Lockstep Group
11 Minnesota Ave
Five Dock NSW 2046

Attention: Secretary, Community Affairs Committee
Department of the Senate
PO Box 6100
Parliament House
Canberra ACT 2600

Dear Secretary

Re: Healthcare Identifiers Bill 2010 (exposure draft)

Lockstep thanks the Senate Community Affairs Committee for the opportunity to make this submission on the *Healthcare Identifiers Bill 2010* (herein referred to as "the Act"). In accordance with the inquiry terms of reference, I address under separate headings below privacy safeguards in the Act, operation of the Healthcare Identifier Service including access to the Identifier, and the relationship to the national e-health agenda and electronic health records.

About Lockstep

Lockstep Consulting is a specialist consultancy dedicated to digital identity and privacy. We provide strategic analysis and advice to clients in the healthcare, government and financial services sectors, on electronic identity management, privacy, cyber security and governance. Sister company Lockstep Technologies researches and develops new solutions to prevent identity theft and enhance privacy online.

Recent Lockstep Consulting clients include the Joint Standing Committee on Health Informatics Standards, NEHTA, DHS (Victoria), DFAT, AGIMO and the Victorian Department of Justice. Lockstep founder and Managing Director Stephen Wilson served as an invited member of the Australian Law Reform Commission's Emerging Technology Subcommittee assisting the ALRC's review of privacy law. He is currently a member of Standards Australia IT Security Subcommittee IT-12-4, and the IT Testing Accreditation Advisory Committee of the National Association of Testing Authorities (NATA). Stephen gave testimony to the recent House of Representatives inquiry into cyber crime.

General remarks

In general, Lockstep supports the concept of health identifiers dedicated to improving the management and integrity of healthcare information. We submit that there is a richness in the

way Individual HIs will be used that has yet to be fully explored, and is not reflected in the draft Act. Because of short term technological constraints—in particular, the absence today of a universal way for individuals to securely carry and convey healthcare identifiers—the HI concept has concentrated on a *centralised* service model that discloses identifiers to users on a demand-basis. We will show below that a centralised IHI model poses inherent privacy risks.

There are alternative, more patient-centric architectures that could augment the IHI service and mitigate these privacy risks. Decentralised means for carrying IHIs in cards, smart phones and like devices can improve privacy (as well as performance) and therefore improve consumer acceptance.[1] As previous health & welfare IT programs have shown, serious attention to privacy is key to public acceptance.

We submit that the healthcare identifier system and legislation should anticipate the advent of personal security technologies for protecting IHIs. In legislating, government should seek to avoid enshrining a single centralised architecture for managing identifiers.

Privacy safeguards

The Act has been drafted around just the one use case for IHIs, namely where a healthcare provider obtains the IHI of a patient by providing identifying information about that patient to the service operator. If this is the main way in which patients and healthcare providers will make use of IHIs, then we contend that serious privacy risks may result.

Consider for example an initial consultation with a mental health professional. The patient may reasonably wish for this consultation to be confidential, but if the provider has to obtain the IHI from the service operator, then patient privacy will be compromised as a result. The fact that a named individual is consulting a mental health professional ought not to be disclosed as a by-product of the provider obtaining the IHI.

It should be noted that the sharing of patient information without express consent between healthcare professionals *even working in the same care team* has been determined by a state tribunal to be unreasonable (see *KJ versus Wentworth Area Health Service* [1]). That finding indicates that the greatest caution should be exercised as to inadvertent disclosures of a patient's clinical encounters. If it is not acceptable for mental health records of a patient to be disclosed without their consent to another doctor providing care to that patient, then it cannot be acceptable to disclose to the HI service operator the fact that an individual is seeing a mental health professional.

[1] Press reports in 2009 suggested that a new smart Medicare card could protect health identifiers (see e.g. "Medicare cards to become smarter", The Australian, 16 June 2009. Lockstep appreciates that these were false reports at the time, and yet they seemed to herald government concerns to better protect identifiers, and an improved public understanding of smartcard technology compared with previous projects. If a new Medicare smartcard did nothing other than simply convey reliable copies of IHIs, then it could be of great value to the HI system.

The IHI service as contemplated in the Act would intrinsically lead to information about patients' consultations with healthcare professionals being disclosed to the government. It would create an audit trail outside the clinical environment of every point where a provider accesses the IHI service, such as initial consultations, hospital admissions and emergency department admissions. As a consequence, participation in treatment by certain types of patients (e.g. those with mental health conditions, drug & alcohol dependency, or sexually transmitted diseases) could be jeopardised if their personal details are to be routinely disclosed to the HI service. Some patients in these categories will simply forego treatment rather than have their personal information escape the trusted local clinical environment.

We submit that options *must* be provided where a patient is able to disclose a reliable copy of their IHI directly to the healthcare professional, so as to minimise the extraneous disclosure of information about the clinical encounter.

Other privacy issues are associated with access controls, as discussed in the next section.

Operation of the Healthcare Identifier Service

Health Identifiers are held to be crucial to the future of health care delivery. As such, the HI service will constitute critical infrastructure. One would expect to see service level obligations commensurate with the importance of this service. Yet the Act sets out no service obligations for the service operator.

It is imperative that tight access rights and controls be codified in the Act or regulations, and implemented in the service. The following questions do not seem to be resolved, and may need to be reflected in the Act:

- Precisely what sort of healthcare providers are to be granted access to the IHI service? Will non-clinical personnel (e.g. hospital clerks) be granted access?
- How will purported providers accessing the IHI service be robustly authenticated?
- Should the legislation contemplate emergency access protocols for obtaining an IHI when a patient requiring immediate medical attention is unable to provide identifying information?
- What requirement is there for the healthcare recipient to grant consent to a provider to access that recipient's IHI?
- What auditing will there be of events where an IHI is obtained? Fine-grained auditability of all accesses to large government databases is a primary defence against abuse by wrongdoers who seek to track down individuals.
- What rights will patients have to know how their IHI has been accessed?

— Will the IHI system recognise any difference between access events when the recipient is involved and when they are not involved?

— Will there be any ability to present an IHI to the service for verification? If so, what access controls would then apply?

Relationship to the national e-health agenda

It is difficult to assess from the draft Act alone how the HI relates to the national e-health agenda. The draft makes no mention of electronic health records (EHRs) and gives no sign that it contemplates use of the IHI to index health records.

After obtaining an IHI from the service, there is no suggestion in the Act as to how a provider should subsequently use the IHI in the context of the national e-health priority programs, like e-prescriptions, e-referrals, decision support and chronic disease management. Yet if IHIs will be core to such systems, then further legislation and regulations will be needed in contemplation of, for example:

— verification of IHIs appearing in e-health transactions such as electronic prescriptions

— means by which a patient may access their own EHR.

Other specific comments on the draft Act

— s.3 *Purpose of this Act* should include mention of healthcare provider organisations (p2, lines 11-13).

— s.3 *Purpose of this Act*: the phrase "health information that is *created when healthcare is provided*" (emphasis added) seems overly restrictive. It is likely that IHIs will be used in relation to information created at other times too. We suggest deleting "that is created when healthcare is provided".

— s.5 *Definitions*: Why is the Medicare Provider number not cited at all as an instance of identifying information for providers, whereas the Medicare number is the very instance of identifying information for recipients?

— s.5 *Definitions*: "for a healthcare provider who is not an individual" should probably read "for a healthcare provider which is not an individual" (p4, line 34).

— s.11 *Disclosure to healthcare provider* describes disclosure to "an identified healthcare provider" (p10, line 8). What does identified healthcare provider mean? Are there no constraints on the type of healthcare provider that has access to IHIs? The same phrase also appears at p10 line 9 and p12 line 5, without further explanation.

— s.13 *Disclosure for authentication of healthcare provider's identity* concerns interfacing the HI service to PKI certification authorities for the issuance of keys and certificates to providers. This is an important function. But there is an inconsistency between paragraph (1) which refers to disclosing a "healthcare provider's information" and paragraph (2) which refers more specifically to disclosing the healthcare identifier.

— s.14 *Disclosure to get healthcare identifier* declares that s.14 applies if "it is necessary for the healthcare provider to disclose the healthcare recipient's identifying information for the purposes of the service operator disclosing the healthcare recipient's healthcare identifier to the healthcare provider". This passage is ambiguous. The 'necessity' mentioned could relate to the provider needing to get the IHI from the service operator, or it could relate to the provider needing to disclose identifying information as one means for obtaining the IHI. As noted above, the Act as drafted seems to presume that there is just one way to obtain an IHI, namely by disclosing patient identifying information to the service operator. This tacit assumption makes the word 'necessity' in s.14 somewhat confusing.

In conclusion, I trust that this submission is useful to your inquiry. Lockstep is eager to see progress made on important e-health infrastructure like health identifiers, and I would be pleased to make myself available to discuss any aspect of Lockstep's submission.

Yours sincerely,

Stephen Wilson
Managing Director.

References

[1]. *Case Note: KJ v Wentworth Area Health Service, NSWADT 84, Privacy NSW; 3 May 2004*
http://www.lawlink.nsw.gov.au/Lawlink/privacynsw/ll_pnsw.nsf/pages/PNSW_07_cnadt84