

## **SDO Digital/Electronic Signature**

### **Testimony before the National Committee on Vital and Health Statistics, Subcommittee on Standards and Security**

**February 1, 2001**

My name is Glen Marshall. I am speaking on behalf of Health Level Seven (HL7), an ANSI-accredited standards development organization, as a co-chair of its Security and Accountability special interest group. Professionally, I am a healthcare system architect employed by Siemens Health Services (formerly known as Shared Medical Systems) and have worked in healthcare IT for 34 years. My focus is on healthcare Security and Privacy systems.

Here are my responses to the questions provided in my invitation to testify:

**1. Why is your SDO interested in electronic signatures at this time and what business processes will be enabled or improved by electronic signatures in the future?**

Although the HIPAA transaction standards, including the proposed claims attachment standard, do not currently require electronic signatures, we believe that future transactions considered for adoption and the expansion of the scope of claims attachments will ultimately lead to such a requirement. Electronic signatures will facilitate mutual authentication, data privacy, confidentiality, integrity, and nonrepudiation. They will also enable a clear representation of the authority and intent of those accountable for the data. We also believe that current cross-industry standards for electronic signatures do not meet these requirements for the healthcare community in general, while the healthcare-specific standard does not hold sufficient promise of being widely implemented.

Absent an electronic signature standard that meets healthcare requirements and can be widely implemented, any HIPAA rule would require trading partners to integrate one-of-a-kind software and/or develop bilateral specifications that interpret the standard. This is contrary to the spirit of administrative simplification and would likely cause provider organizations to opt out of using the underlying transactions.

The current state of electronic signature standards and technology demands a proactive effort by SDOs to develop and deploy a comprehensive standard that can be implemented within the expected compliance timeframe once regulations are published.

**2. What electronic signature standards are practically being used today, to what extent are they being implemented, and for what purpose, in connection with the standards developed by your SDO?**

Today, electronic signatures are most typically used when establishing a secure connection over the Internet rather than in conjunction with any given messaging or transaction standard. That is, at least one of the computers in the connection possesses an X.509 digital certificate and uses a public/private key scheme to establish an encrypted connection. This connection has the attributes of confidentiality and integrity. Data communicated over the channel is secured by a key known only to the connected machines such that any change to the data, whether accidental or intentional, produces a clearly invalid result upon decryption.

**3. What are the problems or limitations of your current electronic signature methods?**

Today's secured connections lack the attribute of mutual authentication unless both endpoints of the connection possess a digital certificate. Because of this, they also lack the ability

to assert nonrepudiation. Mutual authentication and nonrepudiation are important attributes for healthcare data.

Currently implemented standards only authenticate the computing device. They are unable to convey the credentialed authentications of end-users in a data exchange nor the intent, attestation, authority, and accountability of the sender.

Some individual health information systems provide electronic signature capabilities that apply to data stored in their data bases but, in the absence of implemented standards, the signatures are not represented in a manner that is persistent and portable and that provides the ability to detect subsequent alteration of the information that was putatively signed. As stated in the NPRM, electronic signature standards that meet these requirements will certainly require the use of digital certificates; at the same time they must handle the use case where the signer is a consumer who does not have a portable digital certificate.

**4. To what extent do you believe that a HIPAA standard for electronic signatures will benefit the healthcare industry? Do you believe a HIPAA standard for signatures is possible? How would you go about adopting such a standard?**

Electronic signature technology can help substantially reduce the latencies and costs of manual and paper-based processes, both for the transmission and retention of information. The savings desired from HIPAA administrative simplification will not be attained without a systematic reduction of such latencies and costs. A standard for healthcare electronic signatures would support such a solution – assuming requirements for privacy, confidentiality, credentialed authentication, integrity, nonrepudiation, intent, authority, and accountability.

A HIPAA standard for electronic signatures is quite possible, presuming cooperation among SDOs. This cooperation should start with an effort aimed at using *existing standards*, creating implementation guidelines, and culminating in an interoperability pilot project among vendor participants. It is key to note here that existing standards may well suffice, and all that is needed are proofs of implementation and interoperability.

Representatives from HL7, ASTM, X12N, NCPDP, and IETF EDIINT met on January 8, 2001, to initiate such an effort. We agreed to produce a consensus scope statement and work plan by March 31, which I will author.

Assuming positive results and learnings from this initial effort, we may expose a need to update the existing standards. This will require action by the SDOs who are responsible for the standards, using their own processes. A HIPAA electronic signature standard itself, referencing the resulting standards used in the interoperability pilot and any updates to them, can arise from this step.

**5. What will be the impact of adopting a standard under HIPAA that is different from the electronic signature methods you are using today? What will be the advantages and disadvantages? Will your SDO support such a standard?**

As mentioned earlier, the impact of a HIPAA electronic signature standard will be to facilitate mutual authentication, data privacy, confidentiality, integrity, and nonrepudiation, while representing the authority and intent of those accountable for the data. Today we can

only achieve machine-to-machine confidentiality, authentication, and integrity, which are not sufficient to the requirements of healthcare privacy and accountability.

The key disadvantages – perhaps better stated as challenges – are in the implementation. Current digital signature software does not support existing digital signature standards, either industry-wide or healthcare-specific. We will require the active involvement of vendors in an interoperability pilot to demonstrate workable implementations that meet the healthcare requirements based on existing standards. Recruiting such vendor participation will be part of the work plan.

HL7 will support the outcome of joint SDO efforts toward a recommended HIPAA standard for electronic signatures. As co-chair of the HL7 special interest group responsible for security and accountability, I will be personally involved in that effort.

**6. How could your SDO work with other SDOs and with NIST in coming up with such a consensus electronic signature standard?**

As noted above, a cooperative work effort was initiated on January 8. We will publish the scope statement and work plan by the end of March 2001. Although NIST was not a participant in the January 8 meeting, they were identified as a source of input to the effort. NIST participation will be considered as an element of the work plan.

**7. What do you estimate will be the time frame for development of a consensus electronic signature standard that could be adopted under HIPAA?**

I estimate a completion date some 9-12 months from the publication of the work plan, assuming a sufficiently high level of effort from each participant. At the end of that time the implementation guides and any related updates to standards should be ready to be balloted. Actual adoption depends on the meeting schedule and standards-approval processes of each SDO. To the extent that HL7 would need to conduct a ballot for this process it can do so over the Web without the requirement for a face-to-face meeting, consistent with the policy of the American National Standards Institute. We balloted the implementation guide for HIPAA Claims Attachment in two months.

**8. What should be the role of the HISB and of NIST in developing such consensus standard?**

I see HISB providing direct coordination of the multi-SDO project and NIST providing technical guidance on the robustness of the standard and coordination with other government electronic signature projects.

**9. What role would you like the NCVHS to play in this area?**

NCVHS should review the work to ensure that the requirements of healthcare and HIPAA are represented in the various products of the project. Relative to just HIPAA, NCVHS needs to help advocate the adoption of an electronic signature standard.