

nehta

eHealth



SHAPING THE FUTURE OF HEALTHCARE

HPF08 - Workshop 2 - Privacy Analysis of IEHR

Dr Bridget Bainbridge, NEHTA

10 November 2008

Introduction to NEHTA

- Collaboration in e-health - all nine governments of Australia working together
- July 2005 - NEHTA established as a company limited by guarantee - the vehicle for collaboration
- E-health viewed as critical component of broader health reform agenda
- NEHTA's aim: to develop better ways of electronically collecting and securely exchanging health information



Introduction, cont.

- E-health systems have the capacity to unlock greater quality, safety and efficiency benefits
- NEHTA will support the Australian health system in:
 - Improving the quality of healthcare services
 - Streamlining multi-disciplinary care management
 - Improving clinical and administrative efficiency
 - Maintaining high standards of privacy and information security



Key areas of work

- February 2006: COAG funding of \$132 million assigned to NEHTA for healthcare identifiers (individual, provider, organisation) and clinical terminologies
- COAG requested that Health Ministers report back on progress towards a national approach to electronic health records by 2008
- IEHR business case due to go to COAG by the end of the year
- NEHTA also funded to work on a number of related e-health building blocks (including interoperability, privacy, messaging, authentication)



NEHTA & privacy

- NEHTA is committed to developing effective privacy frameworks because a number of NEHTA initiatives involve the collection and handling of personal/health information
- These must comply with all legislative privacy requirements
- These must take community expectations around privacy into account
- A strong privacy foundation is a pre-condition to success



“Figuring” privacy

- It is common to talk of privacy and consent “solutions”; in policy terms, privacy is much better described as a “wicked problem”
- It is a problem for which there is no magic answer or solution - the best approach is to mirror the dual objectives of privacy legislation itself: to seek to protect personal information *and* to facilitate the free flow of information
- Consent should not be isolated from a broader privacy assessment
- Privacy should not remain an abstract notion: assess it in context, in relation to the requirements of a real project



Understanding privacy risks

- Information privacy poses two distinct, interrelated risks:
 - Failure to comply with legislative requirements, resulting in breach of privacy legislation; and
 - Failure to meet community and provider expectations around what “privacy” protection should be in e-health, resulting in lower takeup
- Usually described as “real” and “perceived” risks - both are important although the former is easier (relatively speaking) to identify while the latter is where we see notions like “trust and confidence” becoming critical
- NEHTA is tackling both strands of analysis



NEHTA's approach to privacy

- *NEHTA's Approach to Privacy* (July 2006)
- NEHTA's Privacy Management Framework - structured and flexible - applied to relevant NEHTA initiatives
 - Initial application UHI and IEHR (commenced 2006)
 - Expanded to "packages" in late 2007 (i.e. pathology, discharge, referral and medications management)
 - Includes PIAs, privacy blueprint process, roundtables, public consultation
- A plethora of issues have emerged - in relation to IEHR, these were recently subject to public consultation



NEHTA's privacy toolkit

- Effective privacy compliance will comprise a combination of:
 - Law
 - Technology
 - Governance
 - Safety net mechanisms
 - Accountability
 - Culture
- NEHTA will continue to build its privacy frameworks based upon a range of privacy tools rather than focusing solely on law



NEHTA's key privacy issues

- Australia's "privacy patchwork"
- Governance & legislative support
- Sensitivity labels
- Proposed controls/limitations on controls
- Authorised & nominated representatives
- Audit
- Secondary use



Practical example: sensitivity labels

- Strong and “intuitive” demand for sensitivity labels in e-health systems
- Existence of “quarantined” sensitive health information is highly contested
- No international examples of a successful implementation, local example of inability to honour “promise”
- Technical environment to support sensitivity labels does not exist yet ...



Questions?



nehta

eHealth



SHAPING THE FUTURE OF HEALTHCARE

HPF08 - Workshop 2 - Planning for E-Health - Applying a PMF

Dr Bridget Bainbridge, NEHTA

10 November 2008

Introduction

- Rapid developments in technology encourage business, government and citizens to move to electronic information systems and online transactions
- This focuses attention on information privacy, particularly its incorporation in the development and implementation of these systems
- Often seen as daunting - e.g. complex patchwork of legislation
- Misconceptions abound (BOTPA); reluctance to consult



NEHTA's response

- These issues confronted NEHTA when it was established
- Development of a robust Privacy Management Framework (PMF) equipped NEHTA to navigate the privacy challenges from the beginning
- The PMF has now been applied to a range of NEHTA projects
- While it has been refined in response to feedback and changes to NEHTA's work program, the fundamental characteristics remain constant



What does a PMF provide?

- A PMF provides the methodology and tools to manage privacy in a structured and proactive manner
- It ensures that privacy work is:
 - Undertaken in alignment with key project phases and activities
 - Integrated into design, architecture and policy
- Privacy stops looking like an insurmountable obstacle, instead becoming a key asset in building trust and confidence in a project



NEHTA's objectives for PMF

- Effective management of privacy across the diverse range of NEHTA projects
- Alignment of privacy work with key project development and implementation phases and activities
- Involvement of specialist privacy advisers throughout the project lifecycle
- Incorporation of privacy as a matter of course
- Proactive identification of where privacy risks or benefits may arise and implementation of strategies to mitigate risks and promote benefits



NEHTA's objectives, cont.

- Proportionality in privacy management
- Flexibility in responding to changes in project scope, approach, design and policy
- Emphasis on community and stakeholder consultation
- Consideration of the impact of new and developing technologies when undertaking privacy analysis, and innovation in responding to any privacy or security issues identified
- Visibility of privacy for all participants



External environment

- NEHTA's privacy work also needs to be able to respond to future national reform:
 - Australian Law Reform Commission
 - National E-Health Strategy
 - National Health and Hospitals Reform Commission



Finding a path forward

- No single prescription would resolve or manage privacy issues across the entire NEHTA work program
- While a Privacy Impact Assessment (PIA) is increasingly used to assist in managing privacy impacts - it is not an answer in itself
- A PIA does not provide the overarching structure, ongoing consideration of privacy issues throughout the project lifecycle, or the flexibility in shaping privacy management to different project contexts, that NEHTA required for its e-health projects
- It was in this context that NEHTA's Privacy Management Framework was crafted



Practical examples for discussion

- NEHTA's National Authentication Service for Health (NASH)
- "Family history" - clinical best practice v. privacy



Questions?

