Health
Northern Sydney
Local Health District

Our ref: NSHN/21/47295

Privacy and Personal Information Protection Amendment Bill 2021 Reforms
Policy, Reform and Legislation
NSW Department of Communities and Justice

Email: policy@justice.nsw.gov.au

Dear Sir/Madam,

Submission on proposed changes to NSW privacy laws

Northern Sydney Local Health District (NSLHD) appreciates the opportunity to provide a submission to the proposed *Privacy and Personal Information Protection Amendment Bill 2021* (PPIP Amendment) prepared by the Department of Communities and Justice (the DCJ).

Our general observations of the issues raised by the proposed changes are outlined below.

Submission One - Significant burden placed on Health Services due to the inherent sensitivity of Health Information, the high level of access to information required to support patient care and insufficient timeframes for appropriate assessment and notification of eligible breaches

Health operates in a unique context in regards to access, disclosure and security. NSW public health providers are bound by the *Health Records and Information Privacy Act 2002* (NSW)(HRIPA).

The primary aim of the PPIP Amendment is to require public sector agencies such as local councils, universities and statutory authorities bound by the *Privacy and Personal Information Protection Act 1998* to notify the Privacy Commissioner and affected individuals of data breaches of personal or health information likely to result in serious harm.

The 'one size fits all' approach with the proposed changes is incompatible with public health organisations. Operationally, there is difficulty in auditing access and in determining what qualifies as unauthorised access.

NSW Health have recently rolled out the use of P2 Sentinel which is a tool to audit access to eMR. The tool highlights usage that *may* `be inappropriate but requires investigation on a case by case basis to determine whether a breach has occurred.

Extending the Mandatory Notification of Data Breach (MNDB) scheme to include NSW public health service providers such as NSLHD would result in a significant regulatory burden on our health services who would need to dedicate resources to investigation of potential breaches and notification to both the regulatory body and patients/carers.

All correspondence to be emailed or sent to:
NSLHD-Mail@health.nsw.gov.au

PO Box 4007
Royal North Shore Hospital LPO
St Leonards NSW 2065
Tel (02) 9462 9955 Fax (02) 9463 1029

Northern Sydney Local Health District
ABN 63 834 171 987

The Commonwealth OAIC Notifiable Data Breaches Report July to December 2020[1] reports that the health sector remains the highest reporting industry sector, with a significant number of notifications from human error. We propose that the definition of an 'eligible data breach' be further reduced in scope to at the least exclude human error and also potentially to include a requirement for malice or intent.

Chart 17 – Source of data breaches – Top 5 industry sectors

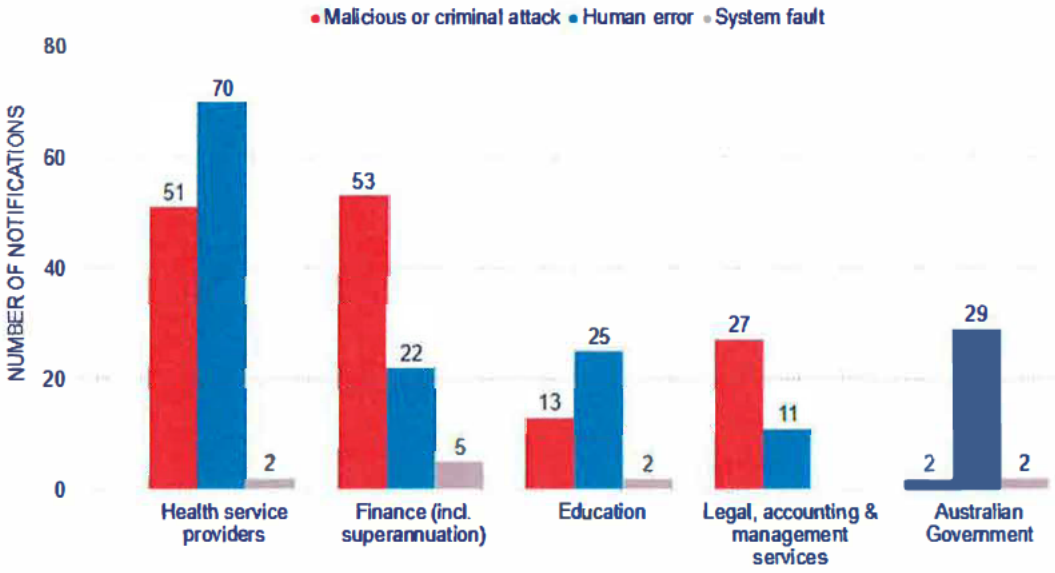

Chart 17: Long text description

Source: The Commonwealth OAIC Notifiable Data Breaches Report July to December 2020

We further propose that an extension to the 30 day period for assessment is required for health services to appropriately assess the nature and extent of the breach and the circumstances of the individuals affected.

Submission Two - Serious harm factors (s59G (g)) to be included in the legislation

Clarity is needed to assist in determining the risk of serious harm and thresholds to apply when dealing with health information. The threshold 'likely to result in serious harm' is subjective and difficult to assess in the context of healthcare, with most breaches that result in a disclosure outside of the health service likely to meet the threshold of potentially causing serious harm to an individual. There is limited guidance around what 'serious harm' may entail for the individual's whose information was unlawfully accessed/disclosed. The Amendment Bill Factsheet states that the *'legislation will prescribe a number of factors to consider when assessing whether an eligible breach is likely to cause significant harm'* however NSLHD does not consider these factors to be clearly articulated in the proposed legislation. It would be preferable for the Privacy Commissioner Guidelines setting out the serious harm factors (s59G (g)) to be included in the legislation for the abundance of clarity.

If the PPIP Amendment is adopted, there should at least be an effective definition of 'serious harm' with examples, guidance and a list of factors that health service providers must consider when assessing whether a privacy breach is likely to cause 'serious harm'. A set of assessable factors or a checklist would be a valuable resource for considering if serious harm could be caused by a data breach.

[1] https://www.oaic.gov.au/assets/privacy/notifiable-data-breaches-scheme/statistics/Notifiable-Data-Breaches-Report-July-Dec-2020.pdf

Guidance issued by the Office of the Australian Information Commissioner provides that, in the context of a data breach, serious harm to an individual may include serious physical, psychological, emotional, financial or reputational harm. The serious harm threshold requires an objective assessment determined from the viewpoint of a reasonable person in the entity's position. The reasonable person is properly informed and assesses based on the information immediately available or following reasonable enquiries. It is not from the position of an individual whose personal or sensitive information was part of the data breach.

In the context of healthcare the unauthorized access or disclosure of an individual's health conditions, diagnoses, treatment and/or related health information may have varying personal consequences in regards to potential harm. It may impact on that individual's ongoing treatment compliance, cause reluctance to divulge important health information in the future to healthcare professionals and could adversely impact on their health and wellbeing. This is of particular concern when dealing with mental health, victims of abuse, child protection and other highly sensitive records with both health and legal implications for the rights of the person/s involved.

We believe that an objective assessment is required with consideration of the individual circumstances of the patient, their health conditions and the nature of the breach in order to determine the possibility of serious harm. This may require clinical review of the patient's current health, ongoing health conditions/treatment requirements and individual circumstances. It may also require investigation into the extent of the breach and the number of individuals involved.

We propose that two alternative thresholds could be considered:

1. 'Serious breach' rather than 'serious harm.' This definition could capture both subjective and objective elements. A serious breach should not include inadvertent or accidental internal disclosures and include an element of malice or intent.

2. The European Union General Data Protection Regulation (GDPR) requires individuals to be notified of a data breach where there is a 'high risk to the rights and freedom of natural persons.'[2] This is a desirable standard to apply in health. Both the likelihood and severity of the potential impact is assessed. Sensitive data such as health information is more likely to be high risk and result in a potential risk to rights and freedoms.

Submission Three - What constitutes a breach should be defined into categories

The European Data Protection Board (EDPB), which is made up of the data protection regulators from across the EU, issued guidance on data breaches[3]. It categorised breaches into three types and a breach can comprise one or a combination of all three:

- confidentiality breach – where there is an unauthorised or accidental disclosure of, or access to, personal data. An example of this would be emailing personal data to the wrong recipient(s)
- integrity breach – where there is an unauthorised or accidental alteration of personal data. An example of this could be amending the medical records of the wrong patient
- availability breach – where there is an accidental or unauthorised loss of access to, or destruction of, personal data. An example of an availability breach would be an incorrectly administered data retention policy where the incorrect data sets were accidentally permanently deleted or destroyed

The above categories would assist the LHD to assess the ongoing impact to the patient, their treatment and potential level of harm caused by the breach.

Submission Four - Consideration of contractors and third party providers

NSW health service providers such as NSLHD engage in agreements with third party providers who handle personal information. An example of this is NSW Ambulance, private hospitals (e.g. Northern Beaches Hospital, the Sydney Adventist Hospital), NSW Pathology, the University of Sydney, Breastscreen NSW, Imaging providers etc. These third party providers use different platforms for handling personal information of patients, as well as, under various governing

---

[2] European Union GDPR 2016/679, Art 3.4

[3] https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf

arrangements, access NSLHD platforms. There are also a variety of information exchange platforms such as HealtheNet where patient health information is regularly accessed across the State by a variety of clinicians who are employed by NSW Health.

The responsibility for the management and notification of data breaches with third party providers and across shared information exchange platforms is unclear in the proposed legislation and may be difficult. Currently there are limited tools or infrastructure to facilitate notification of a possible data breach and carry out an assessment of the impact of any breach. The responsibility of who would audit, notify and investigate these breaches and perform the required assessment of serious harm across multiple Local Health Districts, private hospitals, patients and clinical teams would need to be further considered and appropriately resourced.

Interagency breach could have severe consequences, for example, in relation to the compromise of identity information in sexual assault matters where a number of agencies have access to the same information – for example, Police, FACs and Health. The legislation should clarify that the assessment obligations rest with the Agency where the alleged eligible data breach occurred. Thank you for the opportunity to comment on the proposed changes to NSW privacy laws.

Yours sincerely