

Practice Incentives Program eHealth Incentive Requirement 1 – Secure Messaging Capability

Technical Workshop #1 – Meeting Summary Sydney 8 April 2009

Overview

A Technical Workshop on Secure Messaging was held at the Stamford Plaza at Sydney Airport from 9.30am to 4.45pm on 8 April 2009. NEHTA hosted the workshop with MSIA. Representatives from approximately 15 organisations within the medical software industry attended.

Presentations are available on the NEHTA website at www.nehta.gov.au/pip in *Documents & Presentations* link.

The following is a summary of the sessions that were conducted on the day.

Introduction

Tina Connell-Clark NEHTA, John McMillan NEHTA, Vince McCauley MSIA

Tina and Vince jointly chaired the workshop and welcomed participants.

John outlined that the secure messaging specifications will be collaboratively developed between NEHTA and the medical software industry. NEHTA has proposed a 'strawman' for secure messaging as a base point to commence discussions. Objectives for this workshop were to agree process, framework, identify issues, gaps, timetable and next steps.

Vince outlined that NEHTA is also working with jurisdictions as well as the private sector. Differences of opinions will exist during the consultation process but we need to work through the issues and move forward together in a positive manner.

Issues or Concerns that were raised included:

- Currently up to 10 MSIA nominated members are covered for travel expenses for the workshops. It was requested that NEHTA consider funding up to 15 members.

Member Introductions / Skills Register

Tina Connell-Clark NEHTA, Vince McCauley MSIA

Each person in attendance at the workshop outlined their details including organisation and background. This information will be recorded into a separate Skills/Contact Register. A list of attendees at the workshop is available in Appendix B.

A review of those suppliers on the Eligible Supplier list at www.nehta.gov.au/pip-vendors was also conducted. A follow up of those who had signed the Statement of Commitment but had not participated in the workshops (either by organisation or MSIA/AIIA representation) would be conducted between NEHTA/MSIA.

Issues or Concerns that were raised included:

- If a supplier didn't continue to meet the PIP compliance requirements, would they be removed from the list and how would it impact the Practice quarterly payments? Feedback will be requested from Department of Health and Ageing.

Terms of Reference

Tina Connell-Clark NEHTA, Vince McCauley MSIA

Outcomes of this discussion were:

- Terms of Reference document for the Secure Messaging working group was required to be drafted by NEHTA and agreed by the working group.
- Code of conduct was deemed necessary.
- Confidentiality Agreement wasn't deemed necessary as participants were requested to ensure confidential issues remained within the workshop.
- Workshop is not exclusive to MSIA members and legitimate secure messaging suppliers who are willing to actively participate in the working group are welcome to attend. Option to co-opt individuals with expertise relevant to discussions.
- To ensure the workshop is kept to a manageable size, only one representative from each company could attend. For consistency, the same representative was encouraged to attend the workshop sessions.
- Material that may be too commercially sensitive to discuss at a workshop level can be discussed directly with relevant NEHTA staff.
- Workshops will be jointly chaired by NEHTA and MSIA/AIIA.
- Sub-Workshops/Areas of interest may be created for particular topics.
- Secretariat support to be provided by NEHTA.
- Teleconference use was not advocated for the workshops.
- Organisation chart of NEHTA staff was promised
- Phone list of NEHTA staff was promised

Scope and Deliverables

John McMillan NEHTA, Andrew Berry NEHTA, Andrew Shrosbree NEHTA

NEHTA outlined that they are seeking widespread open, standards based capability with secure connectivity that uses national infrastructure such as Health Identifiers and Authentication Services. Goal is interoperability between all areas of health.

Secure Messaging profile should work generally in most relevant cases. Encrypting all content is the current NEHTA endorsed approach to ensure end-to-end security.

Issues or Concerns that were raised included:

- Legislation timelines for Health Identifiers to be operational was raised as a concern
- Synchronous (real time) messages need to be covered by specifications as they are used in current processing. A request to extend our use-cases to address general messaging was requested.
- Clarification for "documents", "payload" messages, acknowledgements and use cases required, ie the language used for describing these
- Role of contracted service providers such as intermediaries needs to be clarified by NEHTA. Service providers currently have access to the clinical content of the message, ie authorised by Practice. This will be discussed at the next workshop.
- Current specifications may not cover all of the scope of eHealth, eg Images.
- Encryption of payload content when the message is between a direct trusted to trusted link was questioned. A simpler approach was requested.
- Having Interfaces being put forward as a standard was a concern. Rather than referring to standards, suggestion to reference a profile or a handbook. Needs to be discussed further.
- Need to agree messages and exchange formats, eg should be as per current Australian standards.

Connectivity

Hoylen Sue NEHTA

Hoylen outlined how Secure Messaging fits into the context of the whole NEHTA work program. The material consists of:

- Solution Specifications: Clinical Document Delivery; Pathology, Medications, Referrals and Discharge Summary
- Foundation Specifications: Connectivity Architecture; Concepts and Patterns; Web Services Profile; XML Secured Payload; End Point Service
- Support Material: Implementation Guides; Sample Code; Testing Tools

Workshop focus is on secure messaging, not the actual payload content, eg pathology result, discharge summary.

NEHTA is focussed on how organisations externally interface through secure messaging to other organisations, not how the internal organisational processes function. Approach is to have as few options as possible to aid in interoperability.

The Endpoint Location Service (ELS) was explained and also how a 3rd party may host this service.

Issues or Concerns that were raised included:

- HeSA PKI certificates are incompatible with some elements of the Web Services Profile. Hoylen explained that Transport Layer Security (TLS) has been added as an option in the Web Services Profile.

Clinical Document Delivery

Andrew Berry NEHTA, Andrew Shrosbree NEHTA

NEHTA provided an overview of the Clinical Document Delivery approaches.

NEHTA outlined they will be hosting an Endpoint Location Service (ELS) by end of June 2009. 3rd Party Suppliers would also be encouraged to host an ELS. NEHTA will also supply the source code for the ELS.

As Health Identifiers (UHI) and National Authentication Services Health (NASH) are not yet available some options were discussed about interim solutions. Use of Provider number via LDAP to return Registered Account (RA) and then use a web service to retrieve end point and payload format was discussed.

Issues, Concerns or Suggestions that were raised included:

- With the tabled work around solution for use of Provider Numbers, feedback was that multiple Provider numbers exist, ie many may be returned from LDAP service. A mapping of Providers to Organisations would be required but this is contained within Medicare and may be subject to policy/privacy issues at Medicare. Provider number usage is protected, hence the need for UHI services. Medicare does not hold all the mapping information and other groups will need to provide information.
- Suggestion that when an upgrade is done to software or Medicare certificates, that entries are automatically added to the ELS.
- Suggestion that a Compliance check is done when software is installed.
- ELS will need to cater for multiple agents running at an organisation, ie different contracted agencies.
- Solution should cater for sending organisation needing to select which party to send documents to at the receiving end, ie multiple applications on the desktop. Also multiple types of certificates.

- Trust of information uploaded to ELS was seen as a critical issue. How are the entries trusted and what will be the verification process.
- There may be some reluctance by suppliers to share their information from their directory into an ELS.
- If there are multiple ELS's how do you find the correct one to use, which one do you trust? UHI will assist with this but interim solution required until UHI has legislative endorsement.
- Certificate management was also seen as a critical issue. Certificates are required quickly for onsite work to get the Practice going quickly. Critical to have quick availability, timely support and download of updates for ease of operation.
- ELS specifications and information needs to be made available by NEHTA.
- Views expressed that the specifications should be more than just a "gateway" model – needs to apply to GP desktops as well.

Standards Australia

Andrew Caswell Standards Australia

Outcome of Secure Messaging consultation is the submission to Standards Australia of the agreed specifications. Submission to Standards Australia was requested by MSIA during the discussions with Dept of Health and Ageing prior to PIP release. MSIA have specifically requested submission to Standards Australia to avoid lots of ongoing changes to the specifications which would affect suppliers and health professionals.

Andrew outlined the background of Standards Australia and relationship with ISO and also the approach for taking the specifications forward. Standards Australia look for International Standards to be considered and adopted where possible. Also the specifications need to be 'fit for purpose', a general consensus on their adoption is required and they should be 'good industry practice'.

Andrew encouraged Standards Australia having an ongoing participation in the Secure Messaging process.

Conformance Compliance and Certification

David Manfield NEHTA

David outlined that certification will be tied to the Secure Messaging specifications. What the test criteria will be, how it will be performed and who will do the certification will be discussed through consultation. The timelines for the process will also need to be agreed but these are dependent on the specifications.

Issues, Concerns or Suggestions that were raised included:

- Consideration for existing certification approaches and methods was requested, especially international approaches for example CCHIT (Certification Commission for Health Information Technology) and Canada Infoway.
- Consideration for independent non-NEHTA certification was requested.

Final

Vendors thanked NEHTA and MSIA for running a successful event in a positive and collaborative spirit.



Next Workshop

Next Workshop is proposed for Melbourne on 6 May 2009. Details of the event will be emailed separately and updated at www.nehta.gov.au/pip

Primary focus of this workshop will be to gain more direct input from suppliers and to work through:

- Clarification of PIP secure messaging scope and requirements in comparison with NEHTA solution specifications
- Business Use Case / Business Requirements for Secure Messaging

Agenda to be worked through with NEHTA and MSIA and distributed.

Appendix A Summary of Actions

Category	Item	Owner	Date Actioned
Admin	Terms of Reference for workshop is required	Tina/MSIA	
Admin	Organisation Chart for NEHTA to be distributed	Tina/Paul B	
Admin	Phone list for NEHTA staff to be distributed	Tina	9/4/09
Admin	AIIA members didn't get distributed an invitation? Requires followup	Tina	
Admin	Follow up with those suppliers who have signed Statement of Commitment but who are not participating in workshops is required.	Tina/MSIA	
Admin	Workshop summaries and presentations to be loaded onto NEHTA website, advised to attendees	Paul B	17/4/09
Admin	ELS specs to be put up on website and circulated to workshop attendees	John Mc	
Admin	Consideration for Travel Expenses to be reimbursed for up to 15 members (rather than current 10).	Tina/Paul B	
CCA	Investigation of existing conformance/compliance approaches required	David M	
Comms	Collaborative Portal is being developed by NEHTA for working with industry. Information to be distributed to workshop attendees. This will be demonstrated at next workshop	John Mc Next workshop	
PIP	Clarification on how PIP payment is administered. If supplier drops off Eligible Supplier list what are the implications for the practice, eg quarterly assessment? Clarification from DoHA required.	Paul B	
Present-ation	Each supplier is invited to send an overview of their secure messaging solution to pipwg@msia.com.au	All suppliers	
S.Msg	Clarification of PIP secure messaging scope and requirements in comparison with NEHTA solution specifications	John Mc Next Workshop	
S.Msg	Clarification over documents, messages, acknowledgements and use cases required, ie the language used for describing these	John Mc Next Workshop	
S.Msg	Use Case definitions and Business Requirements needs more discussion	John Mc Next workshop	
S.Msg	Complexity with double encryption at transport layer and payload needs to be considered. Simpler option requested between trusted parties.	John Mc	
S.Msg	Role of Contracted Service Provider to be explored more. Privacy requirements to be clarified. Includes encryption approach.	John Mc	
S.Msg	Real time (synchronous) responses and messaging needs to be catered for.	John Mc	
S.Msg	Jurisdictions need to also adopt usage of NEHTA specifications. Jurisdictions to be consulted.	John Mc	
Standard	Standards Australia to be involved in ongoing process	Tina	

Appendix B Attendance List

Organisation	Individual	Role
Argus Connect International Pty Ltd	Julia Davis	Business Analyst
Australian Healthcare Messaging Laboratory (AHML)	Jane Gilbert	Director
CSN Technology Pty Ltd	Brett Avery	Solution Architect
eClinic Pty Ltd	Gavan Lim-Joon	Chief Technical Officer
Global Health Pty Ltd	Katie Nelson	Hospital Systems
Health Connection Network Ltd (HCN)	Staffan Flodin	Software Development Director
HealthLink	Lars Becker	Manager Strategic Projects Product Manager Messaging
iSoft	Paul Doman	Operations Manager, Primary Care
KeyTrust Group	Paul Arch	Director
KeyTrust Group	Ross Bennett	Chief Engineer
Medical-Objects	Jared Davison	Senior Software Engineer
Medical Software Industry Association	Bridget Kirkham	Chief Executive Officer
Medical Software Industry Association	Vince McCauley	President
Microsoft	James Kavanagh	eHealth Architect
National eHealth Transition Authority	Andrew Berry	Solution Architect, Secure Messaging
National eHealth Transition Authority	Andrew Shrosbree	Integration Architect, Secure Messaging
National eHealth Transition Authority	Bill Bolton	Technical Advisor, UHI
National eHealth Transition Authority	David Manfield	Manager, CCA
National eHealth Transition Authority	David Nissen	Technical Manager, NASH
National eHealth Transition Authority	Hoyleen Sue	Technical Architect, Secure Messaging
National eHealth Transition Authority	John McMillan	Manager Secure Messaging
National eHealth Transition Authority	Paul Burnham	Manager Reference Platform
National eHealth Transition Authority	Tina Connell-Clark	Manager Industry Engagement
Orion Health Pty Ltd	John Allinson	Project Manager
Pro Medicus Limited	Steve Williams	Research and Development Manager
Smart Health Solutions	Larry Singer	Jon Hughes/IT Director will be attending from now on.
Standards Australia	Andrew Caswell	Project Manager
Stat Health Systems	Brian Carter	Development Consultant

*** End of Report ***