MSIA

THE MEDICAL SOFTWARE INDUSTRY ASSOCIATION (INC)
ABN 82 324 598 961

Dr Ian Holland,
Committee Secretary
Senate Community Affairs Committee
PO BOX 6100
Parliament House
CANBERRA ACT 2600

Dear Dr Holland,

Inquiry into:
Personally Controlled Electronic Health Records Bill 2011
Personally Controlled Electronic Health Records (Consequential Amendments) Bill 2011

The Medical Software Industry Association (MSIA) appreciates your invitation to provide a submission to the Senate Community Affairs Committee. The MSIA supports the ehealth initiative but has some concerns which need to be addressed.

The MSIA is a national not for profit body which is the recognised official "voice" for the healthcare software industry. With over 120 members and active volunteer engagement by our members as representatives on many of the working groups and committees relating the the PCEHR initiative and ehealth foundations over many years, we welcome the opportunity to provide a submission to the committee.

Healthcare software is used across all sectors to support the clinical process – this may vary from the measuring of a baby in-vitro, providing up to 20,000 different decision support alerts for prescribers, creating the wording on your pill bottle, planning a chemotherapy regime or an advance care directive. Our members support clinicians in all settings – telemedicine, rural and remote, hospital, clinics, GP and allied health including dentists, ophthalmology, etc.

This submission has been informed by extensive polling of our membership both online and using handheld technology on the 19th October 2011. Nothing has happened since that date to change the views of our members.

The MSIA has taken great care to write this submission in a non-technical way in order that the wider public may understand our concerns – and their implications for a "safe" PCEHR. We are happy to provide further technical input should the committee require it.

Yours sincerely

Bridget Kirkham
CEO MSIA
0427 844 645
www.msia.com.au

MSIA

Inquiry Into:

Personally Controlled Electronic Health Records Bill 2011

Personally Controlled Electronic Health Records (Consequential Amendments) Bill 2011

Submission of the Medical Software Industry Association

January 2012

CONTENTS

Executive Summary 4

1. Comments relating to the PCEHR Bill(s) 5

2. Healthcare Identifier safety issues 7

3. PCEHR and EHR Readiness 9

4. Other Issues 11

Recommendations 13

Appendix 1 Previous submission on the PCEHR Bill 15

Appendix 2 List of software program changes required be operational on 1st July, 2012 24

Appendix 3 Status of documents on software development portal (as referred to by page 15 of The Australian Department of Health and Ageing submission) 26

Appendix 4 MSIA White paper on clinical safety issues relating to Healthcare Identifier Service 28

Appendix 5 Peer reviewed paper on clinical safety issues relating to Wave 1 Sites 35

Appendix 6 ehealth foundations for PCEHR system 42

Executive summary

The MSIA welcomes the opportunities that eHealth and the PCEHR provides for the medical software industry and Australia.

However, as with any large projects there have been a large number of challenges for all involved, but primarily a range of issues pertaining to accountability, transparency, and timely delivery.

Today, 24th January, an article in *The Australian* "E-health key trial halted by specifications glitch" caught many in the industry by surprise[1]. While a pause may be necessary, and a review of issues probably essential, no one in industry has been informed of what the issues are, when we may know the size of the problem or which of the many complex programs are incompatible with the build of the National Infrastructure. A failure to adequately inform stakeholders, be transparent, or to provide any timeline is consistent with NeHTA behaviour during the past few years. It does not make for trusting relationships, or inspire confidence in a way that allows industry to make decisions to invest in, and engage with processes in which NeHTA is involved.

This submission is to both provide information that accurately represents eHealth and PCEHR readiness and provides a range of recommendations for the Inquiry's consideration.

[1] http://www.theaustralian.com.au/australian-it/e-health-key-trial-halted-by-specifications-glitch/story-e6frgakx-1226251676081

1. Comments relating to the PCEHR Bill(s)

Comments on the Personally Controlled Electronic Health Records Bill 2011 as presented and read a first time in the House of Representatives November 2011

The MSIA has previously made a submission on the Exposure Draft of the Personally Controlled Electronic Health Records Bill (‘the Draft Bill”). This submission remains pertinent and a copy is annexed at Appendix 1 and can be accessed from http://www.msia.com.au/?pid=17

In essence, the MSIA is committed to Australia having a standards based and privacy compliant personally controlled electronic health record system. The MSIA made 18 recommendations to further this goal in respect of the proposed governing legislation, and is pleased to note that several of the recommendations have in whole or part been adopted including the compulsory breach notification provisions. The current Bill has clearly acknowledged some of the shortcomings of the Draft Bill, and now provides important additional functions of the System Operator in the new Part 2, such as the education of consumers, participants and public about the PCEHR system.

There is more information about the proposed Rules and what they ought to cover, but it is nevertheless concerning that there are severe penalties in place for breaches of the Act from 1 July 2012 although the Rules are not determined and there will be very short periods of time for the parties to understand and establish procedures for compliance with complex new obligations. Underlying this is the problematic policy decision not to provide incentives or recompense to system participants who are nevertheless expected to contribute extensively to the PCEHR and while doing so, assume significant risk in the event of breaches.

A detailed description of the function of all participants in the PCEHR system would assist in the clarity of the legislation. Currently the System operator is described in some detail but the specific characteristics and functions of the other participants, such as the portal operators, repository operators and contracted service providers remain unclear and this will make the education of the public difficult. Without education, consumers and organisations are unlikely to take up the challenge of participating in the PCEHR system.

Areas of concern remain in respect of the independent advisory committee (Part 2 Division 3). The welcome addition of experience or knowledge in Aboriginal and remote and rural healthcare to the criteria is pleasing, but the addition of experience and knowledge in research and secondary uses of data would be sensible given the value and sensitivity of this area in data governance. Similarly, there would be great value in having input from the aged care sector in the independent advisory committee, given that this sector could be one of the most to benefit from shared medical information, along with chronically ill and disabled health care communities.

There should be some advisory role for the informatics community, software industry and Standards Australia to provide and review technical advice to the System operator.

The MSIA believes the System Operator (as described) is impossibly conflicted with roles as System Operator, System funder, and NEHTA Board Member.

The fact that section 45 of the Bill places the onus on the Healthcare provider not to upload data which could infringe copyright or moral rights still remains a concern for reasons specified in the MSIA's original submission. Healthcare workers are not best qualified to judge these matters and the likely default instruction given to them by their organisations will be to not share data which could otherwise be usefully shared and used.

The provisions in respect of access controls remain complex. To prompt involvement by healthcare providers, it is hoped that these can be simplified and that education and training and payment for new services provided.

Fundamentally, the MSIA is of the view that whilst some of the concerns that it and many other organisation and associations raised in respect of the Draft Bill have been met, there remain a number of areas requiring attention. The difficulty of drafting legislation around a system and standards that have not yet been built or definitively described are evident in all the areas raised in the previous MSIA response to the Legislative Issues and Draft Bill. In the case of the Legislative Issues paper, one of the most critical problems was that submissions were requested before the Final Concept of Operations of the PCEHR had been released. The position is not entirely dissimilar in respect of the current Bill. There is still a great of deal to be understood about the PCEHR system and how the participants will interoperate. Until there is transparency about what the National Infrastructure partner is building, it is almost impossible for the legislation to accurately cover the issues of privacy, safety and data governance generally. There is a provision for a review of the legislation in 2 years (section 108), which now includes the requirement for public consultation and submission. This is a sensible addition, but it is hoped that the time can be tightened so that the review can take effect before then if required given that the PCEHR system I is still being built.

2. The Healthcare Identifier Service – safety issues

The healthcare identifier service has now been in operation for over 18 months. Clinically meaningful usage has been extremely low. A few programs are in place that access the unique patient identifiers (IHIs) but most IHI access has been through a NeHTA sponsored Wave 1 initiative to inject IHIs into GP desktop software. This has been done largely without the consent or cooperation of the Software vendors. This is an inherently unsafe process as documented in the peer reviewed paper by McCauley and Williams (Appendix 5). MSIA made NeHTA and DoHA aware of its concerns with this process at the Conformance Compliance and Accreditation Governance Group (CCAGG) over ten months ago. However, the roll-out has continued unchecked and NeHTA has been unable to provide any information about subsequent evaluation of potential errors that may have been introduced into live patient records.

Only in recent months, as part of the development of Conformance test cases for Provider identifiers (HPI-Is) and Organisational identifiers (HPI-Os), has it been revealed that the current design of the Health Identifier service does not allow discovery or validation of these identifiers. Verification of provider identifiers is only possible for providers and organizations that have opted into the Medicare Provider directory and less than 1% of providers have opted in. Whilst a change request is said to be in process to fix this problem, Medicare and NeHTA have not been able to provide either the details of the change or a timeframe in which it might be deployed.

As at the time of writing, no one is able to access HPI-Is or HPI-Os via the HI service because the sector is still determining whether conformance test cases can be developed in a manner that satisfies patient safety concerns because of the design flaws.

In recent weeks a variant design flaw, (similar to a 2010 change request, that was not resolved), affecting patient IHIs has come to light. A patient who has an existing IHI can be assigned a new IHI under a number of circumstances. In particular if the patient’s date of birth is corrected or the patient’s gender changes. In addition a new IHI can be assigned if Medicare detects a duplicate or replicate record in their database. However, once a new IHI is assigned, due to privacy constraints, Medicare is unable to inform practitioners accessing the service of the changed demographics associated with the new IHI. If software attempts to validate the old IHI, the new IHI is returned with a status of “resolved”. Attempting to validate the new IHI, fails because the demographics are out of date. Hence neither the new IHI nor the old IHI can continue to be used because they cannot be successfully verified and there is no mechanism for Medicare to inform practices of the new demographics. In a PCEHR environment, this would effectively cut off access to the patient’s EHR. It would also invalidate all documents containing either the new or old IHI and make it impossible to create documents where an IHI is mandatory.

It is unclear whether these issues are addressed by the proposed legislative changes to the Health Identifiers Act. It is at least certain that these issues will not be able to be resolved before July 1, 2012 when the PCEHR is due to go live.

MSIA has repeatedly asked for the information contained in the comprehensive safety report that NeHTA has stated was performed prior to the Health Identifier service going live. This has not been made available. The results of a recent FOI request to DoHA by *The Australian*, demonstrated that DoHA does not have such a report. The recently discovered design flaws suggest that the safety report, if completed, was not sufficiently comprehensive.

It remains unclear why NeHTA would not provide software vendors designing systems to access the HI service with a safety report so as to permit the safest implementations.

Further it should be noted that the Medical Software Industry Association was repeatedly instructed by Peter Fleming the CEO of NEHTA and other senior managers that we could not even “speak” to the NEHTA Clinical Safety Unit and the Clinical Safety Unit was instructed never to speak to any person from the Medical Software Industry Association.

“Clinical safety” usually relates to the information and procedures that are controlled by clinical staff in a medical setting. However there is another large area of “patient safety” that relates to the “implementation” and workflows relating to health software use. These also need to be fully reviewed. The Inquiry should ask if they could be provided with the safety reports, audits etc that relate to the 12 PCEHR lead sites.

When the Health Identifiers service was introduced on 1 July 2010, a 2 year amnesty period was provided so that accidental breech of the legislation by providers did not necessarily incur severe penalties, including jail terms. This amnesty expires on the day that it is proposed to turn on the PCEHR service. The prospect of jail terms for accidental access to a patient identifier will certainly act as a significant inhibitor to Providers using the PCEHR.

These major unresolved issues with the Health Identifier service, with potential serious impact on patient safety and Provider welfare, along with the immature state of the PCEHR specifications, was a major input to the decision made by MSIA to call for a six month delay in PCEHR implementation in a letter to DoHA in November 2011. The department’s response was that such a delay was unwarranted. The MSIA then proposed a “lite” version of the PCEHR which would meet the political imperative but would allow some parts of the eHealth program to be delayed to ensure the work was done safely.

It should be noted that unique identifiers are not a new or complex part of electronic systems. Each medical software vendor in Australia runs its own “unique” identifier system and there are literally hundreds in our daily life – licences, tax numbers, passports, bank accounts, memberships etc. This is not the difficult bit of the PCEHR but 18 months after the Healthcare Identifier Service went “live” it is still not functioning safely. It is still unclear what the benefits of these national identifiers are above and beyond those used today if they cannot be relied upon for the reasons stated above.

Patients who sign up for the PCEHR must have a “fully informed” consent – are those already signed up through the “sites” aware of these issues?

It is not clear whether the MOU announced on page 11 of the Australian Department of Health and Ageing submission to this Inquiry which provides $34 million to DHS-Medicare to upgrade the HI Service is intended to resolve the issues outlined above.

In spite of best efforts by well-trained staff, incorrect identification of person can occur in any software system, including government and Medicare’s systems. With increased interoperability, it increases the chance of wrong data allocated in the PCEHR to the wrong patient, or the wrong patient having 2 or more PCEHR records – it thus requires the very best of identification systems.

3. PCEHR and EHR Readiness

This submission was a little late – it had been expected that the Questions on Notice for the Australian Department of Health and Ageing (DoHA) from last October would have been posted on the Senate Estimates page – they were due on the 9th of December. Some thirty of those Questions on Notice overlapped with the scope of this Inquiry.

In lieu of those answers the MSIA has used the department’s submission to the Senate Community Affairs Committee as its baseline to show examples that relate to readiness.

Page 4 of the DoHA document lists a number of accomplishments that NeHTA will have achieved by the 30th June 2012 for the ehealth foundations.

a) ***HI service “established”*** – not sure what that means given the $34 million MOU upgrade announced in the same paper
b) ***“digital certificates...introduced***”
c) ***“standard approach to terminology developed***”
d) ***“consistent approach across jurisdictions...developed”***
e) ***E-prescriptions ...implemented”***
f) ***Australian standards...in place”***

This list does not read as though the medical software developers are going to get much time to implement the whole set of e-health foundations for the PCEHR. At Appendix 2 of this submission there is a list of work which is due to be “live” – that is – built, tested and functioning on the 1st of July 2012 – you can seen that the vendors have a large (almost impossible) work program.

On page 15 of the DOHA submission at 4.8.2 PCEHR Standards and Specifications there is much trumpeting about a vendor portal launched in November 2011. What they have omitted is that the site is currently under urgent review for a range of useability issues (which includes the inability of many vendors to sign up to the draconian Terms and Conditions). The DOHA submission notes ***“The bulk of the specifications necessary for PCEHR participation will be available to industry by the end of December 2011.”***

Unfortunately there are 5,346 pages on the site- all loaded since 17th November, 2011 – 20% of the “specifications” are out of date (ie the wrong version has been loaded on to the site, many of the documents are not final (despite what it may say on the front!) Those documents have either future review dates (March 2012 for example) before 1 July 2012, or are missing part of the bundle of documents, or have a list of known “issues” which are unresolved, or are still going through a tiger team process etc. This does not give confidence to the software vendors – yet the Australian Department of Health and Ageing and NeHTA believe a document with the word Final” on the front is “Final” and fit for use.

At Appendix 3 of this submission there is a table of the documents as referred to by the DOHA submission as the **“bulk of specifications”.** You can see them for yourself at https://vendors.nehta.gov.au/public/index.cfm?returnTo=%2Findex.cfm
You don’t need to be a vendor to register or log in but you will see the gaps in the area called PCEHR Core System – not to mention eHealth Foundations etc. You will also note that there is no terminology tab as referred to above for a **“standard approach to terminology’** at that portal. The latest one of the terminology documents – a very technical 240 pages on NCTIS editorial rules can be found at “Whats New” on the NEHTA website (http://www.nehta.gov.au/publications/whats-new) .

Even a casual observer would wonder at the lack of indexing or marking of changes in such a complex document. It certainly does not make it easy for the medical software developers.

The MSIA has chosen this one example of overstatement before substance or delivery – there are numerous other examples of poor planning, failure to complete to deadlines and a range of other unacceptable behaviour that contravene normal Australian business practices – these have led to a reluctance to commit to development work in such a changing and uncertain environment. The risks are great, and the potential for errors that cost lives is high – "first do no harm" is a good motto.

4 Other issues

The advice that MSIA has received from Ken Fleming QC is that NeHTA appears *"to be off all accountability radars. It is not listed as a corporation under the Commonwealth Authorities and Companies Act 1997, or as an agency under the Financial Management and Accountability Act 1997. If there is accountability then it must be outside of the Commonwealth purview. "*

In the tendering and other procurement processes NEHTA does appear to have interfered with the market place on more than one occasion. Unfortunately for the medical software industry the normal processes of review and accountability are not available to the Association or its individual members without legal recourse.

The ACCC , which would look at such issues on behalf of an industry group is unwilling to review issues relating to a "body" which is fully funded by state and federal governments. The Productivity Commissioner is also unable to assist as NeHTA has been constituted as a private not-for-profit entity and therefore not subject to the considerable "level playing field" provisions available to other sectors where considerable amounts of taxpayer's money is being spent in a market place.

This means NEHTA is not required to meet FOI requests or any of the other accountabilities of a government agency which has been spending at least "**a mill a day**" (See webinar (11 January 2012) on NEHTA's website at http://www.nehta.gov.au/ehealth-implementation/pcehr-standards)

Further, one has to question the position and ability of the DoHA Secretary to meet all the obligations of one who is both funder, (and therefore has some accountability) and, as Director of NEHTA with all the attendant corporate responsibilities. It seems therefore, unusual to pass further legislation the makes the DoHA Secretary the "Service Operator" and must surely further muddy the oversight of the eHealth agenda.

The accountability issues have been exacerbated by the failure of DoHA to answer Questions on Notice that were due on the 9th of December last year and which are pertinent to the scope of this Inquiry. Submissions to the Inquiry have had to be prepared without the latest government answers on a range of issues. Given the time frame of the PCEHR rollout this seems unacceptable.

The MSIA has taken some comfort that The Auditor-General Amendment Bill was passed by the Senate late November 2011. More significant amendments include:

- enabling the Auditor-General, at the request of the JCPAA to conduct performance audits in non-Commonwealth entities that receive funding for a Commonwealth purpose
- giving the ANAO the authority to assess the performance of contractors that are engaged by the Commonwealth;
- enabling the Auditor- General to undertake audits of key performance indicators (KPIs);
- providing explicit authority to the ANAO to conduct assurance engagements, such as the Defence Major Projects Review, and utilising the same information-gathering powers that exist for the conduct of performance audits where such engagements have been identified as priorities by the Parliament; and

- clarifying the application of privileges, such as legal professional privilege, to the Auditor General’s access powers.

These amendments represent the most significant changes to the Auditor General’s mandate since the addition of efficiency audits back in 1979.

However the MSIA doesn’t yet know the date new legislation will come into effect. However, it does appear that there may be the possibility of some transparency, audit and accountability in the future.

Recommendations

The PCEHR BILL:

1. Add a more detailed description of the roles of all participants to aid understanding and uptake.
2. Commit to a date to publish “Rules” to allow adequate time for those who may be of risk of breach to be fully aware and compliant.
3. Increase Advisory group to include representation from research, secondary data and aged care experts. Ensure Advisory group reflects the 60% of health care delivery that is not provided by government or government agencies.
4. Make a provision that includes the taking of technical advice from the informatics community, Standards Australia and the software industry associations to ensure future changes and developments are appropriate, safe and timely.
5. Review the conflicts for the proposed System Operator in the various roles held :- as partial funder, system operator and as NEHTA Board Member
6. Review the ‘government furnished data’ liability issues, for example incorrect IHIs, incorrect PBS and MBS information, and incorrect AMT and SNOMED updates. Consider how the potential of such issues to act as disincentives, at worst, or to skew market and patient take up at best.

Healthcare Identifier and Patient Safety Issues

1. Action as an immediate priority, change requests to the HI Service that are deemed to have a potential clinical safety impact.
2. Action as an immediate priority, a government funded field study of AMT Mapping with at least 2 of the market-leading medication terminology vendors exchanging medication data.
3. All patient and clinical safety assessments and reports that have been funded either through NEHTA or other government agencies should be made publicly available immediately to provide confidence in the system. It seems unusual that the Australian Department of Health and Ageing has not required such reports of its manager of the PCEHR (NeHTA) to ensure the safety of the Australian public.
4. Review urgently all the issues in the MSIA White paper on the Healthcare Identifier Service and ensure changes are made to ensure the service can be used safely.
5. Review urgently the issues in the McCauley& Williams paper (Appendix 5). Consider a “consenting adults” model where software that acts in a parasitic way is tested with its “host” for all Conformance Compliance and Accreditation processes. Where such inherently unsafe software has been used there should be a post deployment review to ensure that patient safety and identification has not been compromised.

The PCEHR Program:

1. Reduce the scope of the 1 July 2012 release of the program (Release 1) by deferring elements that are not sufficiently mature or not sufficiently reviewed to ensure patient safety (for example, Australian Medicines Terminology, Health Terminology (SNOMED), Consolidated View, etc.).
2. Clearly define the scope of the national infrastructure partner relative to other software systems, including local PCEHRs and conformant repositories, to facilitate planning and investment by the software industry and healthcare providers.

3. Support the PCEHR program with sustainable, recurrent funding that supports the long-term viability of eHealth across the health sector (consumers, healthcare providers, healthcare provider organisations and technology providers). The National Change and Adoption and Benefits Evaluation Partners have provisionally identified national savings of several billion dollars a year from full operation of the PCEHR program; a modest percentage of these savings must be re-invested in the sector if the PCEHR program is to be successful.

Other Issues:

1. Make NEHTA accountable for its services and activities - NEHTA should be subject to federal FOI legislation (it is 100% funded by taxpayers and is for all intents and purposes a public entity).

2. The Auditor General (through ANAO) should conduct financial, information technology and efficiency audit of NEHTA as soon as possible

Appendix 1

Medical Software Industry Association

Submission on

Exposure Draft Personally Controlled Electronic Health Records Bill ('Draft Bill')

"There are two visions for the future here. One defends individual privacy. The other gives up. One asserts the capacity of law and policy-makers to uphold a fundamental human right in the face of technology. The other says it is impossible – and possibly unnecessary. Resolving these debates presents one of the greatest questions before humanity in the coming century…What is at stake is nothing less than the future of the human condition."

The Hon Michael Kirby AC CMG 13.09.99 "Privacy protection- A New Beginning" 21st International Conference on Privacy and Personal Data protection

INTRODUCTION

The Medical Software Industry Association (MSIA)

The MSIA represents medical software industry members and is committed to improving the safety and efficacy of Australian healthcare. The benefits of improvements to the delivery and accessibility of health care services through eHealth initiatives have been quantified [1] and the Industry is keen to see Australians endorse eHealth initiatives.

Need for reform and balance of interests

The Federal Government has recognised that widespread confidence in the benefits, integrity and security of the Person Controlled Electronic Health record is essential to uptake and success. This requires a finely calibrated approach to balancing the interests of parties involved. Governments are aiming for improved public health outcomes; regulators and professional associations are seeking quality agendas; healthcare Institutions are seeking quality assurance and marketing advantages; practitioners are seeking decision support and more information, whilst the patient is hoping for quality care, confidentiality, anonymity and privacy.[2] The desired outcomes for these ostensibly disparate agendas can be achieved by the overarching goal of improved medical service and privacy, provided that the appropriate checks and balances are in place to attract the confidence of the consumers and introduction by the health carers. It is on this basis that the MSIA makes its submission on the Draft Personally Controlled Electronic Health Records Bill 2011.

It is recognised that both the healthcare and software industry will need to invest in infrastructure and change management and that incentives are one of the five key areas to drive change and adoption.[3] The critical need for a clear business case is not however relevant to this submission. The MSIA is cognisant of the fact that the Draft Bill is required to provide additional privacy protection for Australians, given that the *Privacy Act 1988 (Cth)* was formulated long before "…the Internet and web crawlers, spiders, robots and trawlers which have introduced completely new methods for an intense dataveillance of the individual"[4] The additional protections do however include significant penalties for users. This includes penalties for clinicians whose uptake of the PCEHR is critical to its success. These parties would therefore need to assume extra risk with no incentive being offered to them for the additional effort and potential liability. It is hoped that the Government will follow this recommendation by the Deloitte National E-Health Strategy and National Health and Hospital Reform Commission so that there are the requisite drivers, including financial incentives for use of the PCEHR, are in place to make the PCeHR useful and successful upon its introduction in July 2012.

[1] See for example *Selected Facts and Statistics on Australia's Healthcare Sector – Engaging and empowering citizens and patients is the key to better health outcomes* p. 26 Business Council of Australia, released February 2011.
Accessed 21 .10.11. See also BCA: *Using Microeconomic Reform to Deliver Patient Centred Health Care,* Prepared with assistance Port Jackson Partners Ltd.

[2] Nicholas P Terry, *Electronic Health Records: International, Structural and Legal Perspectives* (2004)12 JLM 26 at 29

[3] Recommendation 123 Australian Government National Health and Hospitals Reform Commission, *A Healthier Future for All Australians Final Report June 2009 at p. 282.*
"With respect to the broader e-health agenda in Australia, we concur with, and endorse the directions of the National E-Health Strategy Summary (December 2008), and would add that: There is a critical need to strengthen the leadership, governance and level of resources committed by Governments to giving effect to the planned National E-Health Action Plan. This Action Plan must include provision of support to public health organisations and incentives to private providers to augment uptake and successful implementation of compliant e-health systems. It should not require Government involvement with designing, buying or operating IT systems…" Endorsing the Deloitte National E-Health Strategy Summary December 2008 at p. 17.

[4] J. Hilvert, in *Information Age*, May 1996, 18 cited in Greenleaf, Privacy in Cyberspace: An ambiguous Relationship" (1996) 3 *PLPR* 5 at 88

Finally, the MSIA firmly supports a standards-based approach to the PCeHR. This will promote the interoperability of software systems to improve best practice and the efficiency of infrastructure. There needs to be clearly articulated standards so that the market can build to these specifications confident in their investment. This will also enable the health industry to make informed decisions about appropriate solutions. It has been stated by the Deloitte E-Health Strategy that Governments should not be involved with designing, buying or operating IT systems[5] and a Standards based approach is critical to achieving this goal. The Draft Bill is not the place for the Standards to be specified but the MSIA is of the view that a robust framework must be specifically established pursuant to the Draft Bill to rigorously promote and enforce a Standards based approach for the benefit of all Australians.

[5] See footnote 3 *Supra*

RESPONSE:

PART 1

Section 3 Object of the Act

The object is stated as enabling the establishment of a voluntary system to improve access to consumer's health care data so it is not so fragmented, is of better quality and reduces adverse events.

Recommendation: – *the fact that these objectives are intended to be carried out in a privacy compliant manner to protect the privacy of consumers should be stated. The fact that it is an opt in system and noted as voluntary is not sufficient.*

Section 5 Definitions

1. "System Operator "is defined as being the party noted in Section 10.

Section 10 refers to the Secretary of the Department and also refers to the Minister in respect of passing regulations. Whilst the Companion Guide refers to the Department of Health, there is no definition of which Department or Minister is referred to in the Draft Bill.

Recommendation: – *the definitions be extended to define the Minister as the Health Minister and the Secretary as the Secretary of the Department of Health.*

2. "Participant in the PCEHR system" includes a registered contracted service provider, *so far as the contracted service provider provides services to a healthcare provider*." This definition envisages the existence of a contracted service provider as defined under the *Healthcare identifiers Act 2010* (Cth) as existing without necessarily providing such services. It is unclear what is intended by this proviso.

It would be positive if the intention was to include all contracted service providers in respect of the regulation of data governance and privacy, without necessarily making all contracted service providers *involve* the System Operator in their system. The definition of contracted service providers in the Draft Bill refers to entities which provide services relating to the PCEHR system, which is sensible and does not require them to involve the System Operator.

A good reason why the definition of a contracted service provider should be consistently used is that many useful eHealth services operate and should continue to operate that relate to or support the PCEHR without necessarily *involving* the System Operator or directly connecting to the PCEHR system.

Recommendation: – *the definition of contracted service provider should not be extended beyond the definition in the Healthcare Identifiers Act 2010 (cth) .*

Recommendation: – *the definition of PCEHR system should not include the necessity to involve the System Operator.*

3. "Personally controlled electronic health record of a consumer" is defined as a record created and maintained by the System Operator. Since the Governments adoption of the National E=Health Strategy (see Minister Roxon and through the Health reform process it has been made clear that the Government was going to provide the infrastructure for a number of conformant repositories to co-exist. This intention was included in the Concept of Operations. This definition excludes consumer records created outside the proposed national repository. It is also inconsistent with the definition of "shared health summary" which is defined as being created by the consumer's healthcare provider and which must be part of the consumer's record -i.e. the System Operator will not have created it. The current definition means that the later definition of "*use"* of health information in a consumer's PCEHR *not* created by the System Operator is not protected by the Draft Bill.

Recommendation: - *the wording of this definition be extended to include consumer records created both by the System Operator and through conformant repositories, as well as clarifying what is meant by the term "created". This will provide greater clarity and protection for the PCEHR which are not created or collated by the System Operator as well as those which are.*

Section 6 Definition of authorised representative of a consumer

A Consumer aged at least 18 who is not capable of making decisions for herself or himself must have a nominated representative appointed by Court or a law of the State, territory or Commonwealth as appropriate.

Some of the consumers who will gain most from this system include the elderly and disabled. There are apparently many instances where the two pre-requisites will not be met and accordingly the consumer, who is currently being cared for by a party other than envisaged by this Draft Bill, will not be able to have the benefit of more co-ordinated and efficient care.

Recommendation:- *the definition should be extended to allow parties who are currently caring for such people to apply to be nominated representatives to enable equity of access to some of the most worthy recipients of improved care in Australia.*

Section 7 Act to Bind the Crown

The Act binds the Crown but does not make it liable for prosecution or a pecuniary penalty. Recent issues surrounding privacy breaches in Medicare and the fact that the Secretary of the Department of Health would be responsible for this National system mean that this provision could be a disincentive. Parties need to trust that the operators of systems which hold their most personal data are need to trust that such a party would be held to account in the event of breaches. There is no automatic Crown immunity in Australia, and there is a rebuttable presumption that the Crown is not bound by a statute: Bropho v State of Western Australia.

Recommendation: – *Consideration be given to making the Crown liable for prosecution*.

Section 12 System Operator to have regard to advisory bodies' advice etc.

This section refers to the need for the System Operator to take advice from 2 undefined entities which are noted in Division 2 and Division 3. There is no reference to their composition or cross reference to the sections which define them in the definition section. These 2 bodies will have a vital role in the establishment of a robust governance system for the PCEHR and should be defined clearly.

Recommendation:– *define the Advisory Bodies in the Definitions consistent with the definition of System Operator which is noted as having the meaning in Section 10.*

Section 22 Appointment of Members (Independent Advisory Council)

This independent advisory body is a crucial part of the PCEHR. It will provide advice to the System operator on clinical, security and privacy issues relating to the PCEHR. All matters of import for Australians to have confidence in the system. Currently the knowledge base does not appear to have specific representation from the areas of Research, Aged Care and Disabilities which will be areas raising some of the most contentious and complex issues as well as being sectors where the cohorts will really benefit from PCEHR. These sectors require representation.

Recommendation: *– include experts in the areas of Research and secondary use of data, aged care and disabilities on the Independent Advisory Boards.*

Section 39 Condition of Registration

Sub section (4) provides that organisations must not upload records which could infringe copyright. This could be a hard call for a registered nurse or exhausted health professional not trained in intellectual property. The only safe course would be to err on the side of caution and not share the information which could prove useful to the care team and improve the health care of the consumer.

Recommendation: *– clarification be provided here for example by the creator of the record noting their copyright and or intention to allow or disallow it to be shared in PCEHR.*

Section 40 Registered Consumers Access Controls

This section provides that healthcare providers must not discriminate against consumers on account of their PCEHR access settings. The practical operation of complex access settings could take time to understand and comply with. While discrimination is not appropriate in respect of the provision of healthcare, it may be too onerous on professionals to insist they also attend to specific access controls upon the request of the Consumer with no recompense for their time in so doing.

Recommendation: – *provide in this section that there is no obligation for the healthcare provider to participate in the access or operation of a PCEHR if it determines it will take time and effort without recompense.*

Section 42 When a Person is eligible for Registration as a repository operator, a portal operator or a contracted service provider

This provision states that a person must comply with the PCEHR Rules. The PCEHR Rules are defines as having the meaning attributed to them in S.97. These Rules of operation are critical for all parties to be aware of from the outset. At present there are only statements about what rules may be made by the Minister about the operation of the PCEHR. Uncertainty in respect of storage, administration participant requirements are all a critical part of the governance spoken of by the Minister of Health on 30 November 2010

"… Consistent with the recommendation of the National e-Health Strategy, we are also working with our state and territory colleagues to ensure robust long-term e-health governance is in place ahead of July 2012.

And yes, that governance will include consumers and ensure strong clinical and privacy safeguards are in place.

We understand that privacy is a key concern, and we are designing this project to take heed of privacy from the ground up.

That's why this will be a truly personally controlled record.

That's why we're establishing new consent, settings for sensitive information and auditing that doesn't currently exist for any of our records.

It is how our system will strike the right balance between security and access.

I can confirm that the Government is not going to build a massive data repository. We don't believe it would deliver any additional benefits to clinicians or patients – and it creates unnecessary risks."[6]

[6] Minister Roxon Opening speech to E-Health Conference, *Revolutionising Australia's Health Care*, Melbourne Tuesday 30 November 2010 at p.6

Recommendation: – *a Governance scheme as envisaged by the Minister of Health almost 12 months ago and re-iterated in the PCEHR Concept of Operations 2011 be detailed and enacted as a part of this legislation from its inception.*

Section 44 Condition about provision of information to System Operator

This section provides that registered repository, portal or contracted service providers must provide information included in the PCEHR of the consumer if requested to do so by the System Operator. There are currently no rules surrounding this and so it is possible to envisage situations where consumers would not have provided the information if they had been aware this was a possibility. This would not therefore constitute truly informed consent and could pose a serious threat to privacy.

The rationale for the blanket request is not stated. Privacy needs to be embedded into the design of a system and cannot have legislation requiring disclosure to a Government body without explanation pursuant to as yet undeveloped or disclosed rules.

Recommendation: – *this provision be deleted or substantially extended to list the permissible reasons for compulsory disclosure so as to ensure that consumers provide fully informed consent to disclosure of their data.*

Section 50 Entries to be made in the Register

The System Operator can decide to have such administrative information as is necessary for the operation of the PCEHR noted on the Register. This is unduly open and could impact on the privacy of the consumer or entity.

Recommendation: – *transparency of the type of information to be recorded requires specification from the outset. As it is for administrative purposes it should be a straight forward task.*

Section 54 (b) (ii) refers to the setting of default access controls by the System Operator.

It would be useful to have these set in the legislation to guarantee default settings are privacy compliant.

Recommendation: – *set out the detail of default settings as many of the target Australians may be incapable of determining their own settings and it should be public and transparent to ensure the dignity of the parties.*

Section 56 Collection use and Disclosure for Management of PCEHR system

This provision authorises the collection and use of information from the PCEHR system for the management or operation of the PCEHR system "if *the consumer would reasonably expect it…"* Realistically a lot of consumers do not even know what the PCEHR system is and as it is a new system nobody could be realistically expected to know how it would operate, particularly a consumer. This clause like clause 44 lacks sufficient detail to engender confidence in the consumer that their privacy and consent to disclosure are being respected. Individuals should have a right to full disclosure of the collections of data to which others will have access and could affect the profile of the individual concerned.

Recommendation: – *delete the provision or provide comprehensive details about what the System Operator intends to collect or disclose.*

Section 67 Certain Participants in the PCEHR system must notify data breaches etc.

Notification of data breaches to parties whose data has been disclosed without their consent are a critical privacy protection allowing individuals to take all precautions and minimise damage, embarrassment and other potential loss. This provision does not make it compulsory for data breaches to be reported to all affected consumers.

Recommendation: – *the section would be enhanced by making the data breach notification compulsory. This is a part of the Privacy by Design Framework which is aimed at providing transparency from the outset to engender public confidence as well as respect for all users*.[7]

[7] See Dr. Cavoukian, Privacy by Design at www.privacybydesign.ca

Section 94 Annual reports by the Information Commissioner and S 95 Annual Reports by System Operator

These reports will provide valuable insight into how the system works and the level of breaches. It would be useful to have it while it was current and given the requirement for transparency of the system it would be appropriate to resource these entities to provide the data in a more timely fashion.

Recommendation: – *provide the reports quarterly*

Section 97 PCEHR Rules, regulations and other instruments

Note detailed comments and recommendation about the PCEHR Rules in respect of s 42 above**.**

Appendix 2

List of software program changes required be operational on 1st July 2012
While not all of these changes affect all vendors, some vendors will be required to make all these changes if there is no change to the roll out schedule. Safe change requires each change to be fully tested before the next change is incorporated into the software. At time of writing 21 weeks to go!

	Initiative	**Description**	**Commencement (go “live” date)**	**Complexity**	**Specs Finalised**
1	Under co-payment data collection	5CPA	1 April 2012	Moderate	Under review
2	Continued dispensing in defined circumstances	5CPA	1 July 2012	Moderate	NO
3	PBS claiming from Med chart (Aged Care)	5CPA	1 July 2012	Major	Under Review
4	MedsCheck	5CPA	1 July 2012	Moderate	NO
5	Staged Supply	5CPA	1 July 2012	Moderate	NO
6	Electronic recording and Reporting of controlled drugs	5CPA	1 July 2012	Major	NO
7	Switching	5CPA	1 July 2012	Moderate	NO
8	Monthly updates PBS continue	ongoing	-	Major	
9	Intro new PharmBiz system for epublishing & distribution	DoHA enhancement	Ongoing from March 1 2012	Major++	NO
10	ETP	eHealth	1 July 2012	Major	NO
11	Healthcare Identifiers	eHealth	1 July 2012	Major	NO
12	NASH	eHealth	1 July 2012	Major	NO
13	Secure messaging	eHealth	1 July 2012	Major	NO
14	AMT -mapping	eHealth	1 July 2012	Major++	NO
15	AMT – in signif no. vendor products	eHealth	1 July 2012	Major++	NO
17	AMT in Prescription Exchange Service	eHealth	I July 2012	Major++	NO
18	MBS Updates	ongoing	-	-	-
19	PCEHR Wave 1/Leadsites –rollout by others	PCEHR	1 July 2012 ?some earlier?	Major+	NO
20	PCEHR Wave 2/Lead sites –rollout by others	PCEHR	1 July 2012 ? some earlier?	Major+	NO
21	Access National Infrastructure	PCEHR	1 July 2012	Major+	NO

KEY for Appendix 2
5CPA – 5th Community Pharmacy Agreement
Ongoing – monthly (or more often) changes to the PBS and MBS
Under review – MSIA working with DOHA on vendor documents
ETP – Electronic Transfer Prescriptions
eHealth – eHealth refers to the foundation blocks needed for the PCEHR
PCEHR – changes required to allow the Personally Controlled portion of the PCEHR – at the time of writing the specifications used by the National Infrastructure Partner are not the same as those being used by the software developers at the PCEHR Wave Sites. Transition arrangements are being negotiated.

Appendix 3 Software Developer Resource Centre

This provides a list of documents claimed to be final and specifications relating to ehealth

SDRC at 22 January, 2012 website headings	**subject areas**	**docs**	**pgs**	**COMMENTS**
PCEHR Core				
	B2B Gateway	9	344	154 pages added since Jan 1,2012
	Call Centre	0	0	Nothing & no due date
	Participation&Authorisation	1	30	
	Portlet	0	0	Due 20 Jan/22 Jan 2012 nothing
	Core Security	0	0	Due Dec/22 Jan 2012 nothing
	Conformant Portal	0	0	Due 20 Jan/22 Jan 2012nothing
	Repository Services	0	0	Nothing & no due date
	Conformant Repositories	0	0	Nothing & no due date
	Template Service	3	115	68 pages added since Jan 1,2012
eHealth Foundations				
	Architecture & Standards	0	0	
	eHealth architecture	2	298	TigerTeam input still required
	PCEHR architecture	1	125	Awaiting update
	NESAF	4	398	All awaiting March12 update
	SMD	2	49	Marked for review & comment ?2009?
	NASH	0	0	Due 20 February, 2012
	HI	0	0	Refer to Medicare NB $34mill MOU
	PCEHR Foundation Informatics	0	0	No due date
	National Product Catalogue	5		Cannot open documents
Clinical Documents	Advanced Care	7	257	Some docs list known unresolved issues
	eDischarge	5	392	Cant open some/"Illustrative purposes
	ETP	17	1021	Completely wrong document set
	eReferral	7	68	"Final"but 9 issues to be resolved
	Consumer entered notes	7	224	Updates expected/known issues
	Consumer entered health summary	7	264	Gender issues will not be done til r. 2
	PCEHR Event Summary*	8	679	"Known Issues" &refers to other docs
	PCEHR Shared Health Summary ^	7	408	"Known Issues"
	Specialist Letter	7	752	"Known issues" & refers to other docs
	Common Specifications #	5	145	Refers to docs that are TBD?
		105	**5616**	

KEY for Appendix 3

***refers to related reading and other documents but doesn’t indicate where they are**

^ refers to changes to audit and medicolegal issues - not sure reflected In current PCEHR legislation

# References - lists 15 documents of which 7 are "under development"

NOTE (a) no notification for documents added since 17 November, 2011(no RSS feed or other)

NOTE (b) There is no indexing within documents on this or the other NEHTA sites

NOTE (c) Medicare Hi Service is noted as "operational"

NOTE (d) A conservative estimate would suggest there are at least 100 documents to come – another five and a half thousand pages?

NOTE (e) No information about clinical terminology – SnoMED or AMT.

Appendix 4

The National Healthcare Identifier Service Current state and issues November, 2011

(An MSIA white paper from the Medical Software Industry Association (MSIA) CEO Forum held 18-19 Oct 2011)

Scope

This discussion paper identifies current issues with the HI service that may impact software vendors, MSIA members and associated software products. Its purpose is to inform member companies and MSIA policies related to HI Service implementation and related software products and interfaces. This white paper was adopted at the MSIA CEO forum (Oct 18-19).

Introduction

The Health Identifier (HI) Service has now been in operation since 1 July, 2010.
The Service provides management capability for three numbers – a patient Individual health identifier (IHI), a clinical provider identifier (HPI-I) and a healthcare organisational identifier (HPI-O). All three identifiers have the same 16 digit format with the type of identifier specified in the first 5 digits which are the same for all identifiers of the same type.

The HI Service is operated by Medicare under specific enabling Federal legislation passed in June 2010. It was designed by NeHTA using web service technology with security provided by location specific (Medicare) PKI certificates. Whilst it is based on W3C web service standards, the actual HI Service interface specification is not based on any standard. There are no plans at present for it to become a Standards Australia standard despite past undertakings by DoHA that funding would be provided for that process. The detailed HI Service specification was developed largely without health software vendor input and it is only now, as members are considering implementation in relation to the PCEHR, that many issues are coming to light. In particular, standard functionality associated with any identification management system, which had been assumed to be available, has been omitted due to “privacy concerns”.

MSIA made the case that the HI service could be used in an unsafe manner and that Medicare was not an appropriate body to be performing software conformance testing. This was strongly opposed by NeHTA. After considerable discussion, the need for a patient safety focussed, conformance/compliance regime was agreed as a mandatory requirement by DoHA, NeHTA and Medicare. Subsequently an HI Conformance and Compliance process has been developed under the governance of the Conformance, Compliance and Accreditation Governance Group(CCAGG) by joint NeHTA/Industry Working Groups. The initial set of Use and Test cases including restrictions on allowed search types and the software testing infrastructure was first available in late June, 2011.

As at October, 2011 only the Test Cases related to verified IHIs, HPI-Is and HPI-Os have been completed and published. Work continues on Test Cases for unverified and provisional IHIs, transfer of identifiers between organisations in electronic messages and documents and implementation of Contracted Service Providers (CSPs) among others.

A number of software products have completed all requirements and are accessing the HI Service as part of NeHTA's Wave 1 program. However, exact numbers remain unpublished. IHIs and HPI-Is have been allocated to all patients (by Medicare) and all providers (by AHPRA). Assignment of HPI-Os is very slow due to difficulties in the registration process and it is likely (Medicare is unable/unwilling to provide exact figures) that there are only a few hundred healthcare organisations currently registered.
MSIA volunteers spent hundreds of hours negotiating the Medicare HI Developer vendor agreement, meeting with DoHA, Medicare and NeHTA on countless occasions, and participating in development of the HI conformance test cases and processes. Despite that considerable investment of resources, significant issues remain.

Functionality
(a) Patient Identifiers (IHI)
Exact versus statistical matching
Whilst all patients have been allocated IHIs, it is necessary to search for an IHI (interactively or via a batch process) to identify the IHI associated with a specified patient and assign this to the local patient record. During the design of the HI service, it was decided to specify this process to use exact matching only i.e. an IHI will be returned, if and only if, all data supplied for a search matches the demographics associated with a target IHI. The data returned is only ever the data supplied plus the IHI if one and only demographic match is found. This design was a consequence of privacy concerns that searching could be used to return information on patients not being treated by the organisation/provider conducting the search.

Such a design is unusual for a patient identity service. The majority of (?all) patient management systems use a statistical matching process, where all patients matching a set of criteria are returned along with as much additional demographic information as possible. An interactive process between the operator and patient is then used to identify the patient. Those involved in patient identification understand the limitations of an exact matching process in the real world of imperfect demographic data.

Testing by the ACT Health service and DHS Victoria in late 2010, demonstrated that using the extensive set of possible searches initially implemented could produce match rates of up to 77%. However, it was apparent that some of these matches were erroneous, principally due to the source data being inaccurate or out of date. It was subsequently recommended that until further research was available, searches should be restricted to five types based on a known IHI, DVA number or Medicare number with only one search based on name, DOB, sex and full address. The requirements for searching by address mandate that every possible address data element be populated in a fully atomic manner. This makes such searching unimplementable by the vast majority of (?all) current healthcare software products.

With the search type restrictions, match rates in the ACT Health trial and subsequent wider testing under an IBM contract with Medicare, were between 50% and 60%. Restricted search types were specified as part of the HI CCA process as a patient safety measure. Obtaining results from these investigations has been difficult outside of the Jurisidictions and in some cases only made available many months after the research was completed. Similar research in the private sector has not been undertaken prior to, or as part of, the Wave 1 projects. DHS Victoria recommended that IHIs could not be used safely in the public sector unless an associated Hospital Medical Record Number was also available.

However, the effect of this search restriction is that a Medicare or DVA number (which has preferably been previously validated using Medicare Online), is needed to discover an unknown IHI. In addition a “known” IHI supplied from an external source (e.g. messaging or from the patient) can be verified against the HI service. NeHTA, as part of the Wave 1 initiative, is currently deploying third-party software (a “bolt-on”) which may be injecting IHI’s into GP practice management systems for upwards of 250,000 patients without any support contracts or integration agreements in place with GP practice management systems. Repeated requests by MSIA to Peter Fleming (CEO of NeHTA) and DoHA, via the CCAGG, for detailed technical information about this process and the possible consequences for MSIA member software products and patient safety, have not been fulfilled. Requests to convene a special meeting of the CCA Working Group to review the conformance points and possible safety implications in light of this unexpected usage of the HI Service have likewise not occurred.

(b) Healthcare Provider identifiers (HPI-I)
Verifying or searching for HPI-Is can only be performed if the provider has chosen to opt-in to the Medicare Provider Directory (a separate entity to the HI service). Currently, very few practitioners have chosen to do so (again Medicare is unwilling to provide figures), making it in general impossible to validate an HPI-I supplied by an external source or to search for an HPI-I. Consequently, it is unknown what issues may arise with searching or other functions. The opt-in nature of the HPI-I, results in the HPI-I providing no clear additional benefit over the healthcare provider identifiers used in eHealth communications today.

(c) Healthcare Organisation Identifiers (HPI-O)
The small number of HPI-Os means there is still very limited experience with their use and management. Verifying or searching for HPI-Os also can only be performed if the organisation has chosen to opt-in to the Medicare Provider Directory. It is unknown what proportion of organisations registered with the HI Service, have opted into the Medicare Provider Directory. It is likely that even if the top level (seed HPI-O) of an organisation

opts-in to the Provider Directory, that associated sub-sections/departments of an organisation (Network HPI-Os) will not. The inability to validate such HPI-Os will make the proposed usage of HPI-Os as messaging endpoints and linkage to the Endpoint Location service (ELS) at best problematic, and in reality, impossible.

(d) Linkage of HPI-Is to HPI-Os

Much of the benefit of HPI-Is and HPI-Os was to be derived from the facility to provide a linking mechanism so that HPI-Is could be associated with one or more HPI-Os. This in theory would make it possible to discover and/or verify that a given provider did indeed work for a given organisation. This capability would mean that software could check that information had been prepared by a person with appropriate authority. For example that a discharge summary had been prepared by a provider associated with the hospital the patient was discharged from or a prescription for restricted drugs came from an appropriate institution and had been prescribed by a provider associated with that organisation. However, again due to privacy concerns, the general ability to access HPIO to HPI-I links has been restricted to authorised administrators (Responsible Officers (RO) and Organisation Maintenance Officers (OMO). It is thus not possible, even if both the Organisation and Provider have opted into the Medicare Provider Directory, to discover or, perhaps more importantly validate, an association between an HPI-I and HPI-O. This restriction even applies to the organisation(s) to which an HPI-I is linked. Thus a hospital emergency department could not use this facility to check that an electronic discharge summary had been prepared by a provider working there, prior to transmission. An organisation receiving a discharge summary or prescription could not verify that the HPI-O or HPI-I are valid nor that the provider has a relationship with HPIO contained in the document. Given that any utility for this linkage mechanism has been effectively removed, it is unlikely that anyone will invest the potentially large effort, in setting up and maintaining HPI-O to HPI-I links.

Safety and Liability

The MSIA membership and especially the clinicians employed by MSIA members, have been concerned about the safety and clinical liability aspects of the current HI service since its specification was first made publicly available. More than six months was spent negotiating with Medicare in an attempt to have Medicare accept liability for errors in the HI Service implementation or data. Medicare refused to do so. The current HI Developer agreement is restricted solely to accessing the Medicare HI development environment. Use of the live HI service is governed by the HI Legislation, associated regulations and Common law. Taking legal action against the Commonwealth is rarely a viable option. All MSIA members that have done so in the last three years no longer exist or have been taken over. Published payout figures by Commonwealth agencies seem grossly inadequate redress for damages incurred by these businesses.

This leaves software implementers potentially liable for any and all adverse outcomes arising from incorrect functioning of the service or bad data supplied by the service. Given the failure of the Medicare Online patient verification facility for Medicare numbers (OPV) two years ago, this is more than a theoretical risk. It is known that the Medicare data is not perfect and Medicare has invested a large effort in cleaning its patient data over the last two years. However, it is possible that duplicate and/or replicate IHIs will occur either in the Medicare database or be introduced by operator or system errors in patient management and downstream systems.

At present, even if Medicare is aware of a problem with an IHI it has no mechanism for informing anyone. A proposed blacklist of IHI numbers (with no associated patient demographics) was unable to proceed, because the legislation prohibits disclosure of an IHI to anyone except providers (or their employees) who have a clinical relationship with the patient. IHIs can change (be resolved) and the initial simplistic view that the IHI/patient relationship would be one-to-one has proved incorrect. The addition of Unverified IHIs for newborns and Provisional IHIs for which there are no clear usage guidelines, further complicates the field and introduces safety risks. It has been agreed that a process should be put in place to allocate verified IHIs to newborns. This is planned to be available before July, 2012. On that basis, the HI CCA Technical Committee has recently recommended that unverified IHIs should not be used as the balance of utility to safety, given current policy settings, was too low.

For the last two years, MSIA has repeatedly requested from NeHTA and DoHA a copy of the safety report on the HI service which the NeHTA CEO disclosed had been undertaken. This has been refused even on a confidential basis. MSIA subsequently initiated an FOI application with DoHA and Medicare (NeHTA was discovered to be FOI exempt) to obtain this document, but this was refused by Medicare (too much work) and DoHA indicated informally they did not have it.

A reasonable inference from this is that, either the work has not actually been undertaken, or that there are serious identified safety concerns that have not been disclosed. The HI legislation provides serious fines and jail sentences of up to two years for anyone accessing an IHI other than as permitted in the legislation. Whilst there is a two year grace period when penalties may be waived in some circumstances, this will expire on 1 July 2012, the “go live”date for the National PCEHR. Currently this means that testing a software system against the live IHI service places all software vendor companies and personnel at risk if they should deliberately or even accidentally access or disclose a patient’s IHI.

An additional facility (Contract Service Provider or CSP) was included in the legislation at the last minute, at MSIA’s insistence. This allows a provider to nominate a CSP (such as their software vendor) that is legally able to access Health Identifiers for patients associated with that provider. The CSP facility has been implemented in the Medicare HI service in mid-October but the related conformance Test cases have not yet been completed. Use of CSPs will not be possible until that work is finalised and incorporated into conformance testing procedures, which is likely to take some months.

Without the availability of CSPs and contracts between software vendors and providers to give them force, any maintenance performed on software that accesses the live HI service or manipulates patient IHIs, is hazardous.

Outstanding Issues and recommendations

Issues:

- The HI service as currently implemented, provides no benefit for identifying patients over that provided by a Medicare Number or DVA number for the vast majority of patients.
- Some concerns over issues for patient safety remain unaddressed.
- Software vendors connecting to the live HI service assume all liability for outcomes and potentially expose their employees and companies to serious sanctions, including jail terms.
- It is not possible to electronically discover or verify the vast majority of HPI-Is or HPIOs (those that have not opted into the Medicare Provider Directory) and there is little experience in their use. It will be necessary to enter HPI-Is and HPI-Os manually into software systems and any accidental misallocation of an HPI-I to the wrong provider or an HPI-O to the wrong organisation, will be unable to be detected. This invalid data will then be able to disseminate via messaging, throughout the eHealth system as none of the receiving systems will be able to perform a validity check.
- There are very few HPI-Os and little or no experience in their use
- The inability to verify the relationship between an HPI-I and HPI-O (other than for an organisation's administrators) has serious implications for utility and safety of proposed specifications for electronic transfer of prescriptions (ETP) as well as a number of other electronic documents.
- Medicare is unwilling to reveal figures on HI service usage, HPI-O availability or Provider Directory opt-in rates other than once a year in its annual report published for the first time recently.
- NeHTA continues to not disclose relevant HI Service patient safety risk assessments and will not reveal quality control and patient safety oversight of the Wave 1 IHI roll-out.
- NeHTA have assured MSIA that all Wave 1 contracts include appropriate liability waivers for software vendors. Requests to provide MSIA with the relevant clauses from these contracts have been denied.

MSIA has been a long-standing advocate of the need for a National patient identifier. Unfortunately, privacy and legislative constraints have significantly restricted the functionality and utility of the HI service to the point where sustainable business drivers for implementation and patient benefits from use of the HI service are difficult to identify. In addition, use of identifiers for providers and organisations that cannot be validated electronically, introduces a level of risk that is unacceptable for the entire eHealth system. The failure of NeHTA to release the patient safety risk assessment apparently undertaken a year ago, indicates that at the very least, they have also found serious issues.
MSIA has proposed a funded "all of sector" roll-out strategy for the HI Service but this has been rejected by NeHTA and DoHA. NeHTA indicated that roll-out of identifiers will occur as part of the Federal government agreements with the pathology industry and pharmacy sector. Identifiers will then flow into primary and specialist care systems. This ignores the fact that the information flow is from primary care and specialists to pharmacies.

Discussions with the pathology industry indicate that they have tied their implementation of identifiers to a prior implementation of electronic requesting, at least in part, so that identifiers would flow from primary care and specialist care into the pathology systems. Specialist and Primary Care providers have little understanding of the potential benefits of health identifiers. A recent survey by MSIA showed that very few customers have expressed interest in systems that support national identifiers.

Lack of demand for healthcare identifier capable systems is likely to remain a serious barrier for the foreseeable future outside of the Wave 1 and Wave 2 projects.

Recommendations - Implementers should :

1. Ensure they have read the DHS Victoria HI implementation guide (available from the NeHTA web site) and are familiar with the HI CCA requirements.
2. Take legal advice with respect to potential liability, inform their software indemnity insurers and ensure end-users sign comprehensive liability waivers.
3. Wave 1 and 2 implementers should ensure that contracts with DoHA and NeHTA include appropriate clauses concerning HI liability.
4. Consider deferring implementation of IHIs until CSPs are available and use them in implementations. Associated contracts with providers, nominating the software supplier and maintenance organisations, will be required to reduce the risk of accidentally attracting criminal sanctions. Note it is not possible to contract out of criminal liability.
5. Consider deferring implementation of the HI Service until user awareness and demand warrants it. A recent show of hands at the Australian Association of Practice Managers (AAPM) conference indicated that only a small minority had any interest in implementing an Identity service by July, 2012.
6. Assess long-term implementation and support costs given that the HI service is being updated every 3 months and the developer contract ensures that only the current version and the previous version will be supported by Medicare. In addition, the costs of HI conformance/compliance testing is likely to rise steeply given the effective exclusion of the only “not-for-profit” e-Health NATA accredited testing laboratory (AHML).
7. Consider implementing manually entered IHIs solely for patients without Medicare or DVA numbers.
8. Consider using a third party agent to perform HI service access under a CSP enabled contract only if required by Users or government contract.
9. Consider implementing Medicare Online patient checks for Medicare and DVA numbers as a proven alternative without the risks of fines and criminal liability. MSIA can provide source code to facilitate this.
10. Engage with proposals for electronic documents that incorporate HPI-Is and HPI-Os in order to understand the safety risks and implementation challenges of incorporating identifiers which cannot be validated, and the associated implications for security and liability.

APPENDIX 5

TRUSTED INTEROPERABILITY AND THE PATIENT SAFETY ISSUES OF PARASITIC HEALTH CARE SOFTWARE

Vincent B McCauley[1] and Patricia A H Williams[2]
[1]Medical Software Industry Association, [2]Edith Cowan University
[1]vincem@mccauleysoftware.com

[2]trish.williams@ecu.edu.au

Abstract

With the proliferation of software systems and products in the healthcare environment, it is increasingly common for such software products to be constructed in a modular design. However, for modular software to be securely interoperable with other software products requires agreed consistent and accountable interfaces. This agreement may take the form of bilateral vendor to vendor arrangements or via a trusted external third-party who coordinates agreed interaction methods, such as a jurisdiction. Standards are a particular form of mutually trusted third party. Unfortunately, this agreed method of interoperability is not always present in vendor software. Where one software product or module interacts with another, in the absence of any agreement, it is referred to as —bolt-on‖. It is perhaps more descriptive to refer to such software in terms of its potential to cause harm and refer to it using the biological analogy of —parasitic‖ software and associated —host‖ software. Analogous to biological systems, parasitic software can operate by data injection into or data extraction from, the associated host database. Both forms of parasitic software exploit access mechanisms or security flaws in the host software independent of the host vendor and in ways not intended or supported by the host vendor. This paper discusses the mechanics of this security vulnerability and more importantly, the potential adverse consequences to patient safety of such susceptibilities. As Australia moves to a national connected e-health system these issues are causes for grave concern. This paper provides a case study of this insecurity to highlight the problem, promote discussion and encourage potential change.

Keywords
Medical software, health information security, third party software, healthcare software, bolt-on software.

INTRODUCTION

The explosion of software products and information systems for healthcare has seen an increase in development of these software products in modular form. Many of these products are sitting _on top of‘ or _alongside‘ existing software providing additional services. The additional services range from aggregation of data for the purposes of healthcare management to programs that facilitate integration of systems with existing products and databases. Healthcare providers currently have to rely on independent third party software/services vendors for access to the essential services of the new national e-health system, such as the Health Identifiers Service (Medical Software Industry Association, 2010). The importance to the healthcare environment is in the benefits that such third party software can provide in both the integration of electronic services and in providing facilities such as clinical audit tools and healthcare practice analysis.

The third-party software is referred to as _bolt-on‘ because it is providing specific functionality outside the normal applications used. As such, these products are of modular design because they are not systems that can run independently of a main (or host) system and its associated databases. However, for modular software to be securely interoperable with other software products requires agreed consistent and accountable interfaces. By definition these applications bolt-on and make use of the existing systems and databases. Parasitic software is a form of bolt-on software that the host system is not aware of or has no agreed consistent and accountable interfaces with.

This paper discusses the mechanics of the security vulnerabilities associated with bolt-on and parasitic software, and their potential impact. This is considered in the context of the Australian e-health environment with specific examples and the important issue of patient safety.

SECURITY ISSUES WITH SOFTWARE

Research has shown that most common vulnerabilities in software are caused by a small number of coding errors and practices (CERT, 2011). These common vulnerabilities and those specific to third party and parasitic software include buffer overflows, input manipulation and application authentication.

Common vulnerabilities

Buffer overflows (or boundary checking) occur where a program writes outside the buffer limit effectively violating memory protection. Due to the various mechanisms that can induce buffer overflows, they are a specific vulnerability in software that can be readily maliciously exploited. These mechanisms include simple arithmetic variable overflows, stack-based overflows, and heap-based overflow attacks. This issue is particularly prevalent when using languages that do not inherently have boundary checking as part of their construction such as C and C++ (Goodrich & Tamassia, 2011).

Input manipulation is vulnerability where filtering and sanitization of data input is not performed adequately. This is not restricted to direct data input; it also applies to data passed from client to server as in web based applications (Ravel & Fichadia, 2007). This vulnerability includes SQL data injection, cross-site scripting, light weight directory access protocol (LDAP) injection used for accessing and updating directories, and application specific input as is common with data passed between web browser and web servers. Format string attacks are another specific type of input manipulation error.

Application authentication, where a user is verified before being allow access, is the basis for right of entry to, and use of, an application and its associated data. Control of connections to a database can be complex and depend on server security controls, database access control, and access restrictions (Burtescu, 2009). In the case of third party software this refers to the authentication of another application to have access to the host application and its associated databases. To date, this third party authentication has been mainly unconsidered in the design of existing healthcare software.

Other vulnerabilities relate to the use of application add-ons (usually web based) and cookies, the manipulation of session ID's, lack of change management control, and the security present in the operating system and databases.

Parasitic software vulnerabilities

Parasitic software has specific application of the common vulnerabilities and as such presents specific threats to host software.

Buffer overflows

Buffer overflows are a real vulnerability in non-standard, parasitic software (Posey, 2005). This is an issue particularly if the host application is running without minimized privileges. Also, where the parasitic software has not followed established standards of development, or has not been developed consistent with the style and construction of the applications and database that it is interacting with, this is a significant threat.

Input manipulation using injection

Analogous to biological systems, parasitic software can operate by data injection into or data extraction from, the associated host database. Both forms of parasitic software exploit access mechanisms or security flaws in the host software independent of the host vendor and in ways not intended or supported by the host vendor. Cross-site scripting may become a larger issue for healthcare as more systems become web-based rather than server-based applications (Symantec, 2008).

Application authentication, unintended uses and change management

The application architecture relies on the application knowing the level of security of its databases and operating system interfaces. When a third party software product is introduced it must rely on an agreement between the applications and provide connection to the appropriate databases. Unfortunately, the databases are often not secured and this access does not require a secure level of authentication.

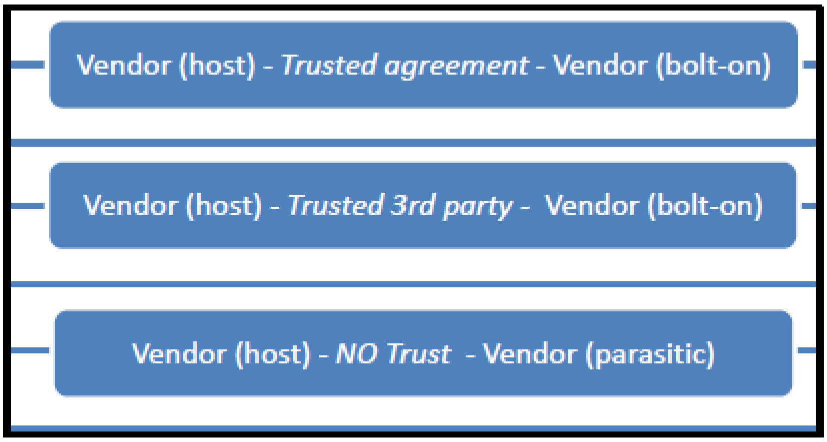
In addition, many existing software products were not designed with the new e-health systems in mind, and therefore lack sufficient controls in regard to bolt-on and parasitic software programs. In effect, unintended use of their associated databases is occurring without sufficient security design measures in place. This leaves the integrity of the data at risk. Further, when program updates occur in the host program, the parasitic software, that has not (by definition) been developed in synchronisation, may be unaware of the changes to the host functionality and database resulting in potential malfunctions and vulnerabilities. Where a bolt-on program has agreement with the host system this may not be an issue as long as there is tested integration between the host application and bolt-on product.

PATIENT SAFETY IN HEALTHCARE SOFTWARE

Conformance, compliance and standards

The role of standards is to ensure safety and reliability, and that software performs consistently in the way it was intended to perform, to a tested and expert specification. Providing a uniform set of rules using a standard also provides a metric for conformance testing (CERT, 2010; Standards Australia, 2010). In considering the security in using bolt-on third party software, the solution lies in the agreements between the software product and vendors. This agreement may take the form of bilateral vendor to vendor arrangements or via a trusted external third-party who coordinates agreed interaction methods, such as a jurisdiction. Standards are a particular form of mutually trusted third party. Unfortunately, this agreed method of interoperability is not always present in vendor software. Where one software product or module interacts with another, in the absence of any agreement, it is referred to as a ―bolt-on‖. It is perhaps more descriptive to refer to such software in terms of its potential to cause harm and refer to it using the biological analogy of ―parasitic‖ software and associated ―host‖ software. Figure 1 illustrates the different types of software agreements applicable to bolt-on software. As can be seen, the bilateral agreement allows for accreditation, and therefore assurance, between the host and bolt-on providers. Where a trusted third party such as a jurisdiction manages the interactions between software vendors this provides a mediation alternative. Conformance to standards is an example of this. Where no concurrence in use of standards, or demonstrated conformance, or agreement is established the relationship is referred to as parasitic.

Figure 1- Trusted interoperability of modular software security agreements


Vendor (host) - *Trusted agreement* - Vendor (bolt-on)
Vendor (host) - *Trusted 3rd party* - Vendor (bolt-on)
Vendor (host) - *NO Trust* - Vendor (parasitic)

Examples of safety issues managing patient identity information

These issues associated with parasitic software are not restricted or peculiar to the healthcare domain. However, the potential for more devastating outcomes from the exploitation of the vulnerabilities are specific to this domain. A well known example of such parasitic software using data extraction is the PEN Computing Sidebar application (PEN Computer Systems, n.d.). It accesses data directly from the database of the host software (e.g. Medical Director) using access mechanisms that were put in place by the host vendor to permit interoperability amongst its own product suite. However, this software does not manipulate patient identity information and the majority of extracted data is presented as aggregates.

The safety issues apparent with parasitic software when managing patient identification and identity, in particular the new Australian e-health individual health identifiers (IHI) are one example. The following are some scenarios of how parasitic software can lead to serious patient safety risks in the context of managing patient IHIs.

Data injection example:

A typical circumstance might be

1. The parasite software designer identifies an —unused‖ column in the host patient database table. For example one called patient_id2;
2. This is done without input from the Host vendor. The column is not populated in any of the clinical desktop systems examined;
3. The column has a data type compatible with the 16 digit format of the IHI;
4. Unknown to the parasite software designer, this column is intended for future use as the patient identifier for anonymous pathology testing as required for HIV tests. It has been designed to use the same ISO based identifier standard as the IHI. The patient identifiers will be unique across sites but specific to the host software product. It will be sent to the pathology lab along with the sex and DOB as the patient identifiers;
5. The parasitic software is deployed. It accesses the host patient table and uses the patient demographics to obtain a corresponding IHI from the Medicare HI service and these are stored in the host patient_id2 column; and
6. Sometime in the future, a host software update implements the use of patient_id2 for anonymous pathology testing. The parasitic software vendor is unaware of this update.

Scenario 1: Data injection

The parasitic software extracts what it thinks is an IHI from the host and sends it in a message to software that is not connected to the validating HI Service. However, it is in fact the host software‘s new internal patient identifier. This incorrect —IHI‖ which may match to some other patient, rapidly spreads to the attached systems.

Scenario 2: Data injection

The host software sends an electronic request for an HIV test to a laboratory. The parasitic software notes the patient associated data has been updated and checks the IHI against the HI service. It finds the IHI is incorrect (because it is in fact a host internal patient identifier) and updates it to the value obtained from the HI service. When the HIV result message is returned noting a new positive result, the patient identifier cannot be matched and the result is discarded. The patient‘s treatment is delayed and a number of sexual partners are consequently infected.

Data extraction example

In these scenarios the parasitic software extracts a copy of the patient demographics and the host software‘s unique patient identifier into a database managed by the parasitic software. It accesses the HI service and adds IHIs to a locally maintained database.

Scenario 3: Data extraction

The host software operator cleans up old patients who have not been seen for some years. These are assigned a new archive patient identifier key and the previous patient identifier keys are re-used as new patients are added to the database. This is necessary in some mature products as the internal patient identifier keys are only sixteen bits and support a maximum of 37267 active patients. The parasitic software is designed to intercept messages being sent out from the host and add IHIs. It does this by matching the host patient identifier contained in the message to its IHI table. New patient identifier keys are assigned starting at the highest patient identifier of the cleaned up patient data. This leads to some patient identifier keys for archived patients being reassigned to new patients. Hence patient identifier keys that have been re-used in the host software will subsequently have the incorrect IHI inserted. Message receiving software that has access to the HI service will detect this error and reject the message. Receiving software that is not able to access the HI service will propagate the incorrect IHI. This may lead to pathology results being filed against the wrong patient or pathology requests and specialist referrals not being received.

It is common practice in software to read the unique patient identifier from the underlying database and then use this as an update key. Where the patient identifier key is shared across different software components any update must involve a two-stage commit process to keep entries in both products synchronised. However, in the absence of this practice in loosely or poorly coupled systems, it is impossible to keep the two separate databases synchronised as there is a deficiency in the required tightly coupled commit process. Failure to implement a two-stage commit for updates across heterogeneous systems, risks updates being applied to only one system and the data becoming inconsistent.

Scenario 4: Data extraction

The host software operator enters two new patients David Smith and his twin John Smith. The parasitic software scans the host patient table, notes these two new entries and adds them to its local patient table after obtaining their IHI from the HI service using their name, DOB, sex and associated Medicare number. David is seen by a doctor that day but John has an appointment for next week. When John comes in, it is discovered that David‘s consultation notes have been entered by mistake into John‘s record. Because the notes can only be altered by David‘s doctor who is not working that day, the front desk staff fix this by changing John‘s name and demographics to David‘s and vice-versa. Now the notes are associated with the correct patient. However, the parasitic software has no mechanism for being informed this has occurred and has incorrect data associated with the Host‘s patient identifier. Subsequently, outgoing messages have the incorrect IHI inserted and this is disseminated. If the parasitic software manages incoming messages on behalf of the host, the data will be matched to the wrong patient if the IHI, surname and DOB are used to perform patient matching.

In this case the two record updates effectively create a transposition of records. Products that have significant penetration of the Australian primary healthcare marketplace currently allow this scenario in their software. Whilst it is acknowledged this is not current best practice software design, it reflects the level of flexibility often required by medical practices and only becomes of major concern when third-party software is also accessing the patient demographics in an uncontrolled manner.

Example summary

In general, maintaining coherence of shadow tables is impossible without a closely coupled communication (insert/update/delete) mechanism. The nature of the software host/parasite relationship precludes this possibility. Once an exact matching view of the host demographics table in the parasite‘s database is lost, it becomes possible for IHIs to be associated with stale or incorrect patient demographics. Depending on the functions using IHIs that are incorporated into the parasite software, this can have significant local patient safety implications. If the parasite software is used to insert IHI‘s into outgoing messages, the invalid information can be rapidly dispersed across the eHealth system. Similar arguments apply to other Australian e-health identifiers for individual healthcare providers (HPI-I) and healthcare provider organisations (HPI-O) although the implications for patient safety may be less significant. Nonetheless incorrect or invalid HPI-Is and HPI-Os could cause significant disruption. In the Australian context, the inability to generally be able to validate the HPI-Is or HPI-Os using the HI service in its current design, to ensure that they are matched to the correct provider and organisation, means that they are more vulnerable to error and dissemination of erroneously matched identities. The Standards community has recognised the safety concerns that arise when multiple interacting e-health software components are introduced without adequate coordination and attention to demographic data coherence. It has taken many years to develop this standards based approach. The international standards organisation Health Level 7 (HL7) incorporates a Clinical Context Object Workgroup (CCOW) Committee which works in conjunction with the HL7 Security Committee specifically to define standards for _linking‘ applications in a secure manner. This standard means that applications are aware of the context in which they operate and ensures that data, and in particular patient demographics, are synchronised and their integrity assured (HL7, 2010).

RECOMMENDATIONS FOR CONFORMANCE AND COMPLIANCE

There are minimum levels of safety that must be assured before deploying software in the health environment, and economics are independent of this minimum level. Indeed, there are always implementation and development costs, however it is only above this minimum threshold that such costs become relevant. At advanced levels it is acceptable that cost benefit analysis should be considered. However, where there are real risks to patient safety that are unacceptable, the fundamental software design needs to be changed and the insecure software design practices need to be forbidden.

Recommendations for software conformance and compliance testing need to be contextualised for the specific functionality of the software integration in place, and thus its status and resulting adverse security impacts, would be minimised.

Using the examples above of the HI Service, recommendations are given below such that software submitted for HI conformance/compliance testing should declare whether it manages IHIs on behalf of other software products either by injection or extraction. If it does manage IHI‘s, it must conform to the following:

1. Describe the communication mechanism with the underlying (host) software, noting potential delays in recording demographic changes;
2. Subsequent testing should be performed both within and outside of the time window in which changes to the host tables are reflected in the IHI Manager‘s tables;
3. Describe the purpose for which Health identifiers are maintained and used – this may have implications for subsequent test use cases. This should be noted on the test report;
4. Software must be tested with any and all software on whose behalf it manages Health Identifiers, as a single test unit. All possible combinations of host and parasite need to be tested;
5. The software that connects to the HI service must demonstrate that it continues to maintain correct patient demographics and the correct associated IHI for every possible operation involving patient demographics supported by each of the intended underlying software hosts (patient demographic data coherence), and especially for patient record merging and de-merging operations; and
6. The testing report should nominate each specific combination of software and the versions of each that were tested.

The examples discussed above are not a comprehensive list however they give an insight into the type of exploitations that are possible. Not all software of this nature is _unsafe‘, but given the potential for rapid proliferation of errors, opportunities for unprofessional practice and exploitation of database vulnerabilities, there is significant cause for concern. Incorrect patient identity information can be disseminated as demonstrated by the incident last year, in 2010, when there was an incorrect update by Medicare to the Medicare Online Patient Verification system such that it returned incorrect Medicare numbers. Because of the closely connected nature of the eHealth IT systems, these incorrect values were distributed rapidly to local attached systems and dispersed across the community. This type of incident will be a major issue as Australia implements its connected e-health system. It is the potential adverse consequences to patient safety of the security susceptibilities discussed that require addressing at the level of software design, implementation and use.

CONCLUSION

Assurance of patient safety should outweigh all other issues in regard to the use of software in healthcare. The examples given with the current specification of the HI service and the interaction with Australian legislation highlights the problems with parasitic bolt-on software. These types of problems will only become more prominent and more prolific as the e-health systems in Australia are established and as healthcare providers make more use of the e-health opportunity. There is no doubt that the use of bolt-on programs can be of benefit in many areas of healthcare provision and administration as long as appropriate governance and testing is in place As Australia moves to a national connected e-health system these issues are cause for grave concern. The recommendations for improvement given in this paper address some of these specific concerns. However, what is required for a safe future in the healthcare software industry is a broader and more coordinated approach to software development and interoperability where third party software is concerned. There is no doubt that the benefits to our healthcare system and improved patient outcomes can be realised as long as due consideration is given to this important and fundamental software security issue.

REFERENCES

Burtescu, E. (2009). Database security – attacks and control methods. *Journal of Applied Quantitative Methods, 4* (4), 449-454.

CERT. (2010). *Secure coding standards.* Retrieved from http://www.cert.org/secure-coding/scstandards.html.

CERT. (2011). *Secure coding.* Retrieved from http://www.cert.org/secure-coding/.

Goodrich, M.T. and Tamassia, R. (2011). *Introduction to computer security*. USA: Pearson.

HL7. (2010). Clinical Context Object Workgroup. Retrieved from http://www.hl7.org/Special/committees/visual/overview.cfm

Medical Software Industry Association. (2010). Submission on Proposed Regulations for the Healthcare Identifiers Service. Retrieved from http://www.health.gov.au/internet/main/publishing.nsf/Content/eHealthregs-047/$FILE/047_Medical%20Software%20Industry%20Association_12-04-10.pdf

PEN Computer Systems. (n.d.). *Primary care sidebar.* Retrieved from http://www.pencs.com.au/product-sidebar-overview.html

Posey, B. M. (2005). *Buffer overflow attacks: How do they work?* Retrieved from SearchSecurity.com

Ravel, V. and Fichadia, A. (2007). *Risks, controls and security: Concepts and application*s. NJ, USA:Wiley.

Standards Australia. (2010). *Benefits of standards*. Retrieved from http://www.standards.org.au/DevelopingStandards/BenefitsofStandards.aspx.

Symantec. (2008). *Symantec Internet Security Threat Report: Trends for July–December 07.* Retrieved from http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_exec_summary_internet_security_threat_report_xiii_04-2008.en-us.pdf

Appendix 6 EHealth Foundations for PCEHR

The report on the E-Health foundations for the PCEHR system as written in the Department of Health and Ageing Submission to the Senate Inquiry (page 4) should not go unchallenged. We had the NEHTA "Year of Delivery " in 2009 – that we have reached 2012 with none of these e-health key foundations completed is a failure of governance, oversight and accountability. MSIA recommends that the Inquiry considers the difficulties in making development business decisions when the "deliverables" – the "e-health foundations" are yet to materialise. See http://m.zdnet.com.au/this-is-the-year-of-delivery-nehta-339294585.htm

(MSIA comments below in bold italics)

"3.1 E-health foundation for PCEHR system

In 2005 the Australian Government and state and territory governments made a commitment to advancing e-health in Australia by establishing NEHTA.
NEHTA has developed and is implementing a number of key foundation e-health standards, specifications and services. By 30 June 2012 NEHTA will have accomplished the following achievements.

(2005-2012 and still not one of (a)-(f) below are functioning as intended)

(a) HI Service established, enabling the safe use of healthcare identifiers in patient information systems resulting in accurate patient identification and fewer adverse events from incorrectly matched data;

$34 million announced January 2012, for upgrades, but as this submission articulates, this system is not working as intended, does not provide a "unique" patient identifier, and can only be used safely to identify patients when used in combination with existing and legacy patient identification systems. Parts of the system relating to IHI-Os and IHI-Ps cannot be used yet. A lot of work to be done before 1 July, 2012. It is difficult to see what value is provided over and above what is currently being used.

(b) digital certificates from the National Authentication Service for Health (NASH) introduced to ensure secure access by healthcare providers to essential healthcare information such as e-prescriptions;

As is noted in Appendix 3, the specifications for the NASH are not due until 20th February. NASH does not provide additional security or access controls beyond the existing Medicare PKIs (certificates) that are currently used for e-prescribing and access control

(c) standard approach to the terminology developed and used in healthcare documents transmitted electronically so that clinicians can rely on the accuracy and consistency of the medical terminology that they receive;

This is a IHTSDO (International Health Terminology Standard Development) process -see http://www.ihtsdo.org/ - hardly all NeHTA's own work as implied here. Updates and roll outs paused for AMT (Australian Medicines Terminology) for 5 months late 2011. Not currently implemented except in very constrained sites. Latest information on "how to" use (240 pages) uploaded to NeHTA website on 6 January, 2011. See: http://www.nehta.gov.au/publications/whats-new
The contracts between NEHTA and vendor providers are not finalised. A major problem is that NeHTA will give no warranty that the terminology set is "fit for purpose" and accurate. As one respected provider of such information has said "Why would you risk your excellent reputation and trusted product by using such information?" Terminologies used in healthcare documents are provided in various forms from a number of vendors and used in all clinical software – clinicians rely on the accuracy of this information in their patient interactions.

(d) consistent approach to hospital patients' discharge summaries across jurisdictions developed, contributing to improving the efficiency of clinical decision making;

There are three different versions of discharge summaries being trialled through the NEHTA Wave Sites – so a consistent approach is still to be determined. Existing systems have been exchanging at least a million discharge summaries a month for a number of years prior to NEHTA's existence.

(e) e-prescription specifications implemented, enabling better and safer medications use for consumers across the health sector; and

Industry is waiting for the Technical Specifications to be finalised through the Standards Australia process before implementation. The next review of the Technical Specifications is due in March. It is extremely unlikely that the Technical Standard will be published before 30 June, and therefore the Technical Standard will not be implemented by 30 June.

(f) Australian standards in place enabling software vendors to standardise their secure messaging products.

Old SMD (secure messaging) specifications are currently being used by industry – NEHTA/NT projects are yet to implement the standards referred to here. The current Standards Australia Technical Specifications were developed by NeHTA with a team of vendors but are predicated on a functioning NASH and Healthcare Identifier Service (IHI-O and IHI-Ps) – neither or which we have at present.