Clay Shirky, Chair, Technical Sub-committee, **Connecting for Health**

Connecting for Health is a public-private partnership, made up of over a hundred organizational stakeholders in the healthcare system. Connecting for Health is dedicated to improving health care in the United States through improvements in the use of healthcare IT. For more than a year, Connecting for Health has convened a Personal Health Technology Council, which envisions a networked health information environment that will enable increased participation by consumers in their health and their health care. The Council's goals include improving the safety and quality of health care by increasing consumers' access to their personal health information, improving consumers' ability to understand and participate meaningfully in their care, and preserving the security and confidentiality of the individual's data.

When considering personal health records, it is crucial to distinguish between the records themselves, and the systems that handle the records. In the same way that the world's email infrastructure requires both standardized data for the email messages and interoperable software that handles that data, it is critical that the personal health records themselves not be tied to any particular provider or tool, but are standardized and portable, and that the software that handles the data be able to both import and export records in standard formats. In these comments, I will use PHR to refer to the actual personal health record (the data) and PHR system to refer to software that produces, consumes, stores, transports or otherwise acts on PHRs.

Question 1 asks how identity proofing and user authentication are currently addressed in the Personal Health Record (PHR) market. Sadly, there is a very immature market today for PHRs; from our point of view, barriers to adoption — such as lack of integration with services that are important to consumers, lack of transportability of data and lack of interoperability on arrival, and a culture that does not habitually involve the patient in his or her own health information management or care — are the primary obstacles. Of the PHR systems that exist today or are in serious design phases, we see three types.

The first are **non-networked PHR systems**. These are pieces of software that are able to accept data entered locally, or to store electronic data sent by other means, but which do not have native or

standard methods of sending and receiving data over a network. While we certainly don't object to non-networked PHRs, we are also skeptical that these applications will be transformative of US healthcare, as their value is closer to that of a safe-deposit box than as a source of near-real-time clinical value.

The second are **networked PHR systems hosted by a Care Delivery Organization (CDO) or other health care entities, such as pharmacy chains.** In this case, a hospital or other CDO will provide credentialed access to a database of clinical data, with the patient typically offered access through a secure web-based application. (CareGroup in Massachusetts is a good example of this function.) The advantages of such a system are that data from the CDO are automatically added to the patients record in a timely fashion, and the proofing and security are handled by an organization that is required to preserve the confidentiality of the data, and already has a relationship with the patient. The disadvantages include providing an organization-centric, rather than patient-centric, view of the data; if a third organization holds data on the patient that the CDO does not have, it can be difficult to add that data to the PHR. The other disadvantage is that a patient's relationship with a particular CDO may be transient, and extracting a PHR from such a system, and adding it to another PHR system elsewhere, is extremely inconvenient if not impossible in today's environment.

The third are **networked PHR systems hosted by third-party providers.** While it is early in the evolution of PHR systems we must recognize that new entrants and innovators will continue to emerge. For example, there is the opportunity for PHR systems to emerge from outside of health care by entities that fit into the category of internet-based customer-service organizations, including Internet Service Providers, consumer-oriented application providers from other sectors, and search engines. These kinds systems can be similar to that of CDO-tethered systems; the PHR will be stored by the organization and made accessible through secure Web access. The potential advantages of such a system are patient-centricity and a relationship that will not terminate when the patient changes CDOs. The potential disadvantages are that such systems are less well connected to existing clinical networks, and therefore must create new agreements and interfaces to share personal health data with

myriad potential sources that currently hold the individual's data. In addition, they lack clarity in the current regulatory environment about their duties to the consumer and their personal health information. In particular, such services may not be regulated by HIPAA, leading to the possibility of large aggregations of clinical data being collected and used in ways that contravene the spirit of HIPAA and other similar regulations, without being bound by the traditional agreements and remedies proposed by those regulations.

It is most likely then, that an ecosystem of CDO-tethered and third-party PHR systems will emerge (with some small group of patients opting for local, non-networked storage of their records.) Our goal should be to establish minimum standards of both conduct and interoperability within that ecosystem. In our view, a networked PHR environment works only if both data sources and data users have high confidence in the compliance of all other parties with a set of key requirements. Each network participant – doctor, insurance company, patient – is exposed to legal, financial, and moral hazards as it shares sensitive information with other participants, and must be assured that identities are confirmed, appropriate authorizations apply, and shared information will be used in appropriate ways. In particular, a commercial entity should not, by dint of contract, be able to aggregate voluminous amount of clinical detail in ways that allow them to re-sell or otherwise re-use the data in ways the patient does not approve of or know of. Particularly dangerous in this regard are the increasingly common user license agreements offered for other sorts of web accessible software, such as music databases or legal research tools, which allow the host of a piece of data to unilaterally change the terms of a contract after the fact. Similarly, networked PHR systems, whether CDO-tethered, or third-party, should not be able to create lock-in or destroy portability of the patient's health data. For the remainder of today's discussion, I will focus primarily on the question of managing identity across a network of patient and consumer users.

To address **Questions 2, 4 and 5**, there is special cause for concern about security and privacy when patients are given access to their clinical records. Security in a medical context is a hard problem; there are technological, legal, and social constraints, and because security often creates

inconvenience, it is possible to design a system that is secure but unusable. As HHS considers the complex issues surrounding identity, authentication, authorization, and auditing, it is important to remember that the ability to describe a problem clearly does not always make it possible to procure a simple solution. Security is such a case; it is a process, not a product, and it is both a balancing act -- how much security for how much cost and at how much inconvenience -- and a moving target -- new opportunities and new threats arise regularly.

In particular, it is risky to draw generalizations from security requirements for clinicians and other healthcare employees, because those organizations have several native advantages in the realm of authenticating their users, including employment contracts with those users, significant control of the network they operate, and regulatory clarity about security requirements from e.g. HIPAA. None of these aspects are true of a data holder's relationship to a consumer -- the consumer is harder to identify, her relationship to the data holder is both more potentially ephemeral and less clearly regulated, and the ability to audit or punish individuals accessing the system is limited.

Because there is a less robust and well-defined set of policies and processes that apply to the relationship between data holders and patients than that between data holders and clinicians, in-person proofing and issuance of credentials is currently and likely to continue to be a critical component of providing consumers with the credentials, tokens, or other means of accessing their data. In practice, this will often mean working with institutions that have pre-existing relationships with the consumer, and arranging for them, under a common set of requirements, to become the issuers of those credentials. In fact, today many CDOs that offer a PHR system, require the clinician to distribute these credentials to their own patients. However, these issuers do not necessarily need to be clinicians or even healthcare entities -- employers, financial institutions and even Notary Publics could be considered for their appropriateness as participants in the proofing process.

Finally, in addressing the issue of security, it is important to note that securing any one aspect of a system produces only partial benefits, if the other areas of concern are ignored (analogous to buying better door locks but leaving your windows open.) Identity proofing and the issuance and checking of

credentials are vital, but they are not the whole security story with PHR systems. In today's environment, by far the biggest risk to security comes not from unauthorized requests or interception of data in transit, but from the loss or theft of large (sometimes enormous) aggregations of data held at the edges. Thefts of laptops, PCs, hard drives and other wholesale removal of large data sets is an issue in many industries today, and if PHR systems grow to the scale we hope they do, the risk of the loss of a database containing hundreds of thousands or millions of records will be the most significant security issue. Simple early measures like requiring data at rest to be encrypted on disk will go a long way towards deflecting that risk rather than having to react to it later.

To address **Question 6**, the appropriate balance between access to medical information and privacy concerns of the consumer is not a single state. There are several factors involved in setting this balance, including the sensitivity of the data involved, the applicable regulatory environment including especially State regulations, the relationship of the accessing organization to the patient, and the consumer's own desire for privacy. Because there is no one answer, we believe that this is a matter best approached on principle.

We propose four principles to guide local decision makers in addressing the appropriate balance: **first, a necessary set of security standards** should be set for those entities who knowingly handle the consumer's clinical data (as separate from the consumer simply using a generic online storage service, say), and those standards should differ depending on the sensitivity of the data to be handled. **Second, the patient should be in charge** of determining who else has access to his or her records to the degree possible. **Third, entities that hold data on the consumer should make that data available** to the consumer's PHR system, but this requirement should not be reciprocal; the patient should be able to control who has access to reading the aggregate contents of the PHR. **Fourth, this collection of preferences should be dynamic.** Should a consumer change his or her mind about the level of access offered to any third party by a PHR system, she should be able to change the access rules easily going forward.

Though Question 6 mentions implementation difficulties, the technological issues here are actually relatively straightforward. Generations of digital tools for collaboration, from Lotus Notes to Groove to simple weblog tools, have adequate methods for allowing individuals decide when and how to offer or revoke access to content. The principal hurdle here is creating a medical culture which allows individuals to both aggregate their own data, and to control subsequent access to that particular aggregation. It is also important to note that we are **not** proposing that the individual consumer's control over his or her own PHR be applied to sharing of data by clinicians caring for the same patient; sharing of data does and should operate on different principles in clinical and personal settings.

To address **Questions 3 and 7**, HHS's role in establishing guidelines will presumably be as an early mover, as an advocate for the value of networked health information generally, and as an advocate for the consumer's rights in such a network. HHS can identify, promulgate, and serve as an exemplar of good data practices as concerns establishing security and preserving patient privacy. In particular, when sharing information with non-governmental entities, it seems reasonable to require those entities to conform to federally mandated privacy and security requirements. Indeed, not to raise to the level of such requirements would be to invite a cascade of increasingly less restrictive regimes through which sensitive clinical data could flow. This will take a mix of policy guidance and self-policing (or, more likely, peer policing) by the participants. Pure regulatory policy is unlikely to work in an environment this varied, but pure self-policing often leads to a gradual decline of standards, as with TRUSTe in the realm of e-commerce, or the failure of self-policing to avert major data breaches in the credit card industry. Per the answer to Question 1, it is unlikely that either the necessary standards of regulatory control or interoperability will be either achieved or enforced solely by self-policing. It is precisely where the actions of a diverse group of actors need to be coordinated that clear policy requirements can provide a good starting point, provided it offers only the necessary requirements rather than trying to dictate the entire behavior of all the participants in the ecosystem.

For **Question 8**, and per the answer here to Question 6 about the relative sensitivity of various sorts of data, OMB Memorandum M-04-04 is a good starting point for considering the relationship between the data involved and the security required. Connecting for Health has used the OMB model in thinking through the tradeoffs of sensitivity of data, security, convenience of use, and cost of implementation.

Finally, to answer **Question 9**, it is critical to note that any data collected to provide an authentication system is itself critical data, and also needs to be protected. The first principle of protecting sensitive data is not to hold it if you don't need to. As a result, no clinical data should ever be collected or used as a proofing mechanism. Instead, collecting a set of non-clinical identifiers (name, date of birth, etc) in clean and highly codified formats should be sufficient for the proofing process, without creating an additional source of risk for the loss or disclosure of clinical data.

Thank you for allowing me to summarize the current thinking of Connecting for Health on these questions. We believe that this is a critical moment in the development of the NHIN and the emerging definition of a new role for patients in US healthcare. If we specify a necessary set of policies and standards for managing individual identity, we will create a more trustworthy system and encourage innovative PHR systems to extract value from personal health data. But if we fail to define these standards properly now, we will run the risk of losing public trust, and limiting the benefits that information technology can provide to Americans and the health care system. Thank you.