technologies. GOSIP became a required Federal Information Processing Standard in 1990 (FIPS 146-1), and included both conformance and interoperability testing by vendors. Despite being federally mandated, internally consistent, conformant, and interoperable, GOSIP was largely a failure because few organizations in the field actually

---

16 Dizard, Wilson III, 2005. Sentinel System will Replace FBI's Virtual Case File. Washington Technology; Glenn A. Fine (Inspector General, U.S. Department of Justice). 2/3/2005. Statement on The Federal Bureau of Investigation's Trilogy Information Technology Modernization Project before the Senate Committee on Appropriations, Subcommittee on Commerce, Justice, State and the Judiciary.

17 Cone, Edward. 2002. The Ugly History of Tool Development at the FAA. Baseline Magazine, 2002; Glass, Robert L. 1997. Software Runaways: Monumental Software Disasters. Prentice Hall.

18 Linda Rosencrance. "IRS: Lack of fraud detection system cost nearly $300M." Computerworld. July 18, 2006.

19 National Institute of Standards and Technology. "Standards For Open Systems: More Flexibility For Federal Users." 1995. Accessed on the Web January 8, 2010: http://www.itl.nist.gov/lab/bulletns/archives/b595.txt.

adopted it. After ten years of work, it was replaced in 1995 by a rewritten Federal standard (FIPS 146-2) that allowed use of standard Internet protocols.

In order to succeed, IT procurement and development of standards need to take into account the progressive nature of standards adoption and concentrate on the most basic issue first, which is making it easier to share data in its current form while protecting privacy and security. When standards have achieved universal adoption, it has been through activity and use in the private sector because they help meet the needs of users. The Web took off when innovators like those at the University of Illinois built a browser through their own innovation to meet the objective of making the Internet a platform for sharing information, not because the government specified the standards and certified the browser.

Second, attempts to attach permissions to data or to entirely rely on novel technology to solve a complex policy problem in other sectors offer important lessons. For example, experience with digital rights management (DRM) and the Platform for Privacy Preferences[20] (P3P) offer important insights whose implications must be further understood in efforts to tether privacy permissions to data in health care. The successful use of technologies that tether rules to data remains elusive particularly in instances where the technology was used to enforce a set of rights and obligations. For example, DRM has failed to prevent or inhibit piracy of copyrighted works,[21] and has had the unintended consequences of resulting in limitations on legitimate use and stifling innovation.[22] Critically, both data users and creators have not been able to get the protections and usability that they expect.

At the same time, communicating privacy preferences as metadata expressed in Extensible Markup Language (XML) could have real value when part of a comprehensive approach to privacy and security. For example, this approach could potentially be used to communicate about permissions across sites of care, while understanding that each entity will need the flexibility to respect these permissions with the policies and tools that best meet their needs. More importantly, the entities and data holders, and not the metadata tags, would be positioned to act as the enforcers and arbiters of who can or cannot access the shared information.

Additionally, initial experience has shown that the technologies needed to execute Web-like search for distributed, encrypted information are extremely slowed down by the heavy

---

[20] Ari Schwartz, Center for Democracy and Technology. "Looking Back at P3P: Lessons for the Future." November 2009. Accessed on the Web January 8, 2011: http://www.cdt.org/files/pdfs/P3P_Retro_Final_0.pdf

[21] Electronic Frontier Foundation. "Digital Rights Management: A failure in the developed world, a danger to the developing world." March 2005. Access on the Web January 8, 2011: http://www.eff.org/wp/digital-rights-management-failure-developed-world-danger-developing-world

[22] Center for Democracy & Technology. "Evaluating DRM: Building a Marketplace for the Convergent World." September 7, 2006. Accessed on the Web January 8, 2011: http://www.cdt.org/files/pdfs/20060907drm.pdf.

computation involved.[23] For example, a general search for a single word could take tens of seconds, and searches with two or more words could increase the search time exponentially. A recent study found that this type of search mechanism is "unacceptably slow" and not yet viable for large-scale use.[24]

Finally, more analysis is needed to learn how granular controls might be used effectively to truly provide individuals with greater control over their information and to learn more about how they can be successfully implemented by providers in care settings.[25] Early assessments of their use in social networking indicate that people are not always able to use the controls as they had intended.[26]

Indexing Distributed Health Information

PCAST recognizes that distributed networks require services that can locate patient records. Several important choices are key for implementing these services so that they meet the dual goals of protecting privacy while enabling information sharing. These choices combined with the cautionary tale of novel national infrastructure weighed heavily on the approach that we took in establishing the Markle Common Framework. We discuss a few of the key elements chosen to minimize exposure of personal data in order to explain our comments and recommendations:

- **Information sharing is a two-step process.** Sharing information effectively calls for a two-step process, which involves active decision making for each exchange of information. This process was implemented in the Markle Common Framework through a Record Locator Service where a requester first queries a directory and gets pointers to authorized records. Then, each provider holding records has the discretion to disclose, depending on the decisions that providers have made with their patients. Thus, there are two decisions to be made locally: whether to index and whether to share. This two-step process was developed in part to assure that the system would not lead to any increased exposure of personal health information while at the same time providing some early value by establishing a way to readily and efficiently locate records in order to improve

---

[23] David Talbot. "Searching an Encrypted Cloud." *Technology Review*. November 11, 2009. Accessed on the Web January 8, 2011: http://www.technologyreview.com/computing/23929/.

[24] Abel Avram. "A Step Toward Better Cloud Security: Searchable Encryption." *InfoQ*. January 14, 2010. Accessed on the Web January 8, 2011: http://www.infoq.com/news/2010/01/Cloud-Searchable-Encryption.

[25] US Department of Health and Human Services, Office of the National Coordinator for Health Information Technology, Privacy and Security Tiger Team of the Health Information Technology Policy Committee. "Transcript of the Consumer Choice Technology Hearing: Cutting-Edge Consumer Choice Technology." June 29, 2010. Accessed on the Web January 8, 2011: http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11673_945903_0_0_18/Consumer-Choice-Technology-Hearing-062910.pdf.

[26] Danah Boyd "SXSW Keynote: Making Sense of Privacy and Publicity." SXSW, Austin, Texas. March 13, 2010. Accessed on the Web January 8, 2011: http://www.danah.org/papers/talks/2010/SXSW2010.html.

health care quality and patient safety, even in environments where electronic records are unevenly available. For example, if a provider restricts records as a matter of policy or as a matter of patient choice, that provider need not index the patient in the directory and, if the provider does participate in an index, they need not respond to a request to share.

- **Indices are local and regional.** Many of the risks of a large centralized repository of health information can be significantly reduced with a distributed model that leaves judgments about who should and should not see patient information in the hands of the patient and the clinicians and institutions that are directly responsible for the patient's care. While the DEAS calls for a distributed model in which health information is stored locally, it creates a single access point to query all national information. Would this single access point create a significant vulnerability? The Markle Common Framework did not contemplate a large central index or national query capability in favor of Record Locator Services that were local and regional to reduce the risk of large-scale failure by simply reducing the number of people who would be affected by an unintended disclosure.
- **Indices are optimized to reduce unauthorized disclosure.** The potential for unauthorized disclosure of personal health information can be minimized by limiting indices to demographic data and not allowing the inclusion of clinical data. Including even seemingly small pieces of clinical information or metadata in a widely queriable index can pose serious privacy risks because this information can be aggregated across multiple sources to reveal a complete picture of an individual's health status. PCAST's proposal takes this vulnerability into account by introducing steps to encrypt all metadata and only expose data elements to searchers authorized by applicable privacy rules and policies. While encryption is one part of an approach to protect metadata, it is not foolproof. In particular, encryption is essential to prevent eavesdropping (so-called "man in the middle" attacks), and to prevent unauthorized recipients from viewing the data. However, encryption does not protect from misuse by authorized recipients. Many breaches, both in health care and other sectors, result from users who unintentionally or fraudulently expose information they are authorized to access. Notable examples, including Equifax and SIPRnet, show that the risk from these authorized "attackers" is large. Thus, while we support good use of encryption, including encryption of data at rest, no amount of encryption, no matter how sophisticated or pervasive, can guard against insider or "authorized" user risk. The Markle Common Framework advises against keeping any clinical information in indices on the network, and advises against release of data, even in encrypted form, to otherwise unauthorized participants. The decision on the part of a data holder to release a piece of data to another organization is a decision to trust the data recipients.

C. Focus on rapid learning and better decision making by many.

Our goal is an information-driven health care ecosystem, where aggregate information can be gathered and used in a timely way to show what works, alert decision makers about emerging

trends, and help clinicians make the best decisions possible to improve care while protecting privacy.

One of the greatest strengths of the PCAST report, among others mentioned previously, is its vision for robust distributed population-level analysis and quality measurement that leverages digitized and networked health information. We believe that ONC is in a good position to take steps toward this vision today by encouraging the adoption of research methods and tools that enable distributed analysis of aggregate clinical data where data are cleaned and analyzed in a common way at the source before being sent in a standardized summary format.

For example, the Meaningful Use Stage 1 requirements for quality reporting, which rely on the submission of de-identified aggregate summary results, provide a promising model. It leverages distributed data sources while minimizing privacy risks by eliminating the need to share personally identifiable information.

The PCAST recommendations go further in supporting greater innovation and enhanced methods for quality reporting and improvement, which can take advantage of many new and varied data sources to inform decision-making. We agree that there is enormous potential for innovation in this area to help drive toward a more nimble and effective quality improvement ecosystem.

We have highlighted other areas of population health that can be bolstered by leveraging decentralized electronic data through the use of health IT in past work.[27] In the areas of comparative effectiveness research, post-market drug surveillance, and public health surveillance, there are projects that begin to demonstrate success using distributed methods of data analysis for a range of research and public health questions, including the following:

- Distribute model for flu surveillance[28]
- DARTNet for comparative effectiveness research[29]
- FDA Sentinel Initiative for monitoring drug safety[30]

---

[27] Carol C. Diamond, Farzad Mostashari, and Clay Shirky. "Collecting and sharing data for population health: A new paradigm."*Health Affairs*. 2009 March 28(2): 454-466.

[28] President's Council of Advisors on Science and Technology. "Realizing the Full Potential of Health Information Technology to Improve Health care for Americans: The Path Forward" December 2010: p. 64.

[29] US Agency for Health care Research and Quality (AHRQ) "Distributed Network for Ambulatory Research in Therapeutics." July 28, 2009. Accessed on the Web January 8, 2011: http://effectivehealthcare.ahrq.gov/index.cfm/search-for-guides-reviews-and-reports/?pageaction=displayproduct&productid=317; Wilson D. Pace, Maribel Cifuentes, Robert J. Valuck, Elizabeth W. Staton, Elias C. Brandt, and David R. West. "An electronic practice-based network for observational comparative effectiveness research." *Ann Intern Med*. 2009 Sep 1;151(5):359-60. Accessed January 8, 2011: http://www.annals.org/content/151/5/338.full.

To varying degrees, the basic approach taken by these examples means that data are cleaned and analyzed in a common way at the source before being sent in a standardized summary format. The data could be made accessible for analysis by different authorized entities across a network without requiring that each entity obtain a local copy of all of the detailed underlying data to conduct the analysis. Trust across the network is enabled by agreement on a key set of information policies and practices to protect data. This serves to minimize the exposure of the underlying data, enables feedback loops to exist natively, and saves the original holders of the data from having to answer multiple separate requests for the same data sets.

One important underlying example of how appropriate policies can reduce privacy risks includes requiring reporting of summary level aggregate data while leaving personally identifiable information to be stored and controlled locally. Instead of revealing all of the detail in a patient's record, this model reveals only summarized data (e.g., counts, numerators and denominators, or key results) and limits the data collection to the minimum needed to answer specific population level questions. It is critical to note that this kind of fundamental policy and practice would be highly unlikely in an environment where consent was relied upon as the sole mechanism to protect privacy. Only by contemplating the full framework of policies, including collection minimization and use limitation, can we expect to have a full complement of protections acting together for patients.

---

[30] US Food and Drug Administration (FDA) "Access to Electronic Health Care Data for More Than 25 Million Lives." July 2010. Accessed on the Web January 8, 2011: http://www.fda.gov/downloads/Safety/FDAsSentinelInitiative/UCM233360.pdf.

III. Recommendations

1. Set clear health objectives to guide health IT investments.

The overarching, nationwide goals of health IT investments should be to improve health care quality, reduce growth in costs, stimulate innovation, and protect privacy in alignment with clear priorities, such as those identified through the National Health Care Quality Strategy and Plan.

Meaningful objectives with appropriate incentives create an imperative to share information, which in turn creates demand for better tools and standards. Critically, however, the converse is not true. More standardized data alone creates no incentive to share.

The report starts with this core challenge: how can we improve the quality of health care and reduce its cost? It is the right starting place. Example after example describe how health IT can be used to improve care. It is the *use* of information that is key. Information use enables a consumer to play an active role in maintaining health and getting the best care, prevents a patient from suffering a medical error, helps a clinician prescribe the right treatment at the right time, allows a care team to coordinate care in the most effective and affordable way, and benefits efforts to improve quality, accelerate research, and advance public health.

Improving interoperability and advancing health IT are foundational building blocks, but are just part of the equation for creating an environment that rewards information use. The challenge of thinking of IT as a tool to improve quality and control costs will require serious attention to transforming the US health care system as a whole, rather than simply computerizing the current setup.

Government leadership is needed to focus the health sector on encouraging the effective use of information to reach specific health objectives. Starting with clear goals and metrics will help maximize the benefits of government initiatives and increase the likelihood that technology will be used in service of health objectives. The Meaningful Use Rule, under the Health Information Technology for Economic and Clinical Health Act (HITECH), marks a critical beginning in this effort. ONC and CMS have laid a promising foundation for encouraging the effective use of health information to improve patient care. Government has the opportunity to add crucial visibility to key health objectives for the nation. For example, a declaration of specific targets—such as preventing one million heart attacks and strokes and cutting medication errors and reducing administrative burdens by half—could add this visibility and focus to future stages of Meaningful Use.

The deliberate and strategic alignment of current HITECH and health reform opportunities, including requirements for Accountable Care Organizations, is critical to create a more optimal

environment for doctors and patients to share and use the best available information for high quality and cost effective health decisions. HHS's emerging national strategy for quality improvement also offers an opportunity to align health IT efforts with the nation's health priorities.

2. Implement a trust framework that addresses a full complement of protections based on FIPs and that is implemented through both policy and technology.

A broad framework of privacy principles based on FIPs and adopted by ONC[31] is a good starting place. It must be used holistically to develop more detailed policies, practices and technical approaches to achieve the PCAST vision for an information-rich health ecosystem. As discussed throughout this commentary, the specification, oversight and enforcement of a complete framework are necessary for trust. Trust cannot be imposed on a system through technology or national infrastructure; it must evolve through participation and experience as well as the appropriate incentives to use information to achieve the required quality and safety objectives.

3. Accelerate standards adoption through bottom-up and top-down approaches.

Most health care is local, and many multi-institution systems that serve particular localities already exist. However, to ensure interoperability between those regional systems as they grow, some national standards must be in place. We agree with PCAST's desire to accelerate the nation's use of common exchange standards.

The path toward this goal starts with the imperfect data of today, and takes into account the varying capabilities of a wide array of health care settings, ranging from sophisticated environments in large integrated delivery systems to small office practices. The challenge is to build from the simplest and most widely adopted solutions that can work in the real world.

The question is not whether to work from top up or bottom down; both are necessary. The question is which problems are most amenable to which type of solution.

As the Direct Project[32] has correctly prioritized, a critical starting point is to identify and specify common and implementable standards for secure transport. This represents very important initial work that cannot be overlooked. Similarly, the government's implementation of a blue button has provided an example of how giving patients access to downloads of their information

---

[31] US Department of Health and Human Services, Office of the National Coordinator for Health Information Technology, NHIN Work Group of the Health IT Policy Committee. "HIE Trust Framework: Essential Components for Trust." April 21, 2010. Accessed on the Web January 8, 2011: http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11673_911635_0_0_18/Lansky_NHINWG_Recs_HIE_Trust_Framework042110UPDATE.ppt

[32] See http://directproject.org/.

available now in the most basic but readable form as a text file, is a building block for individual participation and private-sector innovation.[33] This basic capability has broad support and, if continued as a priority of public-private health IT efforts, will likely increase demand for more standardized formats.[34]

Necessary accelerants for greater standardization and adoption will benefit from coordinated efforts to promote and incentivize the use, and therefore sharing of data in its existing forms to improve a patient's care. The standards chosen under Stage 1 Meaningful Use provide a solid foundation.

4. Create pilot projects and prototypes to test some of the innovative elements of the PCAST report and to facilitate rapid standards adoption.

ONC can support progress by developing pilot projects and prototypes with existing grantees, particularly the Beacon communities and State HIE efforts, and in coordination with other government partners, such as the Center for Medicare and Medicaid Innovation. Both pilots and prototypes provide an opportunity for ONC to harness and analyze early experience in using emerging technologies and to address challenges that may stand in the way of broad adoption.

Promising areas for exploration include the following:

- Evaluating the potential opportunities and criteria for using metadata in direct communications for sharing information about permissions or other categories of information. Tagging information with proper criteria may help facilitate the meaningful exchange of existing information. This information could be effectively exchanged in a human-readable form or intelligently parsed by the receiver based on the receiving organizations capabilities and needs.
- Testing how distributed models for quality reporting and improvement that enable the sharing of aggregate data could be used to make progress towards specific health objectives. The open source population health reporting prototype, popHealth[35] is a promising platform for work in this area.

---

[33] Aneesh Chopra, Todd Park, and Peter L. Levin. "'Blue Button' Provides Access to Downloadable Personal Health Data." The White House, Office of Technology and Policy Blog. October 7, 2010. Accessed on the web January 8, 2011: http://www.whitehouse.gov/blog/2010/10/07/blue-button-provides-access-downloadable-personal-health-data.

[34] Markle Foundation, "Policies in Practice: The Download Capability; Common Framework for Networked Personal Health Information, August 31, 2010. Accessed on the web January 12, 2011: http://www.markle.org/publications/1198-policies-practice-download-capability

[35] See http://projectpophealth.org/index.html.

5. Commit to further evaluation of current proposals in the context of the lessons we have learned from past efforts.

Based on these lessons learned and the vast heterogeneity and asymmetry of US health care, we believe that an optimal approach will:

- Ensure that policy goals shape technology choices, including standards and architecture, and not vice versa.
- Work in a series of simple, progressive steps that create value for participants.
- Design for the simplest sites of care.
- Always default to sharing what information is available if it can improve the care of a patient, in the form it is available, with a preference, but not a requirement, for improved structure in exchange.[36]
- Adopt well-tested standards and mechanisms.
- Keep data as close as possible to where it's captured, and shared as needed.
- Assume that information need not be centralized in order to be shared.

In addition, many past experiences offer important lessons learned which should be addressed by ONC in evaluating the report's recommendations for granular metadata and permissions controls catalogued and moderated by a few national Data Element Access Services (DEAS).[37] Questions to consider in this analysis include the following:

- To what extent has a DEAS-like model been implemented in other heterogeneous industries?
- How can consumers be given the tools and insight necessary to make granular privacy decisions beyond the default settings without potentially unleashing unwanted disclosure? How would this be implemented in provider care settings?
- What approaches could be used to audit the implementation of granular privacy settings in a manner that is scalable?
- What guidelines should be in place to inform efforts to implement granular controls so that they provide individuals with greater control over their information? How can these controls be implemented by providers in a wide variety of care settings?

---

[36] For example, a well marked-up XML document with appropriately tagged fields would be far better than a JPEG of a doctor's handwritten notes, but such an image would, in turn, be better than nothing.

[37] President's Council of Advisors on Science and Technology. "Realizing the Full Potential of Health Information Technology to Improve Healthcare for Americans: The Path Forward," December 2010: pp. 43; 45-52.

- Who is in the best position to manage consumer expectations and understanding of their rights and responsibilities with regard to managing privacy settings?
- What are the risks of establishing a limited number of access points for national health information? Are these risks different than those for a limited number of repositories of health information?
- Would a DEAS-like model require a single authority to monitor the attributes of all users?
- Who would maintain the infrastructure needed to support the DEAS? How would the rules of the road be determined and who would determine them?
- What are the privacy and security risks of the DEAS model and how can they be minimized?
- How would requirements for tethering permissions directly to data elements impact innovation?

Appendix: Markle Connecting for Health Common Framework Core Privacy Principles

Openness and Transparency	Communicate policies to participants and individuals.
	Provide privacy notices to consumers.
	Involve stakeholders in developing information sharing policies.
Purpose Specification	Specify the purpose of the data collection effort clearly and make it narrowly suited to the need.
Collection Limitation and Minimization	Assure that only data needed for specified purposes are being collected and shared.
Use Limitation	Establish processes to ensure that data are only used for the agreed upon and stated purposes.
	Establish what data access is permitted for each user.
Individual Participation and Control	Allow individuals to find out what data have been collected and who has access, and exercise meaningful control over data sharing.
	Give individuals access to information about them, and the ability to request corrections and see audit logs.
Data Integrity and Quality	Provide that data are relevant, accurate, complete and up-to-date.
Security Safeguards and Controls	Establish tools and mechanisms to provide that data are secured against breaches, loss or unauthorized access.
	Establish tools and approaches for user authentication and access.
Accountability and Oversight	Establish who monitors compliance with policies and procedures for handling breach.
	Produce and make available audit logs.
Remedies	Establish mechanisms for complaints.
	Establish remedies for affected parties to compensate for harm caused by breach.

This comment was formulated by a collective view informed by many and diverse collaborators within the Markle Connecting for Health community, and is supported by the following individuals and organizations.*

Christine Bechtel
National Partnership for Women & Families

Hunt Blair*
Office of Vermont Health Access

Adam Bosworth
Keas, Inc.

Jeff Brown
Wal-Mart Stores, Inc.

Alan F. Dowling, PhD
American Health Information Management Association

Steven Findlay, MPH
Consumers Union

Mark Frisse, MD, MBA
Vanderbilt University

Daniel Garrett
PricewaterhouseCoopers LLP

Mark Gorman
National Coalition for Cancer Survivorship

Adrian Gropper, MD
MedCommons

Joseph Heyman, MD
Whittier Independent Practice Association

James Heywood
PatientsLikeMe

Gerry Hinkley, JD
Pillsbury Winthrop Shaw Pittman LLP

Kevin Hutchinson
Prematics, Inc.

Michael B. Jackson
Adobe Systems, Inc.

Scott Kennedy
Target Corporation

Allan Korn, MD
Blue Cross and Blue Shield Association

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

David Lansky, PhD
Pacific Business Group on Health

Philip Marshall, MD, MPH
Press Ganey Associates, Inc.

Deven McGraw, JD, MPH
Center for Democracy and Technology

John Moore
Chilmark Research

Tom Morrison
NaviNet, Inc

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

Amanda Heron Parsons, MD, MBA*
New York City Department of Health & Mental Hygiene

J. Marc Overhage, MD, PhD
Regenstrief Institute, Inc.; Indiana Health Information Exchange

Carol Raphael, MPH
Visiting Nurse Service of New York

Wesley Rishel
Gartner, Inc

John Rother
AARP

Peter Schad, PhD
RTI International

Scott Schumacher, PhD
IBM

Clay Shirky
New York University Graduate Interactive Telecommunications Program

Thomas Sullivan, MD
DrFirst

Kenneth Tarkoff
RelayHealth

Micky Tripathi, PhD, MPP
Massachusetts eHealth Collaborative

Paul Uhrig, JD
Surescripts

Charlene Underwood, MBA
Siemens Medical Solutions

Robert Wah, MD
Computer Sciences Corporation

Jeb Weisman, PhD
Children's Health Fund

Markle Foundation

Zoë Baird
President

Carol C. Diamond
Managing Director, Health
Chair, Markle Connecting for Health

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