

**Personal Health Records & Web-Based Healthcare Delivery:  
Experts Discussion on Authentication & Identity Management**

**9am-12pm, April 11<sup>th</sup>, 2007**

**The Media Laboratory, Wiesner Building, E15  
20 Ames Street, Cambridge, MA 02139, 3<sup>rd</sup> Floor: The Roth Room,  
Contact: Daniel "Daz" Greenwood: 650-504-5474**

**Dear Invited Expert:**

Thank you for your interest in this thought leading topic and your willingness to join an open discussion hosted by the MIT Media Lab. We intend to provide a forum wherein each participant may share ideas and deepen our combined knowledge and perspectives on identity and authentication issues related to electronic records and transactions in healthcare.

**Preliminary Request:**

\* Please e-mail to me ([dazza@media.mit.edu](mailto:dazza@media.mit.edu)) a very brief bio or link and either 1) a brief (2-3 sentences or more) summary of one or more key problems and/or prospects you see for the use of identity management in the electronic purveyance of healthcare, or 2) One or two experiences or activities from your career that identify an issue or further context related to identity management in eHealthcare.

Please note, for the above, we're especially interested in focusing on identity management and authentication of individuals in cross-organization, multi-use and large-scale/production-grade (i.e. not pilot or trial) use in healthcare in such contexts as Personal Health Records, Online Diagnostics, Web-Based Health and Wellness sites and related healthcare consumer-facing networked contexts.

**Draft Outline of Relevant Issues**

The draft document (below) is intended solely to provide an initial frame to support deeper discussion of the relevant issues. It is hoped that the context and knowledge that develops during our discussion will permit us to re-write the draft (perhaps totally) and share a subsequent document on the MIT website that will help guide the broader public dialog on these issues. In any event, we are confident that each participant will leave the conversation with insights and information that will be of value as you continue your efforts in the field.

Best regards, and we look forward to seeing you on the campus of MIT soon!

- Daniel "Daz". Greenwood, Esq.  
Lecturer, MIT. Director, MIT E-Commerce Architecture Project



# **Attachment 1**

## **Invitee List:**

### Convener:

- \* Daniel "Daz" Greenwood, Esq. <dazza@media.mit.edu>  
Lecturer, MIT Media Lab

### Participants:

- \* John Halamka <jhalamka@caregroup.harvard.edu>
- \* Elliot E Maxwell <emaxwell@emaxwell.net>;
- \* Ethan Katsh <katsh@legal.umass.edu>
- \* Claudia Boldman <claudia.boldman@state.ma.us>
- \* Jennings Aske <Jennings.Aske@state.ma.us>
- \* Jason Snyder <Jason.Snyder@state.ma.us>

### Co-Facilitators:

- \* Dan Combs, <dan.combs@globalidentitysolutions.com>;  
National E-Commerce Coordinating Council
- \* Ray Campbell, <RCampbell@mahealthdata.org>;  
Executive Director, Massachusetts Health Data Consortium

## **Attachment 2: Draft Issues Paper:**

### **Personal Health Records & Web-based Healthcare Delivery: Authentication & Identity Management**

Introduction:

While much remains in play in the realm of personal health records and web-based healthcare delivery, it is not too early to begin a deeper dialog regarding authentication and identity management requirements and constraints for such systems. Every major government, non-profit and private sector report on PHR includes a section calling for strong authentication as part of strong security and privacy protections. However, at this point in time, the patient-touching healthcare field generally remains far behind other sectors of the U.S. economy. Integrated authentication of account holders, via inter-bank recognized PIN and card-token combinations, have long been a staple of consumer banking at Automated Teller Machines. Similarly, online banking and other financial services have mature and widely adopted web-based methods for authenticating account holders. Beyond banking and finance, many other large networks have also developed to support secure authentication of users on a large-scale, including for eCommerce, eGovernment, eLearning, Law Enforcement/Intel Information Sharing, Cyber-Warfare and remote workforce/VPN. The advent of several large-scale national identification and tracking infrastructures (including the federal government's TWIK system, the Real ID Act, and the E-Authentication Federation), have led some to consider whether an emerging national identity system can serve as an initial access point to unlock and use personal health records and transactions. It is clear that a national system of PHR remains many years away, and for that reason, it seems prudent at this point to consider a heterogeneous approach to healthcare consumer authentication and identity management for the coming years.

The dialog at MIT's Media Lab on April 11th will explore the applicability and desirability of existing and prospective options for authentication and identity management of end-users (health-consumers) for access to their PHR and to web-based healthcare delivery. How is consent managed across heterogeneous networked organizations? Who owns and controls the systems that permit interoperability and how will key decisions be made regarding use of technology, standards, upgrades, allocation of liability and strategy setting, inter alia? What are the expected large-scale, high-value or medically sensitive usage scenarios whereby a patient or other eHealth consumer will access records and conduct transactions? These are the types of questions that have animated this inquiry.

The following topics have been sculpted to focus on developing common understandings, identifying the areas where standardization is ripe, borrowing best practices from more

mature large scale authentication and identity system of other economic sectors and considering the highest value short and mid-term (2-5 year) business models and cross-organizational options for integration and interoperability.

Invited experts from relevant fields will investigate the following topics, and follow additional lines of inquiry that will doubtlessly arise.

## 1. Strong Authentication is Needed for Personal Health Records and eHealth Delivery

There is a need for strong authentication to assure security and privacy of personal health records. This is especially true when the underlying systems are more accessible via heterogeneous and distributed networks and organizations. However, there are many different ways to achieve strong authentication, and they involve corresponding trade-offs and priority choices. The types and methods of authentication and identity management have broader interdependencies and implications for business, related technologies, legal and policy requirements and constraints.

## 2. Identity Can Mean Different Things and Have Different Rights and Obligations

What is the meaning of “Identity” in this context, and what exactly is being authenticated when a user logs into a web-based personal health record or healthcare delivery system? (Does it mean that they are a customer of a particular pharmacy chain, or a patient of a certain hospital, or a customer of a particular HMO or a veteran not yet enrolled in a VA program, etc, etc? Context matters and is not “one-size-fits-all” where personal identity is concerned). Confusion and disputes resulting from incompatible understandings of underlying identity have slowed authentication efforts in other fields (EAI, EAP, SAFE, TPAs, etc). A simple example: it is not uncommon for the terms and conditions governing different systems to be different or even conflicting, and for consumers to be oblivious or legitimately confused their status and account rights/obligations from one connected system to another. This is, in part, due to a disconnect between the context and contours of their “identity” within each interoperating networked application and system.

Identity: Ownership and Control (note: scope limited to identity and authentication methods, not ownership/control of the underlying health data or financial or business records). Identity Management: First Day/Last Day Account Management (how are accounts created, names changed, rights modified, suspension/termination adjudicated, etc). Who is in charge of the Identity Management underlying authentication? How does the identity management system and authentication method used integrate with the end-user technology and respond to user requests and demands?

Authentication and Privacy: Fair Information Practices and Dispute Resolution: Authentication Privacy and Accountability Policies. (see, for example: <http://www.cdt.org/privacy/authentication/030513interim.shtml>).

### 3. Integration, Governance and Dispute Resolution Require Coordinated Efforts.

Cross-Boundary-Integration (XBI): Calibrating Coordinates on the Spectrum of Openness. (somewhere between a national white pages and a tightly closed one-organization-only system, allowing for relatively simple inclusion of or re-use by additional users and organizations).

Potential Applicability of Large-Scale Federated Models from eCommerce, Banking/ Finance and eGovernment: GSA's eAuthentication Federation (<http://www.cio.gov/eauthentication/documents/EAlaunchesEAfederation.pdf>), the SAFE bio-pharma initiative, the Liberty Alliance, etc.

Organizational Integration: When You Can Say "Yes, You Can Play". Deciding When, How and Whether Additional Parties May Rely Upon Authentication and Identity Information. Business to Business Contracts and Governance, Business Practices and Policies for Handling Authentication Validation, Suspension, Revocation, Reinstatement, Access, Dispute Resolution, Legal Rights and Obligations and Change Management for Migration to Future Authentication Platforms and Practices. There is no issue as important as dispute resolution in this context.

Note: the "governance" issue above deserves deeper attention. There are many ways to support and reflect cooperative agreements between partnering organizations. If a single large company or agency is clearly in control (e.g. the demand for the supply chain or the authorizer regulator), less nuanced governance among partners may be needed than in situations where the interoperating organizations must all agree and are of similar negotiating power. Creating of steering committees, joint-ventures with representative boards, new business partnerships, multi-state compacts and many other options exist, each with features and draw backs from governance and management perspective. A key success factor in large scale cross-organizational authentication and identity management systems are the multi-lateral agreements or other governing rules setting up the foundation for decision making, investment, dispute resolution, ownership and control of the technology, data and identities.

### 4. Observations Regarding Existing and Prospective Solutions

This section will be developed based upon feedback from participants prior to the meeting and from the fruits of our in-person discussions on April 11<sup>th</sup>. We hope to identify next steps and action items that would be helpful to carry forward the ideas captured or generated. It is expected that, at a minimum, MIT will publish a brief paper containing the key ideas and observations.

/end/