Health Informatics Society of Australia

in conjunction with the
Australian Healthcare & Hospitals Association

INQUIRY INTO THE HEALTHCARE IDENTIFIERS BILL 2010

Presented to the

Australian Senate

Community Affairs Legislation Committee

in response to the

'Healthcare Identifiers Bill 2010 and Healthcare Identifiers (Consequential Amendments) Bill 2010'

Author: Professor Peter R. Croll

Chair, Health Informatics Privacy and Security (HIPS)

March, 2010

Health Informatics Society Australia Ltd.

This document has been reviewed and represents a formal submission from the Health Informatics Society of Australia	
	Dr Michael Legg, PhD FAICD FAIM FACHI MACS(PCP) ARCPA **President**, **Health Informatics Society of Australia**

Inquiry into the Healthcare Identifiers Bill 2010 and Healthcare Identifiers (Consequential Amendments) Bill 2010

Introduction

The Health Informatics Society of Australia (HISA) in conjunction with the Australian Healthcare and Hospitals Association (AHHA) welcomes the opportunity to provide this submission in response to the Healthcare Identifiers Bill 2010 and Healthcare Identifiers (Consequential Amendments) Bill 2010.

Since 1993, HISA has taken a leading role in promoting e-Health and advancing the e-Health agenda across Australia. We recognise the importance of establishing a national approach to health identifiers that could lead to a safer and more efficient healthcare system. In fact, privacy and security of health information is one of our key specialist areas that we have been supporting through a number of HISA-led initiatives. HISA recognises that advancement of a national e-Health agenda requires extensive consultation and collaboration. To gather responses from a wide range of stakeholders interested in e-Health we have broadened our consultation to include other relevant associations with whom we work closely, in particular, the Australian Healthcare and Hospitals Association and the association members of the Coalition for E-Health.

Prior submissions made by the Health Informatics Society of Australia (HISA) and the Australian Healthcare and Hospitals Association (AHHA) have been supportive of the introduction of a unique health identifier, provided sufficient safeguards are in place. These submissions included to the Department of Health and Ageing on the Unique Health Identifier and two submissions to the Australian Law Reform Commission on the Privacy Law review (IP31 and DP72).

Our collective memberships represent a wide range of professional practitioners in healthcare. Their opinions on the matters of health identifiers have been sought over the past few years through national health privacy seminars, conferences (e.g. Health Privacy Futures 2009), electronic surveys and online discussion forums.

We will address the key issues that were outlined for the Committee to consider during the inquiry.

1) The relationship to national e-health agenda and electronic health records

This Health Identifier Bill is critical to the advancement of the national e-health agenda. Failure to ratify the Bill would be considered a serious impediment in the progress of our nation's ability to deliver safe and high quality healthcare. We believe that electronic health records are an essential component to support the transformational reforms needed across the healthcare sector to meet the challenges of tomorrow. The unique health identifier will provide a necessary first step towards this aim and, provided the necessary safeguards are in place, will solve many inefficiencies through unnecessary and sometimes dangerous duplications. Furthermore, it will facilitate improved outcomes in research allowing our nation to continue to contribute as world leaders in scientific and medical research.

2) The privacy safeguards in the Bill

We recognise that confidentiality and privacy is of paramount importance to both health providers and recipients. The safeguards not only have to provide adequate protection but be perceived as protecting the individual. Failure to appropriately address privacy concerns is seen as one of the main potential 'show stoppers' for electronic health record legislation. Overall, we are encouraged by this legislation that provides penalties for inappropriate use and disclosure.

We believe the Bill should proceed but wish to point out some identified issues that could be addressed through regulations.

Small business operators (as defined in Privacy Act 1988 Section 6D) that provide, for example, secure electronic messaging services for general practitioners may be exempt from the Privacy Act as they are not classed as healthcare providers. The Health Identifiers Bill should require all such small business operators to register under the Privacy Act and be treated as an organisation (Privacy Act 1988, Section 6AE). Small business operators would be classified as an entity under Subclause 20 of the Health Identifier Bill and authorised to collect and use health identifiers for the purpose of authentication in electronic transmissions. It is a concern if any entity is authorised to collect and use health identifiers while they are exempt from the Privacy Act 1988.

3) The operation of the Healthcare Identifier Service, including access to the Identifier

The operation of the Health Identifier including access has been comprehensively addressed through the legislation. We believe the Bill should proceed but wish to point out some identified issues that could also be addressed through regulations.

It is noted that adoption of the Health Identifier (Subclause 25) does not prescribe 'electronic' information and can therefore also be used as the identifier on paper based records. These do not necessarily afford the same level of privacy and audit that can be applied to electronic records. Any disclosure risk has to be weighed up against the increase in safety for correctly identifying the paper based record. While the Privacy Act 1988 is technology neutral, the Health Identifiers Bill makes specific reference to technologies, e.g. Public Key Infrastructure (Subclause 20(1)). The protections that such technologies provide do not extend to paper based records. This could be addressed by regulation that ensures the Health Identifier is not unnecessarily printed in full when there is a high risk of being read by third parties. An analogy is the common practice of only printing part of a credit card number on a receipt.

We welcome the inclusion of secondary usage for the purposes identified in Subclause 24. We would like it noted that the stated purposes do not directly include quality improvement activities under Subclause 24(1)(a)(ii) with the result that it may instead be classed as research under Subclause 24(1)(a)(iv). Experience overseas has shown that subjecting quality improvement to research approval increases the cost and delays of this important activity that does not attract research funding support. Quality improvement projects do not create new clinical risk for patients since their key goal is to implement evidence-based best standards of practice in the local environment. Without clear authorisation through the Bill, quality improvement activities which might be more efficient through use of the Health Identifiers may be forced to go through lengthy and costly Human Research Ethics Committee approval processes. The regulations could address this in the interpretation of monitoring and evaluation under Subclause 24(1)(a)(ii).

We favour the National Health and Hospitals Network for Australia's Future Report that states as a priority: "**e-health**, to take further steps towards the introduction of a personally controlled electronic health record for all Australians" (NHHN report section 6). To be 'personally' controlled need some controls and responsibilities over the recipient's Health Identifier, especially if we rely more in the future on

Personal Health Records as suggested by the recent recommendations of the National Health and Hospitals Reform Commission (NHHRC). In today's electronic information age, information pertinent to a person's personal, family or household affairs (Subclause 26 (2)(c)) is now increasingly distributed and stored globally. For example, Facebook, Microsoft Health Vault, Google Health, etc. where the data servers are not necessarily in Australia. Who will be held responsible if an international organisation, whose servers store health related information, makes unauthorised use or disclosure? **Regulation together with clear guidelines for both health providers and health recipients is critical to ensure these issues, that are not well understood presently, are clarified.** HISA and AHHA are content experts in this area and can assist in the development of these regulations.
