THE CONNECTING FOR HEALTH ARCHITECTURE FOR PRIVACY IN A NETWORKED HEALTH ENVIRONMENT

SUMMARY

Introduction

A networked health information sharing environment has the potential to enable “anywhere and any time” health decision support, thereby improving public and individual health, and reducing cost. Consumers and patients can benefit directly when their personal information is available to health care providers, and indirectly when their information is available in the aggregate to researchers seeking new ways to prevent, manage, or cure health problems.

At the same time, the potential benefits must be weighed against the risks of privacy and security violations, which may create public distrust if not addressed at the outset. If these risks are not dealt with in a systemic and proactive manner, an environment may be created in which society gets all the disadvantages of privacy invasions with none of the efficiency and health gains promised by new technologies.

If health information technology (HIT) applications are not trusted, both by the public and the health community, then their value and effectiveness will remain limited, no matter how interoperable and technologically feasible they may be. The public—all of us—must be confident that personal information will not be misused or disclosed inappropriately. Without such confidence, any HIT advancement is likely to encounter significant opposition, both at its inception and throughout its existence. That is why Connecting for Health, among other groups, has strongly argued for the design and implementation of a comprehensive “Privacy Architecture,” comprised of policies, rules, practices, and technologies, to enhance trust from the very start of any health information exchange environment.

Why do we care?

A lack of trust in how medical data is gathered, used, and disclosed is harmful because it can lead to so-called “privacy protective behavior.” Such behavior includes hiding evidence of pre-existing conditions from doctors or insurance companies; paying out-of-pocket for treatment; or simply avoiding treatment altogether. A lack of trust has a toll on both individual health and, more generally, on public health.

What are the risks?

While there have always been risks associated with the potential misuse of sensitive medical information in an offline world, they have become more pronounced recently. This is in large part due to the scale of data transactions; the relatively greater ease of collecting, linking, and disseminating information over a network; and the reduced ability to “leave the past behind” and shield sensitive information. The increased risks in a networked environment include:
Secondary use of data, including the use of medical data for employment or welfare purposes; to restrict credit or other financial benefits; or in unsolicited marketing;

- Security breaches, including hacking and other criminal activities that lead to “data leakage”;
- Criminal misuses of data, including fraudulent acts or identity theft that result in financial or other harm; and
- Data quality issues, including data corruption and loss.

Recent high profile cases of security and data breaches—many of which have been reported in the media—have dramatically highlighted the inherent vulnerabilities of networks and information stored in a digital form. From January 1 to November 1, 2005, there were 118 known security breaches which impacted potentially 57 million individuals. So far, many of the breaches have affected financial information, but at least 10 of the breaches have been specifically related to medical information. At the same time, identity theft has become a major consumer concern. According to a recent poll, 20% of American adults, or 44 million individuals, reported in 2005 that their identity has been stolen as a result of data leakage or theft.

These breaches and thefts have substantially increased already existing concerns regarding health privacy. These concerns have been documented by a number of recent surveys:

- A Harris Interactive Survey on Medical Privacy, released on February 8, 2005, indicated that between 62% and 70% of adults are worried that sensitive health information might leak because of weak data security; that there could be more sharing of patients' medical information without their knowledge; that computerization could increase rather than decrease medical errors; that some people won't disclose necessary information to health care providers because of worries that it will be stored in computerized records; and that existing federal health privacy rules will be reduced in the name of efficiency.
- A California Health Care Foundation survey (November 2005) indicated that 67% of Americans remain concerned about the privacy of their personal health information and are largely unaware of their rights;
- A Markle Foundation survey, released in October 2005, found that more than three out of four respondents (79%) supported the right of a patient to control access to personal health information.

These increased risks and the growing distrust cannot sufficiently be dealt with through existing legal provisions and privacy practices.

They require comprehensive “architectural” solutions that build privacy and security protections from the start, rather than as post-fact remedies.
What must be done?

One model for a comprehensive privacy architecture has been developed by Connecting for Health.

The “Connecting for Health Architecture for Privacy in a Networked Health Environment” recommends nine privacy protection principles, building upon the fair information practices model adopted in various countries. Considered and applied together, these principles add up to an integrated and comprehensive approach to privacy that can help overcome the current fragmentation. It is critical that the nine principles be considered as part of one package—elevating certain principles over others will simply weaken the overall architectural solution. The nine principles include:

**Openness**
There should be a general policy of openness about developments, practices, and policies with respect to personal data. Individuals should be able to know what information exists about them, the purpose of its use, who can access and use it, and where it resides.

**Purpose Specification and Minimization**
The purposes for which personal data are collected should be specified at the time of collection, and the subsequent use should be limited to those purposes (or others that are specified on each occasion of change of purpose).

**Collection Limitation**
Personal health information should only be collected for specified purposes, should be obtained by lawful and fair means and, where possible, with the knowledge or consent of the data subject.

**Use Limitation**
Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified.

**Individual Participation and Control**

- Individuals should be able to obtain from each entity that controls personal health data information about whether or not the entity has data relating to them;

- Individuals should have the right to:
  - have personal data relating to them communicated within a reasonable time (at an affordable charge, if any), and in a form that is readily understandable;
  - be given reasons if a request (as described above) is denied, and to be able to challenge such denial; and
challenge data relating to them and have it erased, rectified, completed, or amended.

Data Integrity and Quality
All personal data collected should be relevant to the purposes for which they are to be used and should be accurate, complete, and current.

Security Safeguards and Controls
Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure.

Accountability and Oversight
A data controller should be accountable for complying with measures which give effect to the principles stated above. Compliance with all of these basic principles is especially important for a system which will contain and disseminate highly personal information of the utmost sensitivity.

Remedies
Legal and financial remedies must exist to address any security breaches or privacy violations.

What must be done next?

Of course, the principles remain just that—principles—and their precise manifestation will vary from state to state, and from application to application. Yet while they are broad enough to apply across organizations, stakeholders, and jurisdictions, they are also specific and tangible enough to have real significance and practical effect. The key is to apply them in a thorough and comprehensive manner before creating any new health information network, not as an afterthought, and not as an after-the-fact band-aid solution.