# Confidentiality, Privacy & Security Workgroup

Testimony Before the U.S. Department of Health and Human Services AHIC Confidentiality, Privacy and Security Workgroup

Statement by Mark J. Jacobs, MHA, CPHIMS, Director of Technology, WellSpan Health – York Pennsylvania

I would like to thank the U.S. Department of Health and Human Services (HHS) and the American Health Information Community (AHIC) and the Confidentiality, Privacy and Security Workgroup for holding this public hearing. It is my hope that today will be a turning point in helping community care providers and large integrated delivery systems find common breakthroughs to resolve the massive Identity Management and proofing challenges we face in health care today. WellSpan Health is located in South Central Pennsylvania and includes two hospitals, a tertiary care center with Trauma Services, and more than 7000 clinicians, employees and support personnel. We have 52 outpatient physician practices with 750,000 office visits annually. Wellspan's Outpatient business exceeds inpatient. We utilize over 100 clinical systems, applications and digital products that provide access to more than 32 service lines in 70 points of care. WellSpan's need to fulfill data protection requirements, work under the guidelines of the Health Insurance Portability and Accountability Act (HIPAA), as well as maintain regulatory and audit requirements have forced us to invest in a myriad of security solutions for identity proofing and user authentication. We have been developing our own breakthroughs to allow safe and secure clinical access, adding overhead to the Electronic Health Record. Sometimes, our layers of security impede care, leaving open the possibility of one day limiting our ability to share with other care providers outside of our organization. It is not uncommon to hear the words, "lock-it-down", "prevent", and "restrict". Restricting the use of patient information is important from a privacy and security prospective, but we need to differentiate the roles of the users.

The American Health Information Community can provide the Healthcare Industry with 1) Specific Minimum and Reconcilable Standards that are interpretable for Identity Management and User Authentication and, 2) Guidelines for Role Based Identity Management.

Some of my colleagues are skeptical of the industry's ability to standardize identity access and identity proofing without Federal mandates. However, I prescribe to the opinion that such standards are achievable collaboratively. I am here today to share with you our challenges. I hope to take back to my colleagues a message that the paradigm is shifting and we will solve the problems together.

There is currently no single path for user authentication and identity access. Yet, I believe that we need to provide quick access to the electronic health record to succeed in this endeavor, before we replace paper and film completely.

As care providers, we have already made a huge investment to acquire the Electronic Health Record applications. Now we are faced with additional spending to achieve a secure layer for secure access. At the same time, we add tools (i.e. single sign-on, proximity access) that will make the access quick and easy for the physician. Our greatest challenge will be to safeguard the patient data once it has moves beyond the protection of WellSpan, while facilitating the appropriate sharing of information between the care venues the patient traverses to allow better and more coordinated care. Standards must be agreed upon and universally adopted if we are to meet the goals outlined by the President's Executive Order for Health Information Technology. The gathering of collaborative thought will one day allow the achievement of an agreeable model as a guide for secure access.

My testimony will address four:

- Challenges Health Providers face in Identity Management
- Providers view on Identity Proofing, User Authentication and Provisioning

- Testimony relevant to Secure Messaging for physician practices
- Provide a vision of the future for the care provider who is committed to reasonably protect yet share digital health information with the community

First, let me outline the industry's challenges in providing secure access and identity proofing of their Electronic Health Care Information. The most obvious difference is in the scope of dimension and complexity of the different classifications of care givers requiring access. Since the year 2000, the demand for user maintenance in Identity Management has risen from 5099 to over 12,173 in 2006 at WellSpan, doubling in the last three years. Centralized management versus federated security and access control is a delicate balance for "timeliness" of access. For example, Identity Management and proofing alone is a significant challenge for employed versus non-employed physicians, and for credentialed physicians with admitting privileges to our hospitals versus non-credentialed physicians. Extending role-based access and identity proofing beyond the physician to the medical student, resident, nurse or nursing student, adds to the volume and adds a new layer of complexity to user access management.

Timeliness of access is often a challenge. Allowing full open access is not an option when interpreting HIPAA, 3rd Party Audits and security reviews. Yet, it is not uncommon to see "open door" access to clinical data still occurring in some organizations today. From a clinician's view, security and identity proofing is often seen as impeding care by appearing to be too restrictive. In a large integrated health care setting, the Electronic Health Record represents not one, but many clinical applications and databases. The challenge for the American Health Information Community and the Confidentiality, Privacy and Security Workgroup is to establish a workflow standard for each classification of user accessing the Electronic Health Record.

At WellSpan, we have begun the process of simplifying access to the Electronic Health Record by branding "eCare" as a single reference for clinicians to request up to eight different

best-of-breed vendor systems, ranging from an inpatient Electronic Health Record, Picture Archive and Communication Systems, Ambulatory Electronic Health Record, Email, Patient scheduling, and Clinicians notes to name a few. At WellSpan, we envision an automated online role-based identity proofing process that uses "proof of address" (i.e. credentials, copy of a physician license, employee number, or unique number).

In-person identity is still the ideal and most secure method. Online access should require a "multi-layered" identity verification process. Most vendors are moving to three-factor identity proofing (pass phrase, token and biometrics). However, this is costly and complex when compared to traditional in-person identity checks. In the case of WellSpan's identity process, a two-factor authentication (which the physician has and knows) is seen to be reasonably effective in establishing the initial account, while employing annual online proofing. For remote access to our "eCare" products, a password followed by a pass code (PIN) is seen to be more acceptable versus a token or added biometrics. Routinely, the account is verified and attested to when passwords are reset using an automated compliance tool.

For Identity Management on an initial user setup, a physician is required to provide a physician number, while a nurse provider may access based upon their license number. Both identifiers are fairly accepted with little objection raised.

Any physician credentialed by our organization can request access to WellSpan's Electronic Health Record. Employed physicians are pre-authorized by our Human Resources Department. The difficulty arises in the case of independent, non-employed physicians. We have developed an automated verification against our credentialing database which verifies the alpha/numeric last four digits of the physician's license number and other criteria specific to the physician as an individual.

Secure messaging is being piloted by several of our offices. More than two hundred patients are enrolled through a written patient authorization, now allowing digital dialogue through secure online forms. The barriers encountered do not seem to be voiced by the patient but the office staff. The enrollment process occurs at appointment check-in, where the patient signs an Authorization Consent. A confirmation which includes instructions, ID and password are mailed to their home.

Once the patient has access they can access health education and dialogue with the physician's office through Secure Messaging. The options in use today include "Ask a Billing Question? Ask the Nurse a Question? Request a Non-Urgent Appointment, and Request a Prescription Refill".

The most frequently used is "Ask the nurse a question?" Secure messaging between the physician's office and the patient is of a non-urgent nature. Patients usually inquire as to how secure messaging differs from email. We find that a better understanding of the meaning of Secure Messaging in health care would be beneficial in the industry. From the practice's perspective, secure messaging is viewed as a valuable tool that allows non-urgent issues to be handled in a way that doesn't detract from urgent issues. Our nurses wish patients would use secure messaging regularly. From a patient's perspective, they are able to communicate conveniently with the physician's office without having to deal with an automated phone system, or long call waits. In our experience, patients appear to be very open to signing authorization consent for access and have not raised significant issues regarding confidentiality. Password expirations seem to trick patients from time to time but we view this as a necessary evil. We are promoting secure messaging for our Coumadin patients through a mass mailing invite. This will allow us to contact patients through a secure message center regarding the results of their INR test instead of by phone.

In some instances, providers who use email to dialogue with patients have been seen to do so through un-encrypted secure messaging. WellSpan chooses to be bit more restrictive.

A Personal Health Record is also available through our web site securely hosted. Our patients can record and access their health history and share with their provider anywhere they go.

In the areas of secure messaging and identify proofing, there may not need to be different levels of authentication, merely a method that works. The same scenario could apply to physicians, clinicians or proxy. The process would start with in-person for the initial account setup and the recording of the two or three factor digital identity. The level of access would be dependent upon the pre-assigned role of the user initiating the access. The digital identity could expire after a routine time period, and then be renewed through in-person registration proofing. The clinician would require access to much more detailed medical information, lab results, physician notes and patient demographics in order to complete a diagnosis. Because of the privacy issues, a proxy may not have access to specific medical information unless the patient has "opted-in" by consent. Therefore, identity and authorization would be the same for the patient, a clinician or proxy, but their level of access would be determined by the assigned role. The data should always be encrypted to prevent inappropriate disclosure.

The technology industry practice of three-factor digital identity (pass phrase, token/pin and biometrics) could always be adapted Secure Messaging. Lower cost encryption standards like PGP (Pretty Good Privacy) for Secure Messaging combined with multiple-factor Identification proofing such as a PIN, might be reasonable. Other encryption standards such DES as (Data Encryption Standard) or AES (Advanced Encryption Standard) might be also considered. As we debate the solutions and security risks, our patients and doctors move forward acknowledging and accepting the lack of security in luau of efficiency.

The policies governing methods of identity verification should be specific to the targeted industry. The military may require greater authentication for access to tactical information than a manufacturer of tires. Healthcare needs a leading hand right now to acquiring specific, reconcilable and sustainable guidelines user authentication and identity proofing that do not allow vague interpretation based upon the personal and private nature of the information involved and the regulatory mandates in place. Medical information may not be viewed as tactical as military information; however, unauthorized release of information can be equally devastating to an individual.

WellSpan currently uses a modified version of two-level authentications for in-house access to its systems. Employed caregivers have unique user names, passwords, and an employee number for access. Every employed clinician also has an Identification badge. With the inclusion of a smart chip in the Identification card, WellSpan would be positioned to easily move to a three-layered authentication schema for a username, password and a smart card.

I'm not certain how we will finally agree to properly secure our Electronic Health record, but we must secure electronic access as we transition from paper. The financial industry secures, authenticates and proofs millions of users each day.

Going forward, the role of the individual should determine the amount of access to patient records. The principle of minimum necessary access still applies to healthcare since the caregiver is still seen as the gatekeeper. The user identity information (username, password, and a secondary identity device or biometric) determines the role set for them and the level of access to medical records. The handling of patient health information is covered, in general reference, on the medical disclosure statement handed to every patient.

The requirements for user identification, authorization, and encryption of all transmitted health information should be guided by Health and Human Services and can be facilitated through

accredited Regional Health Information Organizations (vis-à-vis audits, clearances, certifications). On a micro level, Wellspan has implemented a similar Information Security Access Collaborative (ISAC) and has accomplished some breakthroughs in identity management and user authentication enterprise-wide, previously not seen. The breakthroughs are formally solidified through our Information Quality group who formalized the process. This effort might be propagated through formal compliance schema developed by HHS for RHIOs.

From the aspect of the private sector, more than one vendor for each security product would need to be approved in order to spur competition. An approved methodology would make it easier for autonomous systems to communicate with each other when necessary.

Today's Health Care Industry should adopt the concept of multiple assurance levels for identity proofing and user authentication. If a person's banking information can be made secure and accessible, why shouldn't a person's most personal and private health information be just as secure and accessible? The Electronic Health Record would be accurate and secure, for a person from cradle to grave.

Finally, in an ideal Health Care world, a national patient identifier would be idyllic for good sharing of information. The military and Veterans Administration have realized the value in its use long ago. In the mean time WellSpan's physicians, in Pennsylvania will continue to be challenged with reconciling their files with other providers such as Hershey Medical Center, Mayo Clinic or maybe some day Keiser Permanente in California.

Respectfully Submitted by:

Mark J. Jacobs, MHA, CPHIMS

WellSpan Health