CONNECTING FOR HEALTH[SM]

MARKLE FOUNDATION *A Public-Private Collaborative*

U.S. Department of Health and Human Services
Request for Information: Voluntary Storage of Personal Data in Preparation for Emergencies

Collaborative Response[*] by:

Connecting for Health
Steering Group
and
Personal Health Technology Council

July 24, 2006

[*] **Connecting for Health** thanks Josh Lemieux and Daren Nicholson of Omnimedix Institute, and Melissa Goldstein, David Lansky, and Stefaan Verhulst of the Markle Foundation, for drafting this response.

Summary

Connecting for Health, a public-private collaborative group whose goal is to advance health information technology in the public interest, is pleased to offer the following response to the U.S. Department of Health and Human Services's (HHS) request for information[1] (RFI) issued on May 23, 2006. We limit the scope of this response to personal health information. We therefore exclude other types of personal information such as wills or birth certificates, which fall outside the domain of our work.

In sum, we applaud the department's recognition of the importance of having access to electronic records in the case of an emergency. However, we suggest that HHS broaden the scope beyond mass disasters to include individual health emergencies as well as chronic care and self-management.

We have very modest expectations for an approach that relies solely on consumers to store their own health information for emergency retrieval. It is appropriate for the federal government to encourage people to maintain, backup and protect key information virtually. Clearly, Americans can be more personally responsible and better prepared. However, even the most effective government efforts to encourage this behavior will inevitably fail to motivate a very large percentage of the population. Vulnerable populations (i.e., the older, sicker, poorer, uninsured, non-English speaking, etc.) are particularly difficult to reach and will require focused attention from HHS and others.

We discourage the creation of a new "centralized information silo" that will likely be out of date and unfamiliar to health care providers when the next disaster strikes. Instead we urge HHS to coordinate all health IT efforts within a vision of a decentralized nationwide health information network (NHIN).

A variety of solutions will likely be necessary to support the availability of essential health information in an emergency (as opposed to a single, centralized, nationwide database.) HHS should prioritize near-term emergency-preparedness work on achieving minimum consensus on identification, authentication and authorization practices for a wide range of health professionals. We encourage incorporation of the lessons from the KatrinaHealth experience in HHS planning. We believe the government has an important role to help educate and remind all custodians of critical health information to maintain adequate data backup and recovery procedures, as well as consider mechanisms for small, rural, and safety-net organizations and regions to sustain this critical and ongoing effort.

Finally, we feel that HHS should play a significant role to facilitate a collaborative, transparent process to develop electronic health data sharing policies that earn the public's trust.

---

[1] Federal Register: May 23, 2006 (Volume 71, Number 99).

Background

Background on the RFI:

The RFI states:

> To improve emergency preparedness, response and recovery efforts, HHS invites public comment on the availability or feasibility of private sector services through which individuals could voluntarily submit their personal information for storage so that they, their family members, or other designated individuals could access the information in an emergency. HHS invites all comments, suggestions, recommendations, and creative ideas on the establishment of voluntary nationwide services that can best offer this capability.

The RFI solicitation is a response to the White House report, *The Federal Response to Hurricane Katrina: Lessons Learned*, which recommended that the federal government work with the private sector to provide Americans with the means to electronically store and retrieve personal information that would be useful in the event of a natural or man-made disaster, such as an earthquake, flood, pandemic influenza, or terrorist event. The product of this proposed initiative can be thought of as a virtual bank vault, with virtual safe deposit boxes for information. Disaster victims could access the electronically stored data to apply for federal assistance, medical treatment, or insurance benefits. Because of the sensitivity of the personal data stored, strict privacy limitations and protections would be required.

Background on Connecting for Health:

Connecting for Health works to overcome the technical, financial, and policy barriers to bringing health care into the information age. **Connecting for Health** is committed to accelerating development of a nationwide health information-sharing environment by bringing together an array of private, public, and not-for-profit groups to identify common values and principles for system design and support the deployment of technologies that implement those principles.

The collaborators of **Connecting for Health** encompass more than 100 different organizations representing all health care stakeholders. They sit on one or both of the following bodies: the **Connecting for Health** Steering Group and the Personal Health Technology Council, in addition to other committees not mentioned here. The Steering Group provides the strategic direction to **Connecting for Health's** work and focuses on the interoperability of health information technologies and policies. The Personal Health Technology Council focuses on consumer empowerment through personal health records (PHRs) and related consumer-focused health information technologies.

In April 2006, **Connecting for Health** publicly released a set of resources, called the Common Framework, that provides technical and policy recommendations for private and secure electronic health information sharing among existing and developing health information networks. The Common Framework describes **Connecting for Health's** approach to a decentralized nationwide health information exchange network that improves the quality and safety of health care by facilitating authorized access to vital health data.

Building in strong privacy safeguards while designing and testing technical requirements are the foundation of the Common Framework. For more information, see www.connectingforhealth.org/commonframework/index.html.

The Markle Foundation founded and operates **Connecting for Health**. The Markle Foundation and the Robert Wood Johnson Foundation support the collaborative. For more information, see www.connectingforhealth.org.

Background on KatrinaHealth:

Through a collaboration of more than 150 organizations in the public and private sector, the KatrinaHealth project was made possible with the focused efforts and resources of the American Medical Association, Informed Decisions, the Markle Foundation, the Office of the National Coordinator for Health Information Technology (ONC), RxHub, SureScripts, the Veterans Administration, and the State Health Departments in Louisiana and Mississippi. This extraordinary effort provided access to electronically stored, medication-related data to medical personnel treating hurricane victims. Within three weeks of Katrina's landfall near New Orleans, the KatrinaHealth medication lookup service was made available to physicians treating hurricane victims. For more information, see www.katrinahealth.org.

General Response

We, the members of the **Connecting for Health** Steering Group and Personal Health Technology Council, commend HHS for seeking public comment on its emergency preparation efforts. We agree with the importance of improving the nation's ability to respond to any type of emergency that separates people from their medical records.

We offer the following insights based on our collaborative efforts over the last several years to transform health care through the use of health information technology:

1) Focus more broadly than on disaster response and recovery. Our response emphasizes that, even in the absence of a disaster, people are routinely separated from their vital clinical information today due to the fragmented and largely paper-based processes that continue to dominate health recordkeeping in this country. Anyone can have a medical emergency at any time. Health professionals respond to thousands of emergencies each day without rapid and reliable means to retrieve meaningful information about their patients. It is similarly common that people with chronic conditions lack tools to ensure that their many health care professionals each know what the others are doing. It is this state of affairs that motivated the formation of our collaborative in 2002.

We believe that HHS will achieve its goals of improved disaster recovery if it focuses the nation's resources and attention on improving health information interconnectivity in general. We contend that whatever framework is established to facilitate mass-emergency recovery must be based on improvements in our ability to deal with everyday, one-at-a-time emergencies and the management of chronic conditions. Such improvements must also be

scalable to respond to major disasters.

2) Do not place too much burden on consumers. We applaud HHS for exploring the roles of individual patients and their families in emergency preparation. Activating and empowering consumers is a key aim of the **Connecting for Health** collaborative. In fact, there is a significant urgency for making the public aware of the importance of having their information available electronically. However, HHS must not rely solely on asking people to voluntarily store pertinent information and keep it up to date so that it's still useful when a disaster strikes. Health information is typically collected and controlled by institutions and clinicians, not individuals. In general, individuals have little access to their personal health information even in the absence of a disaster. Additionally, prevention and preparedness are not deeply ingrained in the American public. For example, a recent survey by the American Red Cross found that most Americans are not sufficiently prepared for a disaster. Only half of the respondents had a disaster supplies kit. The majority of respondents did not have an evacuation plan or a pre-established family meeting place to reunite in the event of a separation.[2]

It is appropriate for the federal government to encourage people to maintain, backup and protect key information virtually. Clearly, Americans can be more personally responsible and better prepared. There are a variety of personal health record systems available today to help them. However, even the most effective government efforts to encourage this behavior will inevitably fail to motivate a very large percentage of the population. The proposed virtual self-storage approach should be viewed as only a small potential contribution to preparedness for emergencies large or small. Vulnerable populations (i.e., the older, sicker, poorer, uninsured, non-English speaking, etc.) are particularly difficult to reach and will require focused attention from HHS and others. It is a well-recognized problem that people who fall into these groups lack the resources to take advantage of information technology services.[3]

We therefore urge HHS to broaden the approach taken in this RFI — beyond a sole focus on mass emergencies, and beyond an over-reliance on individual consumers.

3) Apply the lessons of KatrinaHealth. We believe there is an opportunity to develop rules for authorizing access to available electronic data streams, particularly prescription medication lists from multiple sources as demonstrated through KatrinaHealth. Recently, the organizations that collaborated to create KatrinaHealth released a document that describes several lessons learned from their experience.[4] Though the effort was commendable, it offered a window into the complex issues that must be addressed to make health information access possible in emergency situations. The report offers the following main

[2] Red Cross [homepage on the Internet]. Washington, DC: The American National Red Cross; last updated: 23 May 2006 [cited 13 June 2006]. Survey reveals Americans not as prepared as they think; [about 3 screens]. Available from: http://www.redcross.org/pressrelease/0,1077,0_116_5398,00.html.

[3] Brodie M, Flournoy RE, Altman DE, Blendon RJ, Benson JM, Rosenbaum MD. Health information, the Internet, and the digital divide. Health Aff (Millwood). 2000 Nov-Dec;19(6):255-65.

[4] Markle Foundation, American Medical Association, Gold Standard, RxHub, SureScripts. Lessons from KatrinaHealth [monograph on the Internet]. New York: Markle Foundation; 2006 [cited 2006 June 22]. Available from: http://www.markle.org/downloadable_assets/katrinahealth.final.pdf.

recommendations:

Engage in advance planning and put pieces in place now:

- Invest in realistic advance planning and analyze actual disasters for lessons.
- Conduct a realistic emergency simulation that includes health information management.
- Determine in advance which agency is responsible for definitively identifying affected areas and for creating registries of affected people.
- Establish business agreements that will allow information sharing in disaster response situations. If these are in place prior to any emergency, then coordination, communication, and access move much faster and more effectively.
- State public health departments' emergency management teams should build relationships not only with federal agencies and local hospitals and providers, but also with non-governmental organizations and faith-based groups who may serve as unofficial first-responders.
- Plan "backups to backups," for when technology inevitably breaks down.

Take advantage of existing resources:

- Examine the potential of existing networks to provide information coordination and surge capacity.

Address system and electronic health record design issues:

- Private industries interested in helping design, develop, and deploy health information systems should use open standards.
- Establish a secure method to authenticate doctors, pharmacists, other health professionals—and patients themselves—to enable access to health information for clinical treatment and care to all who need it.

Integrate "emergency" systems into daily routine:

- Integrate emergency response mechanisms (and people) into non-emergency settings and care.
- Ensure that communications systems set up for emergencies are useful in broader circumstances — and their use regularly reinforced.

Create systems that are simple to access:

- Enable the electronic health information record to be accessible to nurse practitioners, physician assistants, and nurses working with physicians and clinics.
- Establish standards for laboratory results, health claims, and so on, so that more currently digitized data can be easily accessed in emergencies.

Improve communications strategies:

- Help people understand what is involved in their taking responsibility for at least some portion of their own records—especially people with chronic and life-threatening conditions—in both everyday and emergency situations, and facilitate their doing so.
- Develop multiple communications channels:

    - for different audiences (practitioners, the public)
    - using different technologies (not just the Internet) and
    - engage third parties that are respected in the community.
- Make sure these user groups know about information resources and how to use them.
- Find out in advance what types of information people want via the Internet, recognizing that some information is better than none.
- Develop and promote an analog to the 911 system (e.g., ".stat") now, rather than waiting for the next emergency. Sponsors must make clear what the service is capable of offering.
- Identify and leverage people's normal communications channels. For example, ask web search engines to ensure that the most reliable emergency web sites pop up first in searches.

Overcome policy barriers:

- Engage the public and private sectors in identifying barriers to working together, and start working on those now, at the highest levels.
- Re-educate communities on public laws and policies, like HIPAA, that are still poorly understood and therefore have unintended consequences magnified in emergent situations.
- State privacy officers should clarify how privacy rules apply in emergency situations.

We believe it is important for HHS to collaborate more urgently with health care stakeholders on the above KatrinaHealth recommendations and we believe this is a more fruitful path than focusing on encouragement of consumers to store their own data in a new data silo in case of emergencies.

The RFI does not ask key questions about how voluntary, virtual data storage would be integrated into healthcare delivery workflows or local and state public health and emergency response efforts. The RFI appears to imply that this virtual storage system will only be used for emergency purposes. One of the most important lessons learned from the KatrinaHealth experience was the difficulty of introducing and communicating new activities and unfamiliar information systems into clinical workflows during times of emergency — no matter how easy to use. (In fact, it is a huge challenge even in the absence of an emergency.) Similarly, we contend that consumers would be more likely to be engaged in keeping their health information records up to date <u>if they had convenient and secure access to their data held by the health entities that serve them in times of routine and emergency care.</u>

Similarly, state and local public health resources will be important to any scale of emergency response and will need to be integrated into any efforts to make health information available on a day-to-day basis as well as for emergencies. They are the first line of support and response to both personal and population-based "health security threats."

4) Leverage existing systems; avoid new data silos. We are hopeful that this effort will reinforce the need for system interoperability and authorized record access. We would be

concerned if this RFI were a step toward a federally sanctioned, centralized data silo for voluntary, haphazard self-storage of personal information. It is implausible that any one entity can emerge to garner the trust of all healthcare participants and all consumers. An approach based on a centralized approach raises questions central to trust such as who controls the data, who governs the process, what secondary uses and resale of data will be allowed, etc. Additionally a centralized model poses potentially greater risk to privacy since a single security breach could lead to a catastrophic data leak.

Second, personal health information will go largely unused unless it is made available to health professionals within their usual clinical workflows. Attempting a stand-alone solution, whether for emergency or daily use, is likely to fail because providers will not take advantage of it. For these reasons, a distributed model that allows for data from trusted sources to be accessed in a reasonably automated manner is the best approach.

In the near term, some consumers will use systems to aggregate and present their data. Such systems must strive to keep the information up-to-date and enable consumers to authorize convenient, secure access when and where it might be needed. Although near-term solutions that enable data in existing systems to be more readily available in case of an emergency (and solutions that enable consumers to self-report their data and make it available in case of an emergency) can be encouraged, we believe that, inevitably, the optimal solution will enable sharing necessary data conveniently and securely.

5) Focus on rules for a decentralized network, rather than a specific type of application. The many diverse stakeholders of **Connecting for Health** have concluded that fostering a decentralized network is a more practical approach to connecting our already decentralized healthcare system than attempting to build a one-size-fits-all database or application. A decentralized architecture allows for data to be stored in many different applications and locations interlinked across a common network, without requiring mass centralization before information can be made available. We contend that encouraging the development of rules for interconnecting health information networks should be the overarching HHS priority for disaster recovery as well as for everyday care.

The work of **Connecting for Health** has addressed health information. We have not addressed making other types of documents now in the hands of individuals (e.g., birth certificates, wills, etc.) available across a network. However, if enterprises emerge to provide consumers with personal document scanning and networked electronic storage/retrieval services, they could fully participate in a network that conforms to the architectural and policy principles that the **Connecting for Health** Common Framework recommends for the healthcare sector.

A decentralized health information network is desirable because it enables the establishment of health information exchange by building on rather than replacing existing infrastructure. Because it does not dictate technology choices, it allows great latitude for innovation and for tailoring health information exchange networks to meet diverse needs. For example, it may make sense in some geographic locations at high risk for large-scale emergencies to use a centralized disaster recovery approach that pools resources and allows smaller institutions the

ability to tap into a more comprehensive solution. Application vendors and their clients are in the best position to determine what sorts of integrations and displays are required for different users. The optimal network specifies only the necessary network configuration to permit both flexible data access and effective protection of privacy and security. Indeed, the outstanding global success of the Internet is due in large part to its decentralized nature.

Decentralization has its own vexing challenges, of course, since it requires all actors to agree to and implement certain elements (common policies and technical standards for information sharing, reliable availability and backup protocols to meet network requirements, etc.) and maintain a chain of trust across a network. The key requirement for the success of a decentralized approach is the articulation of a small, but necessary set of nationally uniform technical and policy guidelines that every organization that wants to share health information can adopt. **Connecting for Health** has designed the Common Framework in pursuit of this goal. For more information, see www.connectingforhealth.org/commonframework/index.html.

For example, a key element of the Common Framework, the Record Locator Service (RLS), could be enormously helpful in a disaster that displaces large numbers of people. An RLS enables authorized professionals to query a health information network to find the location of a patient's records. For a patient who shows up at an emergency shelter, an authorized RLS query could identify the sources of the patient's information and provide a head start for vital records retrieval or, if necessary, reconstruction. In large-scale disasters, the searches may require queries from one region or network to another. This was a specific use case of the Common Framework Prototype completed in early 2006.

6) Focus on key policies rather than merely technology applications. We have demonstrated that policy decisions must both precede and evolve in parallel with health information technology design and deployment. Policy issues define who has access to the information system, under what circumstances, and with what privacy protections. Without on ongoing process to provide answers to these questions and others, technology cannot be effectively deployed or designed.

For example, confidentiality of personal health information is a deeply rooted human value. Americans are notably protective of information concerning their health. Hence, we believe that the health IT architecture must take a comprehensive approach to privacy. For a detailed discussion of the driving principles for privacy protection, see *Architecture for Privacy in a Networked Health Information Environment*.[5]

The focus on privacy protection has several implications for a system that will be used in the context of a mass emergency. Once a disaster strikes, there is no time for thoughtful policy decisions concerning system access. Rules that specify who is authorized to access information through the network must be in place before an emergency occurs. At a minimum, HHS should prioritize near-term emergency-preparedness work on achieving minimum consensus on identification, authentication and authorization practices for a wide

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

range of health professionals. In addition, there is a need for guidance on how the HIPAA Privacy Rule applies specifically to uses and disclosures of personal health information in an emergency.

Additionally, policies concerning how to handle particularly sensitive data (e.g., HIV status, mental health, substance abuse, etc.) must not be made during a crisis. Finally, separate rules must be established prior to a disaster for the capture, handling, and persistence of health data acquired before, during and after an emergency. For example, what procedures are to be used to protect data stored on a laptop that an emergency response official uses in the field?

The policy process should provide for periodic review and revision, a method for evaluating exceptions (including mass emergencies), and a means for providing accountability to the agreed-upon principles and policies.

The goal of this policy work is to build public trust. Consumers will not participate in a voluntary emergency preparedness measure if they do not trust that their personal health information will be protected from unauthorized disclosure. Therefore, the policy rules mentioned above should be developed in a transparent manner. The decision process should include multiple stakeholders, including representatives of health care consumers.

7) Coordinate with broader health IT efforts. Two critical challenges — integrating the retrieval of electronic health information into clinical workflows and elevating the level of consumer empowerment — are central to HHS's and the American Health Information Community's current efforts to demonstrate the potential of the NHIN. Coordination with these efforts and others, including those of the CDC and state and local public health and emergency preparedness efforts, should be more clearly specified.

We also note that HHS has recently published a separate RFI in which it solicits information on approaches for "establishing a system by which victims of disasters can access multiple benefits and services in a secure and confidential way through magnetic stripe cards, smart cards, biometrics, or other innovative methods."[10] The problems addressed by these two RFIs appear similar to us.

[10] Request for Information: Development and Implementation of Electronic Benefits Transfer System for Victims of Disaster To Receive Federal and State Benefits. Federal Register/Vol. 71, No. 114/ June 14, 2006. Accessed online June 29, 2006 from URL: http://edocket.access.gpo.gov/2006/pdf/E6-9314.pdf

We urge HHS to articulate how it will coordinate each of these efforts related to health information technology and how they relate to a vision for the NHIN.

In summary, we encourage HHS to focus its resources on fostering a NHIN that would serve multiple purposes, ranging from chronic care and single-person emergencies to national disasters. The rules governing the network must be aligned with core principles and values, particularly consumer authorization for any sharing of sensitive health information.

Specific Response

Many of the RFI questions are application-related. As a multi-stakeholder collaborative, we remain agnostic about end-user application technologies and we encourage ongoing innovation in this area. We therefore provide brief statements for each section of the RFI but do not answer each specific question.

Section 1: Approach, Finance, Sustainability, and Roles

Various entities today hold personal health information in digital form that could prove vital in an emergency. Key sources include pharmacy networks, medical laboratories and imaging centers, private health insurance systems, Medicaid and Medicare databases, electronic medical records in doctors' offices and hospitals, data clearinghouses, and vital records agencies. In contrast, most individuals have only a small portion of this information in their home or maintained in well-organized and accessible form. The Internet already provides a remarkable transport medium for moving information to new locations on demand. Of course, the current custodians of digital health information must do a responsible job of storage, security, and backup procedures that include disaster recovery planning. Certainly, institutional managers of health information do these key tasks more reliably than most individuals today.

This environment should encourage HHS to consider information retrieval models that take advantage of existing infrastructure and commitments, rather than contemplating the creation of a new centralized health information database. We prefer a "network of networks" architecture that is decentralized and federated. This confederation should be founded on an adequate set of policy and technical guidelines that will protect consumers' information confidentiality and promote their autonomy. The governance of this confederation should include representatives from all health care stakeholders, including consumer representatives. The confederation should publicly develop and disseminate its policy and technical decisions.

The government does not need to evaluate which end user applications provide value. Instead, it should foster the policies that ensure that the national information environment provides for the secure and efficient movement of personal information into applications that consumers and those they designate regard as appropriate. It should promote an information network that will enable the private sector to create innovative applications. The benefits of

focusing on a network rather than a specific application are:

- The network can be leveraged for multiple uses including both routine health care activities and emergency responses.
- Data can remain in the system where they are captured. In an emergency, data will be accessed in their most current and accurate state if they are stored close to where they were captured.
- System failures are less catastrophic since they would only affect a small portion of the network. System failures in a centralized system are more catastrophic.
- Given the fragmented nature of the U.S. health care system, it is more realistic to implement a network approach as opposed to a single database.
- The costs of developing and maintaining a distributed information-sharing environment are shared among many participants. Leveraging the existing infrastructure for multiple purposes reduces the need for categorical budgeting, creating separate management and staff resources, and subjecting the process to political pressures.

In addition, the government does have a role to ensure that the capabilities of this network provide equitable access to critical personal information in an emergency to everyone regardless of income, language, insurance status, or disability. The network approach is more likely to achieve this objective than a model that requires individual collation and management of personal documents.

Section 2: Function, Capabilities, and Performance

We urge HHS to focus its disaster preparedness planning on developing a robust set of network policies, as opposed to a stand-alone health IT application or centralized repository. We do not recommend a single solution or application. The market can and should generate many alternatives and innovations; these innovations should be connected and accessible in emergencies because they take advantage of common technical standards and policies.

In emergencies, it's vital to provide authorized health professionals with the most relevant and accurate data on affected people so that they may receive optimal care. (See the Common Framework document *Background Issues on Data Quality*.[11]) As evidenced by KatrinaHealth, there is a wealth of digital medication data currently available in electronic form. The first generation of electronic disaster preparedness planning should focus on medication data because of its availability and clinical significance. Though a large proportion of laboratory and medical claims data are also currently stored electronically, these data may prove to be more difficult to access than medication data. Nevertheless, these data should not be overlooked given the fact that they are currently available digitally.

If successful, ongoing efforts to promote a variety of standard patient information snapshots (including those put forth by the American Health Information Community for an electronic "clipboard," a clinical summary record, immunization record, etc.) could improve the value of near-term data-sharing efforts. The government can certainly add visibility and urgency to

[11] Available online at:
http://www.connectingforhealth.org/commonframework/docs/T5_Background_Issues_Data.pdf

these important efforts in standards development organizations. Importantly, however, no one standard is likely to satisfy all requirements for patient information.

Given the sensitivity of personal health data, it is important that consumers have control over their data. They should be given the power to decide who is authorized to view their data. Previous work by **Connecting for Health** provides significant detail on the policy principles that support consumer choice. Please refer to the first policy document of the Common Framework, titled *Architecture for Privacy in a Networked Health Information Environment*.[12]

The network infrastructure that we recommend needs to be scalable so that it can grow incrementally. Also, it should be robust enough to simultaneously handle the normal nationwide (non-emergency) traffic and the high-volume traffic that would occur during a localized emergency.

One of the guiding principles found in the Common Framework is that consumers should be able to find out where their health information is located and how it is being used. Please refer to the document titled *Patients' Access to Their Own Health Information*[13] of the Common Framework for detailed policy discussions on this subject. If special rules concerning data access and use are to be applied during disaster responses, then these rules should be directly disclosed to consumers.

Section 3: Rights, Rules, Responsibilities, and Enforcement

It is essential to establish clear policies concerning data capture and use before an actual disaster occurs. Policies that specify who is authorized to access the system should be discussed openly and disseminated before an emergency occurs. The interested parties include, without limitation, consumers, providers, payers, laboratories, pharmacies, pharmacy benefits managers, technology vendors, civilian and military emergency response teams, and public health and policymakers.

Inappropriate disclosures include but are not limited to the following scenarios:

- Disclosure to an unauthorized individual (e.g., a physician who is not involved in the care of the given patient).
- Disclosure of information for the wrong patient, i.e., incidental disclosures. (See the Common Framework document *Breaches of Confidential Health Information.*[14])
- Disclosure of information for non-authorized secondary uses.

Discussion of consumer choice should begin (but not end) with the following principles articulated earlier by the Personal Health Technology Council:

1. Individuals should be guaranteed access to their own health information.
2. Individuals should be able to access their personally identifiable health information

[12] Available online at: http://www.connectingforhealth.org/commonframework/docs/P1_CFH_Architecture.pdf
[13] Available online at: http://www.connectingforhealth.org/commonframework/docs/P6_Patients_Access.pdf
[14] Available online at: http://www.connectingforhealth.org/commonframework/docs/P8_Breaches.pdf

conveniently and affordably.

3. Individuals should know how their personally identifiable health information may be used and who has access to it.
4. Individuals should have control over whether and how their personally identifiable health information is shared.
5. Systems for health information exchange must protect the availability, integrity, security, and confidentiality of an individual's information.
6. The governance and administration of health information exchange networks should be transparent and publicly accountable.

Section 4: Security and Standards

The Common Framework approach to security and standards is published at: http://www.connectingforhealth.org/commonframework/index.html.

Section 5: Potential Federal Roles

The federal government can play a significant role in coordinating and encouraging the growth of a nationwide health information network by participating in an open, multi-stakeholder policy development process. The government can work in the public interest with other stakeholders (e.g., provider-based institutions, vendors, insurance plans, consumer groups, etc.) to resolve conflicts concerning data sharing.

Much still needs to be learned about how people will use PHRs and how health care professionals can be encouraged to integrate PHR information into their interactions with patients. In response to an RFI issued by the Centers for Medicare and Medicaid Services in August 2005, [15] **Connecting for Health** advised that HHS agencies have an important role in designing and financing pilot projects to help determine the motivating factors and values derived from the use of PHRs.

The federal government also can play an important role in promoting emergency preparedness. This role would primarily involve educating and reminding not only consumers but also all holders of health information about the importance of backup and recovery plans for critical information. As indicated in our response above, there should not be an over-reliance on individuals to self-store their personal information for emergencies.

Summary

We agree with HHS that access to health records is a vital component of disaster planning and we applaud efforts to make health data available to authorized people in emergency situations. We strongly discourage the creation of a new information silo that will likely be out of date and unfamiliar to those who need it when the next disaster strikes. We also strongly

[15] Opportunities for CMS Actions in Support of Personal Health Records - Connecting for Health Steering Group and Personal Health Technology Council Response to RFI. Available online at: http://www.connectingforhealth.org/resources/CMS_Response_Final_083105.pdf

discourage any approach that places too much burden on consumers to store their own information. We have very modest expectations for an approach that relies solely on consumers to store their own health information for emergency retrieval. It is appropriate for the federal government to encourage people to maintain, backup and protect key information virtually. Clearly, Americans can be more personally responsible and better prepared. However, even the most effective government efforts to encourage this behavior will inevitably fail to motivate a very large percentage of the population. Vulnerable populations (i.e., the older, sicker, poorer, uninsured, non-English speaking, etc.) are particularly difficult to reach and will require focused attention from HHS and others.

We suggest that HHS broaden the scope of its emergency response planning so that it can be used for both individual and mass emergencies, as well as chronic care and self-management.

We encourage incorporation of the lessons from KatrinaHealth in HHS planning. HHS should prioritize near-term emergency-preparedness work on achieving minimum consensus on identification, authentication and authorization practices for a wide range of health professionals. We urge HHS to coordinate all health IT efforts within a vision of a decentralized nationwide health information network. We believe it appropriate for HHS to remind all custodians of critical health data to maintain adequate data backup and recovery processes, as well as consider mechanisms for small, rural, and safety-net organizations and regions to sustain this critical and ongoing effort. Finally, we feel that HHS should play a significant role in facilitating a collaborative, transparent process to develop electronic health data sharing policies that earn the public's trust.

APPENDIX A: Connecting for Health Steering Group

** Note: State and Federal employees participate in the Steering Group but make no endorsement.*

Antoine A. Agassi*, State of Tennessee eHealth Council

Peter A. Andersen, MD, Lockheed Martin Information Technology

Zoë Baird, Markle Foundation, (ex-officio)

Robert Bogin, MD, American Cancer Society

William Braithwaite, MD, eHealth Initiative, (Co-Chair, Policy Subcommittee)

Claire Broome*, MD, Centers for Disease Control and Prevention, United States Department of Health and Human Services

Carolyn Clancy*, MD, Agency for Healthcare Research and Quality, United States Department of Health and Human Services

Janet Corrigan, PhD, National Quality Forum

Mike Cummins, VHA Inc.

Francois de Brantes, Bridges To Excellence and Prometheus

Mary Jo Deering*, PhD, National Cancer Institute/National Institutes of Health, United States Department of Health and Human Services

Carol Diamond, MD, MPH, Markle Foundation, (Chair, Connecting for Health Steering Group)

David A. Epstein, IBM Software Group

Colin Evans, Intel Corporation

Mark Frisse, MD, MBA, MSc, Vanderbilt Center for Better Health, (Co-Chair, Policy Subcommittee)

Daniel Garrett, Computer Sciences Corporation's Global Health Solutions Practice, (Vice Chair)

J. Peter Geerlofs, MD, Allscripts Healthcare Solutions

John Glaser, PhD, Partners HealthCare System

John Halamka, MD, CareGroup Healthcare System

Douglas Henley, MD, American Academy of Family Physicians

Joseph Heyman, MD, American Medical Association

Kevin Hutchinson, SureScripts

Michael Jackman, Eastman Kodak Company

William F. Jessee, MD, Medical Group Management Association

Y. Michele Kang, Northrop Grumman Corporation

Michael L. Kappel, McKesson Provider Technologies

Brian Keaton, MD, FACEP, American College of Emergency Physicians

Linda Kloss, RHIA, CAE, American Health Information Management Association

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

David Lansky, PhD, Markle Foundation, (Chair, Personal Health Technology Council)

Gail Latimer, MSN, RN, Siemens Corporation

Jack Lewin, MD, California Medical Association

Stephen Lieber, CAE, Healthcare Information and Management Systems Society

J. P. Little, RxHub, LLC

John R. Lumpkin, MD, MPH, Robert Wood Johnson Foundation, (Vice Chair)

Patricia MacTaggart, EDS

Janet M. Marchibroda, eHealth Initiative

Howard Messing, Meditech

Arnold Milstein, MD, MPH, The Leapfrog Group

Margaret O'Kane, National Committee for Quality Assurance

Dennis O'Leary, MD, Joint Commission on Accreditation of Healthcare Organizations

J. Marc Overhage, MD, PhD, Indiana Health Information Exchange; Indiana University School of Medicine, Regenstrief Institute for Healthcare

Herbert Pardes, MD, New York-Presbyterian Hospital, (Vice Chair)

Alison Rein, National Consumers League

Russell J. Ricci, MD, Meditech

Craig Richardson, Johnson and Johnson Health Care Systems, Inc.

Wes Rishel, Gartner Group

William Rollow*, MD, Centers for Medicare and Medicaid Services, United States Department of Health and Human Services

David Schulke, The American Health Quality Association

Steve Shihadeh, Microsoft Corporation

Clay Shirky, New York University Graduate Interactive Telecommunications Program, (Chair, Technical Subcommittee)

Ellen Stovall, National Coalition for Cancer Survivorship

Thomas Sullivan, MD, Women's Health Center Cardiology, AMA-Council on Medical Service and DrFirst.com

Paul Tang, MD, Palo Alto Medical Foundation, American Medical Informatics Association (AMIA)

Randy L. Thomas, IBM Corporation

Robin Thomashauer, Council for Affordable Quality Healthcare

John Tooker, MD, MBA, FACP, American College of Physicians

Micky Tripathi, Massachusetts eHealth Collaborative

Charlene Underwood, Healthcare Information and Management Systems Society, EHR Vendor Association

Scott Wallace, The National Alliance for Health Information Technology

Robert B. Williams, MD, MIS, Deloitte

Rochelle Woolley, Woolley & Associates

Hugh Zettel, GE Healthcare Integrated IT Solutions

APPENDIX B: Personal Health Technology Council

** Note: State and Federal employees participate in the Steering Group but make no endorsement.*

Tim Andrews, Health Innovation Partners

Wendy Angst, CapMed, A Division of Bio-Imaging Technologies, Inc.

Rodney Armstead, MD, FACP, Arizona Physicians IPA

Annette Bar-Cohen, MPH, National Breast Cancer Coalition

Cynthia Baur*, PhD, Office of Disease Prevention and Health Promotion, United States Department of Health and Human Services

Marc Boutin, JD, National Health Council

Patti Brennan, PhD, University of Wisconsin Madison

Helen Burstin*, MD, MPH, Agency for Healthcare Research and Quality, United States Department of Health and Human Services

Rex Cowdry*, MD, Maryland Health Care Commission

Kelly Cronin*, Office of the National Coordinator for Health Information Technology, United States Department of Health and Human Services

Mary Jo Deering*, PhD, National Cancer Institute, National Institutes of Health, United States Department of Health and Human Services

Richard Dick, PhD, You Take Control

Stephen Downs, Robert Wood Johnson Foundation

John P. Driscoll, Medco Health Solutions, Inc.

Esther Dyson, CNET Networks

Ed Fotsch, MD, Medem

Peter Frishauf, Healthcare Marketing & Communications Council, Inc.

Janlori Goldman, Health Privacy Project

Ken Goodman, PhD, University of Miami

Jonathan Hare, Resilient

Jim Karkanias, Microsoft, Inc.

J.D. Kleinke, Omnimedix Institute

Linda Kloss, RHIA, CAE, American Health Information Management Association

David Lansky, PhD, Markle Foundation, (Chair, Personal Health Technology Council)

J.P. Little, RxHub, LLD

Gail McGrath, National Patient Advocate Foundation

Kathleen Mahan, SureScripts

Jack Mahoney, MD, Pitney Bowes Corporation

Phil Marshall, MD, MPH, WebMD

Omid Moghadam, Intel Corporation - Digital Health Group

Jonathan Parker, Americans for Health Care, Service Employees International Union

Ginger Price*, Department of Veteran's Affairs

Alain Rappaport, MD, PhD, Medstory, Inc.

Alison Rein, National Consumers League

Marie Savard, MD, Savard Systems

Albert Shar, PhD, Robert Wood Johnson Foundation

Clay Shirky, New York University Graduate Interactive Telecommunications Program, (Chair, Technical Subcommittee)

Michael Simko, RPh, Walgreen Pharmacy Services

Joel Slackman, BlueCross BlueShield Association

Paul Tang, MD, Palo Alto Medical Foundation/American Medical Informatics Association (AMIA)

Randy L. Thomas, IBM Corporation

Tony Trenkle*, Centers for Medicare & Medicaid Services, United States Department of Health and Human Services

Rochelle Woolley, Woolley & Associates

Anne Woodbury, Fleishman Hillard Health Solutions Navigator

Matthew Wynia, MD, American Medical Association