Private Healthcare Australia

Better Cover. Better Access. Better Care.

Data Retention Review – PHA Submission

March 2025

Contact:

Ben Harris – Director Policy and Research

0418 110 863

ben.harris@pha.org.au

About Private Healthcare Australia

Private Healthcare Australia (PHA) is the Australian private health insurance industry's peak representative body. We have more than 20 registered health funds throughout Australia as members and collectively represent 98% of people covered by private health insurance. PHA member funds provide healthcare benefits for over 15 million Australians.

Introduction

PHA welcomes the opportunity to provide feedback to the Department of Home Affairs and Attorney-General's Department's review of Commonwealth data retention provisions. Data retention is an important issue for our sector given the large volume of members' information health insurers hold. PHA's member funds have allocated considerable funding and resources in recent years towards strengthening cyber security measures to better protect members' information from future threats. But health funds face ongoing challenges trying to meet overlapping legislative and regulatory obligations in relation to data retention and many other areas of business. Most health funds are national organisations, therefore, must comply with legislation created by nine different Parliaments as well as a range of other obligations imposed by state and territory regulators, which can be onerous.

Response

Conflicting data retention requirements in different legislation

Under the *Privacy Act 1988 (Cth)* (the Privacy Act), entities including private health insurers are obliged to take reasonable measures to permanently destroy or deidentify personal information of former members after seven years as it is no longer considered needed for any purpose permitted by the Privacy Act. The Privacy Act allows insurers to retain personal information where it is required by law.

But these obligations are at odds with health insurers' obligations under *the Private Health Insurance Act 2007 (Cth*) (PHI Act) and the Private Health Insurance (Lifetime Health Cover) Rules (LHC Rules) regarding Lifetime Health Cover (LHC) loading. The PHI Act states that insurers need to keep the information required for calculating the LHC loading throughout the lifetime of a person.

This raises a potential conflict between:

- insurers destroying former members' personal information which it no longer 'needs' (e.g. because any applicable mandatory record retention periods under the Corporations Act or State and Territory health records legislation (Retention Period) have passed); and,
- insurers keeping former members' records to assist those who have left private health insurance, do not have a transfer certificate and wish to return to private health insurance, to substantiate their LHC calculations.

There are serious financial consequences of up to $30,000 per individual and $60,000 for couples who, after leaving private health insurance, wish to later return and are unable to demonstrate, for the purposes of LHC, days of hospital cover held since July 2000 from the year they turned 31.

PHA recommend to the Department of Health and Aged Care in 2024 that consumers' LHC loading information should be stored on members' MyGov accounts. This would help Australians avoid unnecessary LHC penalties and enable people to re-enter health insurance when they wanted. It would also remove the requirement on health insurers to retain and store records for the duration of members' lifetime and reduce the risk of information being targeted by data breaches.

Inconsistencies between data retention obligations in different states and territories

Data retention legislation also differs between Australian states and territories, making it incredibly hard for health funds – especially those that operate nationally and/or those whose records are stored in the same location – to comply.

Health records legislation in Victora, New South Wales and the Australian Capital Territory, for example, requires any health service provider, or 'record keeper' under ACT legislation, to retain health information in the case of:

- an adult, for a period of seven years after the last occasion on which the provider/record holder provided a service to the individual; or
- a person under 18 years of age, until that person turns 25 years of age.

Particularly in the ACT, these retention periods may be burdensome in the context of private health insurance providers due to the definition of 'health record', which includes any record containing personal health information. Any document containing information about a health service claim may include health information and will, therefore, be subject to the minimum retention periods. But this requirement is limited to 'health service providers' under Victorian and NSW legislation. As health insurers only pay for rather than provide health services, the data retention provisions do not apply in those jurisdictions. However, for organisations with a national footprint, often with centralised data storage infrastructure or uniform data retention policies, it can be difficult to manage varying obligations with regards to health information retention and/or deletion.

Inconsistencies in data deletion obligations in different states and territories

Health records deletion obligations also differ between Australian states and territories. In Victoria and NSW, for instance, the health service provider, or record keeper in ACT, is also required to create a separate record whenever health information is deleted or disposed of. That record must include the name of the individual the health information relates to, the period covered by the health information, and the date on which the information was deleted or disposed of. In the ACT, such a record is required to be kept for a minimum of seven years. However, in Victoria and NSW, there is no minimum retention period enshrined in the

legislation, leading to some confusion about whether that means such a record must be kept indefinitely.

Further, given the broad definition of health information and health records in all jurisdictions, the requirement to create a deletion record will generally apply to any record created by a health service provider or record holder, which contains health information, even if that record is not a primary health record. For example, this could mean everything down to a recording of a phone conversation that contains health information could arguably be covered.

Suggestions for the review to consider:

The Data Retention Review should consider:

- the policy basis for retention periods generally, or as they relate to non-health service providers
- whether uniform requirements across all jurisdictions should be implemented
- whether standard periods in all government legislation, which should be agreed with state and territory governments, should apply to data retention, such as short (three years), medium (six years), medium-long (12 years) and long (30 years)
- the policy basis for the obligation to create a deletion record, the scope of the obligation and the time periods for which deletion records must be held, and
- creating some sort of reasonableness or due diligence test on non-compliance with a data retention obligation where the entity has destroyed records in accordance with a reasonable data destruction policy.