Submission No 9

INQUIRY INTO THE MANAGEMENT OF HEALTH CARE DELIVERY IN NSW

Organisation: Office of the Privacy Commissioner

Name: Ms Maria Fomicheva

Position: Investigation, Review and Statutory Advice Officer

Date Received: 28 April 2017

office of the privacy commissioner
new south wales

Mr Bruce Notley-Smith
Committee's Chair
Public Accounts Committee
Parliament House
Macquarie Street
SYDNEY NSW 2000

Our Reference: **IPC17/A000065**

By email: *Bjarne Nordin, Main Contact*
pac@parliament.nsw.gov.au

28 APR 2017

Dear Mr Notley-Smith

Submission to Inquiry into the Management of Health Care Delivery in NSW

Thank you for the opportunity to make a submission to the Committee's Inquiry into the Management of Health Care Delivery in NSW.

The NSW Privacy Commissioner has a responsibility for the protection of the privacy of NSW citizens' personal and health information. The relevant legislation establishing my position and statutory functions are the *Privacy and Personal Information Protection Act 1998* and the *Health Records and Information Privacy Act 2002*.

Privacy is an essential element of quality health care delivery. Because doctor-patient confidentiality is one of the key pillars of effective health service delivery, the protection of patient privacy is critical to the development of citizens' trust in health service provision of all levels. Internationally, health privacy is a priority being advanced by the UN Taskforce on health data privacy. In addition to my Office's continuing contributions to this Taskforce, NSW will have a direct input through Mr Chris Puplick AM, a member of the Taskforce.

My Office has been receiving an increasing number of health privacy complaints from the public concerned about improper handling of their personal health information. The recent breach of approximately 1,600 medical reports found in a Sydney bin raises serious concerns about the accountability of both public and private health service providers. The proposed solution of digitalising health records in Electronic Health Records systems, while providing benefits, will not solve the problem but rather present a new set of risks, not just to health privacy. The Terms of Reference of the Inquiry provide an opportunity to examine these concerns in further detail.

This submission is composed of the following parts:

1. Summary of recommendations according to the Terms of Reference of the Inquiry;
2. Legislative instruments applying to the privacy of health information in NSW;
3. The role of privacy in producing good health outcomes; and
4. Management of privacy risks.

[redacted]

Yours sincerely

[redacted]

Dr Elizabeth Coombs
A/NSW Privacy Commissioner

office of the privacy commissioner
new south wales

Public Accounts Committee

Inquiry into the Management of Health Care Delivery in NSW

Submission to Terms of Reference on efficiency and effectiveness of health care service delivery

April 2017

office of the privacy commissioner
new south wales

SUBMISSION TO THE INQUIRY INTO THE MANAGMENT OF HEALTH CARE DELIVERY IN NSW

Summary of recommendations according to the Terms of Reference of the Inquiry

Term of Reference	Recommendations
a) The current performance reporting framework for monitoring the effectiveness and efficiency of health care service delivery in NSW;	• The current performance reporting framework to include measures relating to privacy protection (both prevention and contravention).
b) The extent to which efficiency and effectiveness is sustained through rigorous data collection, monitoring and reporting;	• Where the efficiency and effectiveness of health service delivery is sustained through health data collection, individuals' consent be reinforced wherever possible. • To underpin Electronic Health Records systems: o the ability of the individual/patient to control information that identifies them and their health condition(s) be maximised; and o an 'opt-in' model be implemented with the requirement to obtain the express consent of an individual in accordance with Health Privacy Principle 15.
c) The adequacy of the provision of timely, accurate and transparent performance information to patients, clients, health providers and health system managers;	• Regular training be provided to all health staff to ensure they comply with the policies and procedures for the protection of privacy and health information. • Guidance materials be developed to educate patients on their rights under the privacy legislation, to support the provision of timely, accurate and transparent performance information.
d) The extent to which the current framework drives improvements in the health care delivery system and achieves broader health system objectives;	• Consultation occurs with the public on the Committee's recommendations to facilitate broader health system objectives. • Public confidence in health care delivery and Electronic Health Records systems by strengthened by the introduction of a mandatory data breach notification scheme. • The HRIP Act be amended to increase the accountability of employees and contractors who contravened health privacy law.

office of the privacy commissioner
new south wales

Legislative instruments applying to the privacy of health information in NSW

1. The *Health Records and Information Privacy Act 2002* (HRIP Act) is the governing NSW legislation on privacy protections of health information. The HRIP Act confers requirements on health information holders in both the public and private sectors. It contains 15 Health Privacy Principles (HPPs) that are legal obligations describing what organisations must do when they collect, store, use or disclose health information.

2. The HRIP Act was designed as a comprehensive piece of privacy legislation in NSW to cover all health information regardless of who holds or maintains it, and provide a strong, clear and transparent framework for privacy protections to support the proposed linked Electronic Health Records systems (EHRs).[1]

3. In the private health sector, the HRIP Act empowers the NSW Privacy Commissioner to receive and investigate complaints regarding alleged contraventions of the HPPs by health service providers, and, organisations that hold health information with a turnover of more than $3 million per year.[2]

4. In the private health sector the jurisdiction of the HRIP Act overlaps with the federal *Privacy Act 1998* (Cth). These two Acts offer different benefits to individuals pursuing complaints against private health service providers. For instance, certain matters included in the access provision for the private sector in the HRIP Act are not mirrored in Australian Privacy Principle 12 of the *Privacy Act*. These differences can result in different outcomes for the same conduct depending on the jurisdiction in which the matter arises. In regards to the private health sector, my Office received 103 complaints about private sector health service providers in 2015-16,[3] almost double the number reported in 2011-2012.[4] The majority of these complaints relate to individuals' requests to access their health records, or improper use or disclosure of their health information.

5. In the public health sector, the HRIP Act uses Part 5 of the PPIP Act, which contains the provision to enable an aggrieved person to make a privacy complaint regarding their personal or health information to a respondent public sector agency or public hospital. This is separate to the mechanism for dealing with private health sector complaints, as outlined in point 3 above, whereby the NSW Privacy Commissioner has powers to conduct investigations.

6. In addition to functions concerning compliance with the HPPs, the NSW Privacy Commissioner also has a statutory power under section 64 of the HRIP Act to issue guidelines. Statutory guidelines have been developed in relation to the non-consensual use of health information for research purposes,[5] and the non-consensual disclosure of a patient's genetic information by health service providers to a patient's genetic relatives.[6] These statutory guidelines are legally binding and ensure that health information is only used and disclosed for limited purposes and in particular circumstances.

---

1 Ministerial Advisory Committee on Privacy and Health Information Report to the NSW Minister for Health "Panacea or Placebo?", December 2000
2 *Health Records and Information Privacy Act 2002*, Part 6
3 Office of the Privacy Commissioner (NSW), *Annual Report 2015/2016*, p43
4 Information and Privacy Commission, *Annual Report 2011/2012*, p36
5 Section 64, *Health Records and Information Privacy Act 2002* Statutory Guidelines, published September 2016, available at http://ipc.nsw.gov.au/resources-public-sector-agencies
6 Available at http://www.ipc.nsw.gov.au/nsw-genetic-health-guidelines, published October 2014

The role of privacy in producing good health outcomes

7. Privacy is an enabler that, if well managed, can build trust in health service delivery. It facilitates individuals to be honest and open with their health care professionals, enabling better health outcomes.

8. As well as health information being inherently sensitive, many illnesses and conditions have some stigma attached to them. Improper handling of health information may lead to individuals suffering hurt and embarrassment, or being discriminated against, including but not limited to for insurance or employment purposes. For example, the AIDS Council of New South Wales (ACON), in their submission the Statutory Review of the *Public Health Act 2010,*[7] notes that HIV continues to be heavily stigmatised and that many people with HIV continue to experience discrimination based on their HIV status, both within the general community and within health care settings. As a consequence, without the assurance of privacy, individuals are reportedly deterred from disclosing important health information when seeking treatment, or, avoid seeking treatment all together.

9. The importance placed on the privacy of individuals' personal health information is also reflected in the strong emphasis in health service provision on doctor-patient confidentiality. The role of health service providers to act as trustworthy custodians of their patient's health information is imperative for an effective delivery of that patient's care. The privacy protections in health care provision must be sufficient for the general community to feel confident that their health information is well-protected. In this regard, the Office of the NSW Privacy Commissioner has contracted a survey of community perspectives on privacy, which includes specific questions on health privacy. Survey results will be available in May 2017 and might be of use and interest to the Committee.

10. The importance of health privacy is especially evident in cases of vulnerable members of society such as minors and Aboriginal people. For example, the research conducted by the Society for Adolescent Medicine in 2004, stated that for adolescent residents in NSW concerns about confidentiality is the most common barrier to accessing health care services.[8] There is also a pronounced difference in the reported level of privacy by Aboriginal patients compared to non-Aboriginal patients. In particular, Aboriginal patients report being given less privacy than non-Aboriginal patients when discussing their condition or treatment.[9] I note that ensuring that the health needs of Aboriginal people are considered in health care provision, is an objective of the NSW Health current performance reporting framework. The reported disparities, if they remain unaddressed, raise concerns about fairness and equal access to health service provision, and, detract from efficiency and effectiveness of health care delivery.

11. Public participation is a fundamental prerequisite to achieving broader health system objectives. I stress that to drive improvements in the health care delivery system, health service provision must be equally accessible, fair and considerate of all factors including a patient's culture, religious beliefs, sexual orientation or disability. Accordingly, privacy protections must be not regarded as concessions being made by health service providers but their legal responsibility to all patients. Under the NSW privacy legislation individuals have *legal rights* in respect of their own health information and health service providers have *legal obligations* in respect of that information.

---

7 ACON Submission to the Statutory Review of the *Public Health Act 2010*, June 2016

8 Booth, M. L., D. Bernard, S. Quine, M.S. Kang, T. Usherwood, G. Alperstein and D. L. Bennett (2004), Access to Health Care Among Australian Adolescents Young People's Perspective and Their Sociodemographic Distribution, *Journal of Adolescent Health,* **34**, 97-103

9 Bureau of Health Information, *Patient Perspectives – Hospital Care for Aboriginal People*, August 2016, p35

12. To ensure NSW is at the forefront of quality health care delivery, the Committee needs to consider alignment with international stances on the role of privacy in the provision of health care. The NSW privacy legislation is a derivative of international expectations. Health privacy has been identified as a thematic priority by Professor Joseph A. Cannataci, the UN Special Rapporteur on the Right to Privacy (SRP) and is the subject of a UN Privacy Taskforce. The SRP intends to prepare and present a report for the UN General Assembly in October 2018 titled "Improving safeguards and remedies for privacy and health data." My Office contributes to the UN Taskforce on health data privacy. National and regional developments in health privacy protection will be facilitated through NSW Taskforce membership.

It is **recommended** that:

1) Consultation occurs with the public on the Committee's recommendations to facilitate broader health system objectives as per Term of Reference (d);
2) Regular training be provided to all health staff to ensure they comply with the policies and procedures for the protection of privacy and health information; and
3) Guidance materials be developed to educate patients on their rights under the privacy legislation, to support the provision of timely, accurate and transparent performance information as per Term of Reference (c).

Management of privacy risks

13. Data breaches threaten public confidence in health service provision and the risk of health data breaches is real and growing. Aggregated public health data can help achieve efficiency and effectiveness in health care delivery, particularly where this data is stripped of personal identifiers to protect individual privacy and ensure accurate and full information provision by patients.

14. In a recent case, more than 700 public patients have had their privacy breached after more than 1600 medical letters were found disposed of in Sydney bin by a sub-contractor for a company tasked with transcribing medical letters sent from specialists to general practitioners.[10] It has been suggested that digitalising health records in EHRs will prevent such breaches from occurring in the future. However, the benefits of EHRs come with an increased risk of greater access and possible disclosure on an even larger scale, thereby elevating the risk to individuals and reputational damage for organisations.

15. Storage in EHRs brings together, in one place, large quantities of personal health information about individuals. This makes the information easily accessible to health care professionals for the purposes of patient care, but also potentially, for unauthorised and unlawful purposes in the absence of appropriate safeguards. The risks to individuals, whose health information can be used without their consent, are increased as a result. For example, there is growing interest from a range of quarters in monetising health data by data custodians. It is not appropriate for individual health data to be monetised.

[10] NSW Health press release http://www.health.nsw.gov.au/news/Pages/20170421_00.aspx (accessed 24/04/17)

16. One way to address these risks, as My Office has consistently advocated, is to adopt a client-centric approach to EHRs, whereby individuals have control over the use of their health information, as the best approach to dealing with individuals and their health information. This includes the requirement that EHRs operate on an 'opt-in' basis, with the requirement to obtain the express consent of an individual in accordance with HPP 15 before their health information is included in an EHR. This view has also been supported by community attitudes, with the Office of the Australian Commissioner reporting that in 2013 a substantial proportion of Australians (one in three) considered the transfers of their health information between health service providers inappropriate without their consent.[11]

17. As outlined in my Special Report to Parliament *NSW Informational Privacy Rights: Legislative Scope and Interpretation Employer, Employee and Agent Responsibilities*, other recent examples of data breaches included:[12]

    - Employees of public and private health service providers improperly collecting, accessing and disclosing the health information of patients for their own purposes. E.g. the case of "Witness A";[13]
    - Researchers obtaining medical records, including identity details, from health service providers without patient consent and then sending spam to the subject person;
    - Poor software design that leads to large scale data leaks;[14]
    - The use of personal information for in-house human research or releasing it to external researchers without a privacy impact assessment, ethics approval or a compliance check against privacy legislation; and
    - Information transfers to organisations without due diligence checks on the adequacy of data security measures to protect data from insider abuse and external attacks.

18. Effective health care delivery cannot exist without intrinsic regard to privacy. Great care should be taken to incorporate privacy by design into the EHRs, with a focus on data security and data minimisation, providing for regular audits to ensure that these qualities are maintained. This approach is premised on the view that privacy and security are embedded directly into EHRs, and, where personal health information is aggregated for secondary uses such as research, it is robustly de-identified.

19. I draw the Committee's attention to a recent case where academics found it was possible to re-identify personal information in the Medicare Benefits Schedule and Pharmaceutical Benefits Schedule datasets published online.[15] Robust de-identification should involve testing the datasets for these types of risks. In particular, I acknowledge the greater utility of the Centre for Health Record Linkage (CHeReL) to perform linkages of health-related data in accordance with privacy requirements and to provide researchers with de-identified datasets.
20. The current state of technological advances is capable of enabling specifications that allow interoperability among healthcare-related information made by different providers, without detracting from privacy protections of individuals' personal health information.

---

[11] Office of the Australian Information Commissioner, *Community Attitudes to Privacy Survey, Research Report* , 2013, p31

[12] Office of the Privacy Commissioner (NSW), Special Report under Section 61C Privacy and Personal Information Protection Act 1998, *NSW Informational Privacy Rights: Legislative Scope and Interpretation – Employer, Employee, and Agent Responsibilities*, February 2017, pp9-10

[13] While Witness A was under anaesthesia in a private hospital for a routine gynaecological procedure, a nurse took a photograph of Witness A's genitals using her iPhone for non-work related purposes. A fuller description of this case is available at: NSW Parliament, Standing Committee on Law and Justice (March 2016) Report - *Remedies for the serious invasion of privacy in New South Wales*, Sydney, 20-21

[14] See, for example, the Australian Red Cross Blood Service data breach http://www.donateblood.com.au/media/news/blood-service-apologises-donor-data-leak (accessed 12/04/2017)

[13] Australian Medical Association press release https://ama.com.au/ausmed/medicare-data-breach-prompts- law-change-0 (accessed 18/04/2017)

21. While efficiency and effectiveness of health care delivery is assisted by rigorous data collection, the collection, retention and use of health data must be in line with the privacy standards, such as the *NSW Government Digital Information Security Policy* applicable to all NSW Public Service Agencies. This Policy specifically discusses the requirement for digital information and digital information systems to be in accordance with the obligations imposed by the NSW privacy legislation.[16]

22. I also make reference to the need for internal controls, governance, data security and privacy emphasised by the NSW Auditor-General's *Report on Finance, Services and Innovation (including Insurance) Volume Five 2016*.[17] These data governance mechanisms should be a priority in any computerised system that enables multiple users to access large volumes of personal and health information of an organisation's clients.

23. In particular, I would encourage NSW Health to adopt privacy as a key objective in its performance framework, to deliver effective eHealth-enabled healthcare services across NSW. In line with the *eHealth Strategy for NSW Health 2016-2016*,[18] a trusted digital environment for storage of medical records is required, to ensure security, privacy and legislative controls are built into all eHealth programs.

24. Maintaining the privacy of health information is critical for an effective health service delivery. Dealings with the health information of individuals should be subject to a robust privacy regime. An information ethics and governance framework must have a central place in every health agency's culture in order to deal with information in ways that help health service providers maintain the trust of the community.

25. By recognising privacy as an enabler of quality health care, NSW has an opportunity to showcase leadership aligned with international best practice in building privacy by design approaches that can achieve concurrent goals of increased efficiency and effectiveness in health care provision, and a framework which facilitates broader societal and individual health care benefits.

It is **recommended** that:

1) In accordance with the Term of Reference (b), where the efficiency and effectiveness of health service delivery is sustained through health data collection, individuals' consent be reinforced wherever possible;

2) To underpin EHR systems:

   i. the ability of the individual/patient to control information that identifies them and their health condition(s) be maximised; and

   ii. an 'opt-in' model be implemented with the requirement to obtain the express consent of an individual in accordance with HPP 15.

[16] *NSW Government Digital Information Security Policy*, April 2015, p5
[17] NSW Auditor-General, *Report on Finance, Services and Innovation (including Insurance)* Volume Five 2016, p27
[18] *eHealth Strategy for NSW Health 2016-2026*, launched on 3 May 2016, p13

3) To drive improvements in the health care delivery system as per Term of Reference (d):
    i. public confidence in health care delivery and EHR systems by strengthened by the introduction of a mandatory data breach notification scheme; and
    ii. the HRIP Act be amended to increase the accountability of employees and contractors who contravened health privacy law.

4) In accordance with the Term of Reference (a), the current performance reporting framework to include measures relating to privacy protection (both prevention and contravention).