Privacy Policy

Purpose

1. MHCC collects information from individuals and organisations for various purposes, including: member registration; event attendance; information dissemination; and for research purposes.

2. This policy sets out how MHCC will manage this information so that the organisation is compliant with the Australian Privacy Principles as set out in the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*.

3. This policy also includes a Data Breach Response Plan (attached) setting out how the MHCC will respond to a data breach or suspected data breach.

Scope

4. This policy:

    - covers the collection and management of information pertaining to individuals and member organisations and how this information is stored by MHCC
    - applies to MHCC Personnel (Board Directors, employees, contractors and members)
    - does not apply to students in the Learning and Development Unit. MHCC Learning and Development should refer to the Training Privacy and Confidentiality Policy for Students.

Policy Statement

5. MHCC Personnel and stakeholders have a right to confidentiality of personal and professional information.

6. Professional and ethical practice requires that there is no unnecessary sharing of private and confidential information. Except as outlined in this policy, MHCC will not share or disclose, any information collected to another person, organisation or agency unless consent is provided by the information owner, or when MHCC is required by law to disclose.

7. When **personal information** is disclosed, MHCC Personnel must be respectful of the individual's right to privacy and confidentiality and limit disclosure to only that which is necessary and admissible under Australian Privacy laws (refer to Related Legislation section of this policy).

8. MHCC will take all reasonable steps to ensure we comply with and store all information in line with the Australian Privacy Principles as outlined in the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*.

9. MHCC will report any **notifiable data breaches** as outlined in the *Privacy Amendment (Notifiable Data Breaches) Act 2017.*

10. MHCC will maintain robust privacy and data governance procedures and appoint a senior member of the management team to be responsible for privacy.

Procedures - Compliance with Australian Privacy Principles (APP)

11. MHCC Personnel (Board, employees, contractors and members) must take all reasonable steps to ensure compliance with the Australian Privacy Principles (APP).

12. MHCC CEO and Managers must inform any new Board Directors, employees or members of their obligations to maintain privacy and confidentiality.

13. All new MHCC Personnel must sign the relevant confidentiality agreement on commencement with MHCC.

Open and transparent management of personal information (APP 1)

14. MHCC Personnel must advise persons, from whom personal information is sought, as to:

    - why the information is being collected
    - how it will be collected
    - how it will be stored
    - how it will be used.

15. MHCC Personnel must not share personal information with any other person or organisation without the explicit permission of the individual, or as required or authorised by legislation.

16. In regard to member organisations, MHCC must only share publicly available generic information, such as their main phone number, email and address.

Anonymity & pseudonymity (APP 2)

17. When providing information or making an enquiry to MHCC, individuals have the right to remain anonymous or use a pseudonym.

18. To enable statistical analysis of views on the MHCC website, MHCC staff must only collect low level non-identifying metadata, such as IP addresses.

Collection of solicited personal information (APP3)

19. MHCC collects personal information through:

    - Registration to events
    - registering for MHCC communications such as our e-newsletter
    - membership application and renewal processes.

20. Information provided during the membership application or renewal process may include individual information as well as **organisational information**. Any individual information provided on behalf of an organisation must be used solely for the purpose of disseminating member relevant information to the member organisation.

21. Information relating to individuals (including internal and external staff/consultants) and organisations must be stored within the MHCC Customer Relationship Management (CRM) System. The CRM must be password protected and access restricted to only those MHCC employees who require the information to perform their roles.

22. Except where information is collected for the purposes of specific projects and research, personal information about an individual may include (but not limited to):

    - name (first and last)
    - contact details (address, phone numbers, email address)
    - organisation of employment
    - job Title.

23. Information collected about an organisation may include (but not limited to):

    - organisation's name
    - organisation's parent company and ABN
    - primary account contact details (will be entered as an individual)
    - organisational contact details (phone, address, email, website)
    - organisational service areas.

24. Where information is provided by an individual for payment of a service, such as credit card details, this information must **not** be stored once the payment has been processed.

Dealing with unsolicited personal information (APP4)

25. In the event that MHCC receives unsolicited personal information about any individual, and it is unlikely that MHCC should have been provided with this information, then MHCC Personnel must delete or destroy the information immediately and advise the sender accordingly.

Notification of the collection of personal information (APP5)

26. In the event MHCC receives unsolicited information about an individual and the information is relevant, and it is likely MHCC could have collected it from the individual through our processes, MHCC will inform the individual, including how MHCC intends to use the information and seek the individual's permission to retain the information.

Use or disclosure of personal information (APP6)

27. Information must not be provided to third parties for the storage of and dissemination of contact details unless the individual has consented to the sharing of their information, or it is required or authorised by legislation.

28. Information collected by MHCC may be used to inform:

    - members and other stakeholders of upcoming events (including possible training and/or events)
    - members of information considered relevant to them
    - the broader mental health sector of information we consider to be relevant to them.

29. Personal information must not be used for other purposes unless:

    - the individual has consented
    - it is somehow required or authorised under legislation
    - it is required to locate a missing person
    - it is required for the purpose of a confidential alternative dispute resolution
    - it is requested by an authority to gather evidence of processes when undertaking an audit.

30. Where information is used for the above purposes and the individual has not consented the relevant line manager and CEO must be informed as soon as practicable.

Direct marketing (APP7)

31. MHCC must only use personal information collected from an individual for the purpose of direct marketing where the individual has expressly indicated their approval to do so.

32. All direct marketing will provide a simple way of unsubscribing or altering subscription preferences to any future direct marketing campaigns or emails.

Cross-border disclosure of personal information (APP8)

33. MHCC information is stored within Australia. In the event that the location of information storage changes in the future, MHCC must seek assurances that the storage company complies with Australian Privacy laws in its handling of information and has effective cybersecurity controls in place to protect the data.

Adoption, use or disclosure of government related identifiers (APP9)

34. MHCC must not use other **government related identifiers**. MHCC Personnel must not disclose a government identifier should they become aware of it unless:

    - permission has been given to disclose it
    - it is necessary for MHCC to carry out its activities or obligations
    - it is required or authorised by or under Australian law.

Quality of personal information (APP10)

35. MHCC must take reasonable steps to ensure information collected and stored by MHCC about an individual or organisation is accurate, up-to date and complete.

Security of personal information (APP11)

36. MHCC must take proactive steps to protect personal information, including:

    - undertaking regular reviews of its technical and organisational measures for protecting personal information
    - ensuring employees have access to regular training on privacy and cyber risks.

37. Information stored within the MHCC records management systems must only be available to select internal MHCC employees. Employees must only use information stored within these systems that is relevant to their specific role or assigned tasks for MHCC operations.

38. In accordance with MHCC Records Management Policy, MHCC must periodically review the retention periods for the holding of personal information.

39. Where personal information is no longer required (or requested by the individual) MHCC must destroy, delete or de-identify the information in accordance with relevant legislation and the MHCC Records Management Policy.

40. All hard copy forms that contain personal information must be stored securely until such time as they are no longer required. Hard copy forms no longer required must be securely disposed of by use of a secure bin provided on MHCC premises.

41. Soft copy forms that contain personal information must be stored securely in selected cloud-based folders. Access must be restricted to MHCC staff who require the information to perform their roles.

42. Staff are responsible for ensuring soft copy **confidential information** is electronically deleted from the MHCC cloud-based record management systems, in accordance with the Records Management Policy.

43. Where confidential information is in the form of an email or email attachment this must be deleted once stored securely and no longer needed in email format.

44. All third-party service providers used for storing and transmitting data must agree to maintain the privacy of MHCC data.

Access to personal information (APP12)

45. Access to information stored within the MHCC record management systems must only be provided to the individual the information relates to, unless the information relates to an organisation, in which case access the information will only be provided to the nominated contacts for that organisation within the relevant MHCC records management system.

46. Requests for access to information must be made in writing to MHCC and will be responded to within a reasonable timeframe, and where possible within the format requested. Consent must be obtained from the information owner before their information is shared.

47. MHCC may reasonably refuse to provide an individual access to the information stored where:

    - it would pose a serious threat to life, health, or safety of any individual, or to public health or public safety
    - giving access would have an unreasonable impact on the privacy of other individuals
    - the request for access is frivolous or vexatious
    - the information relates to existing or anticipated legal proceedings between MHCC and the individual, and would not be accessible by the process of discovery in those proceedings
    - giving access would reveal the intentions of MHCC in relation to negotiations with the individual in such a way as to prejudice those negotiations
    - giving access would be in breach of the privacy laws
    - MHCC has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to MHCC's functions or activities has been, is being, or may be engaged in. Giving access would be likely to prejudice the taking of appropriate action in relation to the matter
    - giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body

- giving access would reveal evaluative information generated within MHCC in connection with a commercially sensitive decision-making process.

48. Where an employee receives a request for information, they believe is private or confidential they should refer the matter to the relevant line manager.

49. In the event MHCC is unable to provide access to information, MHCC must provide the reason access has not been granted and provide information on how to make a complaint about access not being granted.

50. In some instances, MHCC may have a legal obligation to release this information.

Correction of personal information (APP13)

51. MHCC must work to ensure information maintained within their record management systems remain accurate, current and complete. However, in the event that MHCC is notified of inaccurate information, the requested changes must be made within two (2) working days of receiving written notification from the relevant person.

52. Where MHCC is unable to make the requested changes, MHCC must provide the reason the request will not be actioned and information on how to make a complaint.

Complaints

53. Complaints about breaches of privacy can be made directly to MHCC. MHCC can be contacted at the below details:

MHCC
PO Box 668
Rozelle NSW 2039
02 9060 9627
info@mhcc.org.au
http://www.mhcc.org.au

54. Alternatively, complaints about breaches or privacy can also be made to:

Office of the Australian Information Commissioner
GPO Box 5218
Sydney NSW 2001
1300 363 992
enquires@oaic.gov.au
http://www.oaic.gov.au

Notifiable Data Breaches

55. A data breach occurs when personal information an organisation or agency holds is lost or subjected to unauthorised access or disclosure. For example, when:

- a device with a customer's personal information is lost or stolen

- a database with personal information is hacked
- personal information is mistakenly given to the wrong person.

56. MHCC must notify individuals and the Australian Information Commissioner of any '**eligible data breach**'. An "eligible data breach" arises when:

    - there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an organisation or agency holds
    - a data breach is likely to result in serious harm to one or more individuals
    - the organisation has not been able to prevent the risk of serious harm with remedial action.

57. Whether a data breach is likely to result in serious harm requires an objective assessment, determined from the viewpoint of a reasonable person in the entity's position.

58. Not all data breaches are eligible. For example, if an entity acts quickly to remediate a data breach, and as a result of this action the data breach is not likely to result in serious harm, there is no requirement to notify any individuals or the Australian Information Commissioner.

59. In the event that an employee is notified or becomes aware of a data breach or suspected data breach, MHCC has 30 days to make a determination about whether an eligible data breach has occurred and for any such breach to be reported and responsive action taken. The Data Breach Response Plan must be followed to assist in making the determination and any actions to be undertaken.

Roles and responsibilities

60. The CEO has responsibility for:

    - oversight of this policy and its implementation
    - ensuring staff are aware of their obligations under this policy and undertake any necessary training
    - reporting all eligible privacy breaches to the Australian Information Commissioner
    - establishing and oversighting any data breach response team
    - ensuring the Board and other relevant stakeholders are informed of data breaches, as relevant.

61. Line managers are responsible for ensuring their staff are aware of this policy and establishing processes within their teams to ensure compliance with this policy.

62. All MHCC Personnel are responsible for complying with this policy.

Related Policies and Procedures

63. Related policies and procedures:

- Board Charter
- Code of Conduct
- Conflict of Interest Policy
- External Complaints Policy
- Records Management Policy

Related legislation

64. Relevant legislation:

- Privacy Act 1998 (Cth)
- Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth)
- Privacy Amendment (Notifiable Data Breach) Act 2017 (Cth)
- Privacy and Other Legislation Amendment Act 2024 (Cth)
- Corporations Act 2001
- Work Health & Safety Act 2011 (Cth).

Definitions

Confidential information	Confidential information may be organisational or personal in nature and extends to: member records and related documents, conversations, staff personnel files, job applications, financial and payroll records, staff and members' addresses and telephone numbers, draft policy and submissions, Funding and Performance Agreements.
Eligible data breach & Notifiable data breach	" arises when: there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an organisation or agency holds; a data breach is likely to result in serious harm to one or more individuals; the organisation has not been able to prevent the risk of serious harm with remedial action.
Government related identifiers	A number, letter or symbol, or a combination of any or all of those things, that has been assigned by certain government entities and is used to identify the individual or to verify the identity of the individual. The following are examples of government related identifiers: • Medicare numbers • Centrelink reference numbers • driver licence numbers issued by State and Territory authorities, and • Australian passport numbers.

Organisational Information	Information that is related to the operations of the organisation and may include: policies, submissions, funding applications and agreements.

Approval and Amendment History

Original issue date	Last Updated	Author/ reviewer	Policy Owner	Approver	Next review
March 2014	23 February 2024	Nazli Munir Evelyne Tadros Roslyn Bowes Neuda Spencer	CEO	MHCC Board	**23 February 2027**
March 2014	February 2025	Nazli Munir Evelyne Tadros	CEO	MHC Board	**February 2027**

Amendment summary

Date approved	Describe changes
23 February 2024	Modernisation of policy and moving the policy into the new template
February 2025	Inserted updates to comply with new Privacy and Other Legislation Amendments Act 2024 (Cth)

Attachment 1 - Data Breach Response Plan

1. This Data Breach Response Plan (Response Plan) sets out procedures and clear lines of authority for MHCC staff in the event that a data breach occurs (or suspects that a data breach has occurred). All staff must be made aware of this plan and the appropriate action they need to take.

2. The OAIC website https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme should be used as a reference guide in the event of a data breach or suspected data breach.

3. Data breaches must be dealt with on a case-by-case basis, by undertaking an assessment of the risks involved, and using that risk assessment to decide the appropriate course of action.

4. A data breach occurs when personal information an organisation or agency holds is lost or subjected to unauthorised access or disclosure. For example, when:

    - a device with a customer's personal information is lost or stolen
    - a database with personal information is hacked
    - personal information is mistakenly given to the wrong person.

5. An "eligible data breach" arises when:

    - there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an organisation or agency holds
    - a data breach is likely to result in serious harm to one or more individuals
    - the organisation has not been able to prevent the risk of serious harm with remedial action.

6. As soon as MHCC believes, on reasonable grounds that an eligible data breach has occurred, it must notify the Office of the Australian Information Commissioner (OAIC) setting out specific details of the breach and notify the affected individuals as soon as practicable.

7. This Response Plan is intended to enable MHCC to contain, assess and respond to data breaches in a timely fashion, to help mitigate potential harm to affected individuals. It sets out the appropriate staff to contact in the event of a data breach, clarifies the roles and responsibilities of staff, and documents processes to assist MHCC to respond to a data breach.

8. It is important to note that the OAIC is only concerned with breaches that involve personal information. Where there is a data breach (or suspected data breach) for organisational information the below process must still be followed, however the OAIC may not need to be notified.

When a data breach is discovered or suspected

9. When MHCC employees discover, or are alerted to a suspected data breach is, they must:

    - immediately notify their line manager
    - record and advise the line manager of the following:
        - the time and date of the suspected data breach
        - the type of personal information involved
        - the cause and extent of the breach
        - the context of the affected information and the breach
    - where possible, attempt to contain the suspected data breach, e.g.:
        - try to recall an email that was sent to the wrong recipient and/or ask the recipient to permanently delete the email
        - remove a document incorrectly published on the MHCC website
    - If a suspected data breach is successfully recalled, as in the above examples, MHCC staff must keep a record of the suspected data breach and inform their line manager.

10. The line manager must:

    - determine whether a data breach has or may have occurred
    - determine whether the data breach is serious enough to escalate to the CEO (some breaches may be dealt with at line manager level)
    - immediately escalate to the CEO, where appropriate.

11. Once alerted, the CEO must convene a response team comprising of those with knowledge of the breach as well as those that can assist in mitigating harm caused by the breach.

12. Line managers must escalate a data breach or suspected data breach to the CEO.

13. Some data breaches may be comparatively minor, and able to be dealt with easily. For example, a MHCC employee may, as a result of human error, send an email containing personal information to the wrong recipient. Depending on the sensitivity of the contents of the email, if the email can be recalled or, if the employee can contact the recipient and the recipient agrees to delete the email, it may be there is no need to escalate the issue.

14. When a line manager escalates a data breach or suspected data breach to the CEO for further action, the line manager must send a brief email to the CEO that contains the following information:

    - description of the breach or suspected breach
    - action taken by the line manager or staff member to address the breach or suspected breach

- the outcome of that action
- the line manager's view that no further action is required.

15. A copy of the email must be saved in the Data Breach Response file in SharePoint Information can be sent to the Admin Officer for loading.

16. When considering a data breach or suspected data breach, the CEO must consider the following questions:

- Are multiple individuals affected by the breach or suspected breach?
- Is there (or may there be) a real risk of serious harm to the affected individual(s)?
- Does the breach or suspected breach indicate a systemic problem in MHCC processes?
- Could there be media or stakeholder attention because of the breach or suspected breach?

MHCC Data Breach Response Checklist

17. This Response Plan was developed with reference to the ACNC and OAIC Data Response Plan and forms part of the ongoing Risk Management Strategy for MHCC.

Step 1 - Contain the breach and make a preliminary assessment

• Establish the data response team and the CEO to appoint an officer to lead the investigation.
• Convene an urgent meeting of the data response team (within the same working day) where possible and/or within 24 hours of the breach.
• Identify how to contain the breach and whether external parties will need to be involved to support managing the risk –e.g., third-party IT vendors or cloud-based systems that maintain personal data (e.g., Student information).
• Immediately contain the breach e.g.: stop the unauthorised access, recover the records, and notify the relevant parties to cease operation of the system and instruct them to shut the system down.
• Ensure evidence is maintained for later use if needed. Keep accurate records and a timeline of events and associated actions electronically for later use.
• Consider the need for a media strategy, communication plan for both internal and external stakeholders that would be impacted by the breach.

Step 2 - Evaluate the risks for individuals associated with the breach

• Conduct initial investigation, and collect information about the breach promptly, including:
  ○ date, time, duration, and location of the breach
  ○ the type of personal information involved
  ○ how the breach was discovered and by whom
  ○ the cause and extent of the breach
  ○ a list of affected or possible affected individuals
  ○ the risk of serious harm to the affected individuals
  ○ the risk of other harms.

• Determine whether the context of the information is important.
• Assess priorities and risks based on what is known.
• Keep appropriate records of the breach and actions taken, including steps to rectify the situation and the decisions made.

Step 3 - Consider breach notification

• Determine who needs to be notified of the breach (internally and potentially externally) at this stage.
• Determine whether affected individuals need to be notified – is there a real risk of serious harm.

• Consider whether others need to be notified
  ○ OAIC (form available from www.oaic.gov.au)
  ○ police
  ○ other organisations affected by the breach
  ○ contractual need for notification.

• Notification should occur as soon as practicable, however in some instances delay may be necessary.
• Notification should be direct (phone, letter, email) to the affected individual(s) where possible. Indirect notification (website, media) should only occur where direct notification could cause further harm, is cost prohibitive or the direct contact of the affected individual(s) is unknown.
• Details in the notification should include: ○ incident description

- type of information involved
- response to the breach
- assistance (if any) offered to the affected individual(s)
- other information sources designed to assist in protecting against identify theft or interferences with privacy (e.g. www.oaic.gov.au)
- MHCC's contact details
- Whether breach notified to OAIC or other external contacts
- Legal implications
- How individuals can lodge a complaint with MHCC
- How individuals can lodge a complaint with OAIC (where the information is personal information).

- When notifying OAIC complete the associated form.

Step 4 - Review the incident and take action to prevent future breaches

- Fully investigate the cause of the breach.

- Report to CEO (Chair if serious breach) on outcomes and recommendations:
  - Update security if necessary
  - Update policies and procedures if necessary
  - Re-train/ train staff if necessary
  - Update this response plan if necessary.

18. Steps 1-3 above must ideally be undertaken either simultaneously or in quick succession. Depending on the breach not all steps may need to be completed, but consideration should be given to all steps to determine appropriateness.

19. All records created during or as a result of the investigation into the breach or suspected breach should be emailed to the CEO.