Will current plans for the Nationwide Health Information Network undermine patient privacy and trust?

From my son's pediatrician to my father's specialist, physicians are talking about electronic medical records (EMRs). Instant widespread EMR adoption is a goal of the American Recovery and Reinvestment Act of 2009 ("ARRA" or the stimulus bill) [1], which provides financial compensation to healthcare providers and hospitals for "meaningful uses" of EMRs in years 2011 to 2015 [1]. If successful, ARRA will ignite a mass exodus from a prehistoric paper age into a tech-savvy networked cosmos called the Nationwide Health Information Network (NHIN) in which patient information flows seamlessly across computers, devices, organizations and locations as needed. For lasting success, special care must be taken to allow widespread sharing of patient information while protecting patient privacy, and that brings into question the recently released list of requirements from the Centers for Medicare and Medicaid that include no privacy incentives and the current NHIN approaches from the Office of the National Coordinator that lack privacy and utility.

Like many Americans, I pay bills electronically, email photographs, search the Web for supplemental health information, and complete so many functions online I rarely visit brick and mortar offices. Yet my son's pediatrician uses paper records like those of my father's pediatrician.

The technology mismatch is striking. About 61% of Americans looked online for health information in 2009 [3], but only 4% of American office-based physicians used fully functional EMRs in 2007 [4] even though evidence exists that using EMRs improves care [5].

The Centers for Medicare and Medicaid (CMS) just released the first of about three rounds of meaningful uses [2]. As these reimbursement requirements roll out over the coming years, the NHIN should eventually support about 100 meaningful uses. One is listing patient allergies and medications at the time and place of service [2]. If I present unconscious at a California emergency room, the NHIN would allow attending physicians to reference my Pennsylvania information. Naive solution: give patients smart cards containing relevant information, but smart cards alone cannot satisfy all uses (e.g. a lab sending timely results to the requesting provider). So,the NHIN should provide sufficient utility to support the full spectrum of meaningful uses.

Technical bliss also requires the NHIN keep patient information confidential. Privacy is essential to doctor-patient trust allowing patients to freely communicate intimate behaviors and details to physicians and physicians to freely store related facts and

notes. A significant loss of privacy in the NHIN will render it useless and can cause serious personal harm as patients seek to opt-out and doctors find unforeseen ways to hide sensitive patient information. ARRA specifies numerous requirements for patient privacy protection [1] yet the CMS list of meaningful uses for 2011 [2] includes no privacy incentives.

EMRs and the NHIN enable quick and easy sharing of patient information widely and in bulk for many worthy purposes beyond direct patient care. As data sharing increases, risk of personal harm tends to increase thereby intensifying the tension between limiting data sharing to direct patient care (more privacy) and sharing data widely (more utility). The techno-policy infrastructure that enables data sharing, the NHIN, controls this tension and the NHIN design can itself introduce additional adverse consequences and worthy uses. There is a false belief one must be traded against the other –i.e., to reap benefits of the NHIN, Americans must give up privacy. Unfortunately, the current NHIN approach is worse, making it unlikely Americans will have privacy or utility.

ARRA charges the Office of the National Coordinator (ONC) within the Department of Health and Human Services with promoting EMR adoption and NHIN development. Tasks involve identifying meaningful uses, aligning economic incentives, establishing information exchange standards, and promoting privacy protection mechanisms. ONC's job rivals the Twelve Labours of Hercules [6], as I have witnessed many of ONC's heroic accomplishments from the vantage point of the privacy and security seat of the HIT Policy Committee, a federal advisory committee established by Congress to advise ONC. I was appointed through a national search and am the only professional computer scientist.

With only months remaining before early adopters start using new and retooled EMRs to qualify for compensation in 2011, the time seems ripe to examine privacy and the NHIN and seek corrective action.

The current approach to NHIN design is "let a 1000 flowers bloom" [7]. Regional and state groups receive financial support from ONC but are left alone to navigate the immature technical terrain and make isolated decisions. The lack of overall architectural coordination promises autonomous local NHINs that are not likely to interoperate and can expose patient information to different hazards.

ONC's website describes the NHIN Limited Production Exchange (NHIN Exchange) as today's NHIN [8]. Federal entities (e.g., the Social Security Administration, the Veteran's Administration, and the Centers for Disease Control) lead the effort with participation from private parties (e.g., Kaiser Permanente).

Technical operations are: (1) *patient lookup*; (2) *document query*; (3) *document retrieval*; (4) *audit log query*; (5) *authorized case follow-up*; and, (6) *event messaging* [9]. These functions allow participants to locate patient information, identify available documents, retrieve patient documents, etc. The last operation, *event messaging*, stores criteria and automatically forwards matching patient information when it appears. Overall, this

is not a bad set of operations, but there are problems with the overall design. Here are a few.

Given explicit identifiers of a patient (e.g., name and Social Security number), *patient lookup* returns institution-specific identifiers for that patient using patient registries [10]. Each register is a master patient index containing patient name, telephone, gender, date of birth, Social Security number, the patient's unique identifier at each organization, and optionally, deceased information, marital status, religious affiliation, race, ethnicity and address. There are concerns with this approach. For example, insiders (anyone at any participating facility who can access patient information) can do malicious surveys to locate patients and patient records at other facilities. For example, a domestic violence stalker can use the system to locate victims.

In one version [11]*, event messaging* allows 3rd party notification of patient information without the patient's knowledge. This function may help public health agencies receive reportable information, but as designed, enables unsupervised surveillance. For example, an insider could receive notifications of all abortions performed at other organizations.

Participating institutions maintain patient information portals. If deployed widely, these portals would be in environments (e.g. provider groups) having no professional staff to follow the latest computer security practices.

Security additions may help but don't seem forthcoming and other concerns would still remain because of the overall design of NHIN Exchange. These problems are not inevitable as other possible designs don't have them. It is therefore prudent for local communities to understand how different technical designs for the NHIN have an impact on patient privacy.

ONC's website also describes NHIN Direct [12]. Microsoft and Cerner representatives mentioned replacing fax with email over secure channels to combat eavesdropping [13]. A crowd-sourced effort emerged [14]. Unpaid volunteers jointly construct technology for fax-based scenarios (e.g., provider-provider and provider-lab). One concern with this approach is an inability to achieve all meaningful uses due to over-fitting fax scenarios. For example, an emergency room doctor cannot reasonably retrieve allergies and medications for an unconscious out-of-state patient using email. How does the emergency room doctor know which provider to email? Will responses be timely? How does the recipient know the email is legitimate? The NHIN requires more machinery, but is NHIN Direct a stepping-stone or a distraction? No roadmap shows how the effort eventually achieves all meaningful uses. Common problems to email (e.g. spam, fraud, privacy) and free public labor (e.g. legal responsibility, software fusion) remain unaddressed. For these reasons, the utility of NHIN Direct is gravely uncertain.

It doesn't take a doctorate in computer science to know the prognosis for the NHIN is not good and it doesn't require political sensitivity to know what public reaction will be. With few months remaining and a desire that EMR adoption be successful and long

lasting, I propose an intervention. Develop a "flowerpot," a single conceptual NHIN defined by trust invariants based on stakeholder barriers (e.g. patient privacy and provider liability). A local NHIN participates in the flowerpot only if a risk assessment proves its implementation satisfies constraints. Then, no matter the services or technical architecture deployed by local NHINs, the overall flowerpot of NHINs gives universal responsible guarantees to patients, providers, and other stakeholders. So, "let 1000 flowers bloom" … *in a single flowerpot*!

1   American Recovery and Reinvestment Act of 2009 (ARRA). Public Law 111 – 5. http://www.gpo.gov/fdsys/pkg/PLAW-111publ5/content-detail.html

2   42 CFR Parts 412, et al. Medicare and Medicaid Programs; Electronic Health Record Incentive Program; Final Rule. Released 7/13/2010 http://ofr.gov/OFRUpload/OFRData/2010-17207_PI.pdf

3   Fox, S. and Jones, S. The Social Life of Health Information. Pew Internet & American Life Project. June 2009. As of 4/21/2010 http://www.pewinternet.org/Reports/2009/8-The-Social-Life-of-Health-Information.aspx

4   Hing, E. and Hsiao, C. Electronic Medical Record Use by Office-based Physicians and Their Practices: United States, 2007. CDC National Health Statistics Report, 23. March 31, 2010. As of 4/21/2010 http://www.cdc.gov/nchs/data/nhsr/nhsr023.pdf

5   Chaudhry, B., Wang, J., et al., Systematic Review: Impact of Health Information Technology on Quality, Efficiency, and Costs of Medical Care. Annals of Internal Medicine, Vol. 144, No. 10, 2006.

6   Ancient Greek mythology. See also Riordan, J. and Balit, C. Twelve Labours of Hercules. Francis Lincoln Ltd. 1997

7   Blumenthal, D. There Is No 'One-Size-Fits-All' in Building a Nationwide Health Information Network. Press Release. Office of the National Coordinator. U.S. Department of Health and Human Services. May 14, 2010.

8   NHIN Limited Production Exchange. Office of the National Coordinator. U.S. Department of Health and Human Services. As of 4/21/2010 http://healthit.hhs.gov/portal/server.pt?open=512&objID=1407&parentname=CommunityPage&parentid=8&mode=2&in_hi_userid=11113&cached=true (Archived at advancehit.org/NHINarchive/2/)

9   2010 NHIN Final Production Specifications. Office of the National Coordinator. U.S. Department of Health and Human Services. As of 4/21/2010 http://healthit.hhs.gov/portal/server.pt?open=512&objID=1407&parentname=CommunityPage&parentid=8&mode=2&in_hi_userid=11113&cached=true (Archived at advancehit.org/NHINarchive/3/)

10   NHIN Patient Discovery Web Service Interface Specification v1.0. Office of the National Coordinator. U.S. Department of Health and Human Services. As of 4/21/2010 http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11673_910524_0_0_18/NHIN_PatientDiscoveryProductionSpecification_v1.0.pdf (Archived at advancehit.org/NHINarchive/3/)

11   NHIN Connect. As of January 25, 2010, at http://www.connectopensource.org/display/Gateway/CONNECT+Community+Portal (Archived at advancehit.org/NHINarchive/4/)

12   NHIN Direct. As of 4/21/2010 http://nhindirect.org/ (Archived at advancehit.org/NHINarchive/5/)

13   Nolan, Sean. Prepared Remarks on Authentication. Testimony before the HIT Policy Committee NHIN Workgroup. January 7, 2010.

14   NHIN Direct Crowd-Sourced Wiki. As of 4/21/2010 http://nhindirect.org/