

**Statement of Don Sepulveda, GE Healthcare  
for Virtual Hearing on Trusted Identity of Patients in Cyberspace held by the  
HIT Policy Committee Privacy and Security Tiger Team and the HIT  
Standards Committee Privacy and Security Workgroup**

November 29, 2012

Hello, my name is Don Sepulveda, and on behalf of GE Healthcare, I would like to thank you for this opportunity to share with you our experiences and insights regarding patient identity proofing and authentication.

GE Healthcare provides medical technologies and services shaping a new age of patient care. GE's health information technology (HIT) products cover a broad span of clinical, administrative, and financial applications serving customers who range from small physician practices to large integrated delivery networks. Our electronic health record (EHR) products and related technologies are especially relevant to this hearing, and to the HITECH Act. GE Healthcare's broad portfolio of provider solutions incorporates both natively developed as well as 3rd party applications to our customers.

My remarks today will focus on our U.S. experience with patient portal solutions, which are a key component of our product portfolio. We offer several portal solutions, which tend to vary by customer size and complexity. We provide solutions for large enterprises to single providers, who combined, represent millions of patients across the country.

I first want to emphasize that the "Risk" profile that needs to be considered for patients is very different than that for healthcare providers. An improperly identified provider exposes all records in the EHR. An improperly identified patient ID exposes one record, and usually in a read-only form. There already is much effort ongoing to create identities for providers –such as Direct, DEA, and CMS. – and these projects are focused on very high value identities, thus needing high-assurance but also justifying the costs. As we balance approaches for assuring secure patient identity, we need ways that are focused on the risk profile of patient access.

In reviewing each of the solutions that integrate with our EHRs, we find that they are all very similar in the manner by which patient identity proofing and authentication takes place, generally using a system of usernames and passwords and technology and process solutions to validate initial user identity. For example, as it relates to identity proofing, it is common to use information that is known by the organization about the patient and a secret passphrase to support online sign-up. This approach uses information like the patient's name, address, date of birth or other demographic data designated by the healthcare provider. Then either a PIN or Temporary password given by the provider organization would be used to give the initial access to the patient, at which point they would create their own password. The PIN or Temporary password may either be provided in person at the clinic, or sent via secure message to the patient. Most provider organizations prefer to provide this information while the patient is physically in front of them at the clinic. This method not only is most accurate, but also provides more influence on the patient to actually go to the portal and sign up. Many providers will even have on-site kiosks to have the patient authenticate before leaving the clinic.

Of course, the workflows by which the identity proofing takes place can differ depending on the integration with the EHR. But, the methods that I have described are common, as they have become best practices as established over years of use.

Using other methods, such as 3<sup>rd</sup> party identity proofing solutions have been investigated, but currently, we have not deployed any of these given patient concerns regarding the personal information used by the 3<sup>rd</sup> party solutions, which tend to make patients nervous about how their healthcare provider would know such information about them. Such questions can include “your most recent mortgage payment” or “the address where you lived at 5 years ago”. Additionally, this type of personal information brings up concerns related to patient confidentiality when a divorced spouse or emancipated child may learn about such information, providing potential access to sensitive information when that access has not been approved by the individual patient.

This issue highlights the more general set of Further challenges exist that relate to family access to accounts and healthcare information, involving such scenarios as parent/child, spouse/spouse, child/elderly parent. Such access is commonly needed from a care taker perspective, and identity proofing and providing access to multiple patient charts using a single portal account is available today. However, when a patient no longer wants others to access their information, the process to end the access currently requires a call to the clinic to have the access of the other individual(s) removed. This is probably not the most ideal workflow and is an area where continued improvement is needed.

I should also note that some of the patient portal systems integrated with our EHRs allow for 3<sup>rd</sup> party authentication using tools such as LDAP, OpenID or other types of identity and authentication software. These are generally used by larger enterprises that use these tools across their entire solutions portfolio and are locally hosted within their own network infrastructure. This approach seems to work well for such larger and more sophisticated environments, which can consistently deploy their policies and manage their entry points into their solutions. The cost of these types of solutions currently may be prohibitive to many providers other than large enterprise institutions.

For smaller provider organizations, the costs associated with identity proofing involve primarily the time and effort used by the staff to manage the access to the portal for their patients. During the implementation of the patient portal, workflows will be designed to best meet their patient capacity and staffing levels. In the context of such costs, however, many of our customers have said that the most expensive portal is the one not actually used. Through active use of the portal by both patients and their representatives and providers, the savings achieved by the providers and staff in workflow efficiencies, for example allowing patient self-service for immunization records, medication refill requests and online history forms far outweighs any costs for the provider to manage the system.

In summary, patient identity proofing and patient authentication is critical to ensuring the security and privacy of patient information. We believe that many of the portal products used with our EHRs have evolved to similar methodologies and have formulated best practices for implementation of these workflows consistent with HIPAA requirements and patient and provider needs, balancing risks, costs, and benefits. Although certain challenges remain, the utility of a well-used portal will generate substantial benefits for both the provider and their patients. As we consider the evolution of patient identify proofing technologies and approaches, it is essential to consider the actual risks, best practices from other industries relating to online

access, the cost to providers and patients, and the impact, both positive and potentially negative on patient acceptance use of the portal.

Finally, I would like to underscore GE Healthcare's strong commitment to robust security and privacy practices to protect sensitive patient information. In addition to our work internally and with partners and clients, we are involved in efforts to develop solutions to the e-identity in cyberspace: problem. For example, GE Healthcare technical experts are actively involved with such initiatives as NSTIC, the S&I Framework, Direct, HealthWay, IHE, ISO, HL7, DICOM, and others. We look forward to leveraging identities that can be safely reused rather than proliferating multiple identities. Our primary focus and objective in these efforts is the right balance of usability and privacy/security.

On behalf of GE Healthcare, I want to thank you for this opportunity to share our experiences with you today.