Written Public TESTIMONY of

Ashutosh (Ash) A Ghogale

Recognized Industry Subject Matter Expert

Previous Presentations and Submissions

State of Maryland IT Security and Privacy Conference

http://www.dbm.maryland.gov/dbm_publishing/public_content/dbm_search/security/tocitsecurityconferencesept2004.html

Few of the Representative Organizations Ash has been associated with (current, past, memberships etc.) include Deloitte, Center for Health Solutions (Chaired by Former HHS Secretary and four times Governor of Wisconsin Tommy G. Thompson) ,KPMG (BearingPoint), Maryland Dept of Transportation, PMI (Project Management Institute),BCBS, Tata, Corpus Inc, Symantec etc.

Testimony Before

American Health Information Community Confidentiality, Privacy and Security Workgroup Hearing Meeting

Federal Advisory Committee Act (Pub L.No.92-463, 5 U.S.C., App)

Department of Health and Human Services

Office of the National Coordinator for Health Information Technology

Established by White House Executive Order (April 27, 2004)

Sept 29, 2006

Director Judith Sparrow, Co-chairs Paul Feldman and Kirk Nahra distinguished members of the committee and "The Community". Thank you for providing an opportunity to respond to the questions posed for the testimony. It is indeed an honor and a privilege.

I applaud the work of this workgroup in its effort of making the Presidential directive for decade of Health IT a success. I respectfully submit this testimony with the hope that it will enable the members and public to gain better understanding of identity proofing and user authentication in HealthIT from a broad IT industry perspective.

Responses to questions posed

1. Does an in-person identity proofing process provide greater benefit than automated on-line processes, or vice-versa? Please explain.

Response – Both processes have their associated benefits and depending on the circumstances under which each process is implemented the benefits achieved will outweigh the risks associated.

In-person proofing has higher benefits and lower risks when applied to situations where a) An identity is being established for the first time b) Credentials or Documentation establishing the identity might require human verification/substantiation

Automated process provides more benefits over risks in situations where a) Proofing needs are repeatable b) Have to be available 24x7 c) Identity has been established earlier and needs only to be reconfirmed.

2) Identify and particular concerns regarding the type of information collected for identity proofing or the storage of such information.

Response – Some of the concerns regarding the collection of information are a) Privacy b) Sensitivity c) Legal considerations. Concerns regarding the storage of the information are a) Data maintenance and accuracy b) Data encryption (any encryption technology used today can be broken tomorrow except maybe quantum cryptography) c) Data Ownership e) Storage Costs. It is essential that proper guidelines and procedures be established before any kind or PHI or sensitive data is collected and stored.

3) Should there be different identity proofing and user authentication processes for:

a. A patient versus a clinician. If yes, please explain and identify the scenario;

b. The primary user of a PHR versus a proxy for that user?

Response:

a) Yes. Even though the technology behind the authentication processes for a Patient and a clinician can be shared proofing processes for both have to be different. For example a clinician performing a specific procedure may need to be proofed against his current credentials in that field which may require interfacing with external certifying authority.

b) Yes and No. While it is preferable to have different processes for both considering the risks and the costs associated it is usually technically more feasible to have them shared across both the roles with only minor role based variation.

4) Are there other industry policies and practices related to identity proofing and user authentication and could be used successfully in any of the Community identified breakthroughs (see above)? If so, please described these policies and specify how these could be implemented in a way that would minimize the risks and maximize the benefits as well as how they would compare to alternative methods in terms of risks, benefits and feasibility of implementation.

Response: A combination of PKI[1] (Public Key Infrastructure) and Digital Signature technology can be successfully used and leveraged for the purpose. PKI is not simply software or hardware. It is an infrastructure, that is, a combination of products, services, facilities, policies, procedures, agreements, and people that provide for and sustain secure interactions on open networks such as the Internet. The infrastructure provides assurances that information is protected while being entered, during transit, and when stored. The underlying technology is already developed by private industry and is being marketed and used commercially. The PKI promotes interoperability

[1] Ref : NIST Special Publication 800-25 Federal Agency use of Public Key Technology for Digital Signatures and Authentication

among commercial products and the early integration of security features into those products. Three areas of risks associated with the use of public key technology are (a) fraud; (b) failure of the system to fulfill its purpose (service failure or shortfall); and (c) liability. The use of digital signatures may actually reduce risk compared to existing electronic and paper-based processes. Once a digital certificate has been properly issued, the ability to impersonate usually reduces to a simple question: can someone get that party's private signature key used for making his or her digital signature? If not, then identity fraud becomes extremely difficult. There are reasons to believe that public key infrastructure-based systems have the potential for substantial public acceptance for transactions in the private sector. Historical data as in the use of Credit Cards and Mobile phone technology fully supports this.

5. What is the appropriate balance of access to medical information in electronic form (through the use of stronger identity proofing and user authentication) against the privacy concerns of the consumer/patient? If possible, please discuss comparable programs/efforts in the past that have been successful in doing this?

Response : There are reasons to believe that electronic information in electronic form have the potential for substantial public acceptance even if it creates more privacy concerns and creates increased uncertainty about prosecuting certain kinds of fraud owing to legal factors, such uncertainty may diminish with time as legislation is enacted or case law develops. The risks may be far outweighed by the economic and other advantages gained. For example, use of credit cards beginning in the 1950s significantly increased potential and actual fraud compared to the use of checks or other paper transactions for exchanging funds. Yet, as history has shown, the public has accepted that the benefits derived far outweigh the drawbacks. Likewise the potential for fraudulent use of cellular phones is far higher than for hard-wired phones in one’s home, yet once again, the public has accepted that the benefits of cellular phone use far outweigh that drawback. Additionally, in both situations, industry has adapted and developed new controls and technology enhancements to reduce fraud while continuing to experience tremendous growth in these sectors.

6) What/how do you see the HHS's role, if any, in establishing guidelines for the health care industry with respect to identity proofing and user authentication? Or should the industry self-police in this area?

Response: HHS should act as a catalyst and establish broad guidelines for the Industry .The guidelines should be broad and open enough to facilitate Industry innovation while facilitating interoperability Enforcement and implementation aspects of the guidelines should be left to the industry.

7) If private industry EHR or PHR services were to import data from Federal agencies (who are required either by statute or policy to protect data in certain ways), would it be reasonable to expect that the EHR or PHR service provided would comply with Federal information security practices?

Response: Yes it is a reasonable expectation but the practicality of implementation is very thin. With current high healthcare costs and outsourcing trends it will be difficult to enforce the information security practices among service providers.

8)Should the health care industry adopt the concept of multiple assurance levels when performing identity proofing and user authentication functions, similar to what OMB *has defined for the Federal Government in OMB Memorandum M-04-04? When responding to this question, please cite, if possible other models that may exist specifically for health care?*

Response: Yes the industry should adopt similar model. While the OMB Memorandum defines four assurance levels along with the risks and potential impacts associated with them another important factor to be considered in case of the HealthCare industry is Time. Response time especially on the provider side in case of emergency situations will have to be factored in to the assurance levels for a similar model in Healthcare industry.

9) Based on your experience (personal/organizational) discuss how identity proofing and user authentication are currently addressed in the Personal Health Record (PHR) market from a technical, policy, and implementation perspective. Please ensure that your answers identify:

a. How the type of PHR (i.e., who provides/sponsors the PHR) could impact the identity proofing and user authentication method chosen;

b. Who is capable of providing data to the PHR;

c. The potential impact the type of data (which may vary in levels of perceived sensitivity, e.g., a medication history that lists a drug for an ear infection versus a drug for HIV) could have on the identity proofing and user authentication method chose; and

d. How data is entered into the PHR, for example, by a health care consumer, or from a provider through a ``push model'' where data is automatically sent to the PHR without a request by the consumer.

Response:

As Government agencies and health systems start initiatives for increased PHR adherence with Executive[2] and bi-partisan congressional support [3] the PHR market is gaining more and more visibility. Being in the initial stages the current security and privacy mechanisms, policies and technical implementation of those policies in a PHR including user authentication and proofing are heavily dependent on the user equipment (desktop/laptop/software) and also the mechanisms provided by website (example WebMD) offerings. User, Providers, Testing facilities have the ability to update the PHR, given it has been set up properly for the same. An automatic update of the PHR and alert/notification to the physician on an adverse drug interaction might can many times be a lifesaving event. To summarize current PHR security and privacy mechanisms regardless of which model they follow (push/automatic) are more tailored towards facilitating alerts and notifications.

10) Based on your experience (personal/organizational) with EHR technology, that can at a minimum provide access to current and historical laboratory results and interpretations, should identify proofing and user authentication methodologies (technical, policy, and implementation) differentiate based upon:

a. The reception method of the data

i. For example: Accessing a laboratory's secure Web site for results and typing them into a patient's EHR vs. automatic population from the lab to the EHR; and

b. The interconnectivity of the EHR

[2] President Bush 2004
[3] Gingrich and Kennedy 2004

i. For example: A doctor in a large health care system may be able to query another provider's EHR for data as opposed to querying the lab directly.

Response: Yes. Identity proofing and user authentication methodologies (technical, policy, and implementation) should differentiate based upon the reception method of data and the interconnectivity of the EHR. Specifically if we consider a) Reception method of the Data – Data being received from a testing facility may be in Batch or bulk mode while data reception from individual users will be in form of single updates and transactions. It will be much more proficient if the underlying authentication and proofing techniques and processes are designed accordingly. Also the connectivity and polling intervals of established connections will be different in all the three cases. A secure connected connection will need to be authenticated and proofed only while making a connection while an individual transaction coming over across the internet will need to be authenticated each time.

In closing I would like to again thank advisory Committee members for providing me the opportunity for this testimony. I hope the responses have been beneficial to the community and will help further the committee and workgroups cause. Please feel free to contact anytime and I will endeavor my best to answer any queries or provide more details

Thanks

Ashutosh (Ash) Ghogale

Contact info: Email – AGHOGALE@HOTMAIL.COM

Cell phone : +001.312.933.8171