Data breach process

The data in the Medicare Mental Health Intake System is very sensitive. NWMPHN is obligated to identify areas of risk and implement controls that mitigate the risk of data breaches. You are obligated to be vigilant in protecting the data and report possible breaches. A data breach occurs when personal information that an entity holds is subject to unauthorised access or disclosure or is lost.

You must be aware of how data is stored and shared, particularly when doing something outside the normal process. You should avoid sending data insecurely, such as screenshots containing names in an email. It is safe to email the URL of a client or referral, as the URL cannot be used by an external party to identify a person.

Your organisation's data breach policy will guide you on what you should do in the event of a potential breach. If you or your manager believe that a data breach may have occurred you must also notify the NWMPHN Medicare Mental Health Support team by sending an email **marked urgent** to pmhcis.support@nwmphn.org.au. The NWMPHN team will follow their Data Breach Response Plan for investigating potential breaches and taking remedial action, if required to do so. The NWMPHN's Plan's high level steps are:

1. Identify, Contain, Collect. Identify the breach, contain it, and collect information.
2. Evaluate the risks for associated with the breach and conduct preliminary assessment.
3. Notification.

May 13, 2025 16:52:38