Privacy and Privacy Breach Policy & Procedure

Purpose

NOR is committed to protecting the privacy and the confidentiality of personal information of our customers, clients and staff; via complying with the 13 Australian Privacy Principles (APPs), as set out in the Privacy Act 1988.

NOR's *Privacy and Privacy Breach Policy & Procedure* has been developed to assist all parties understand how we collect, store, use and disclose personal information in order to comply with the above privacy legislation; during the course of operating our business and the delivery of our services. The policy also describes the process of how individuals can request to access and correct their personal information and complain about any suspected privacy breach.

NOR is committed to:

- Managing personal information in an open and transparent way;
- Maintaining accurate, complete and up to date personal information;
- Handling personal information in a secure manner;
- Supporting our staffs' understanding of their responsibilities in relation to the privacy legislation; and
- Providing an accessible policy for our staff, clients and customers.

It is expected that management and staff will adhere to this policy and in doing so fulfil their obligations to comply with the privacy legislation.
Where personal information is provided to NOR in person or via email, fax and website; NOR will ensure information remains private and is used in accordance with the privacy legislation and our policy. By providing NOR with your personal information, individuals also consent for NOR to collect, hold, use and share it in accordance with this policy.

Definitions

"Personal information includes a broad range of information, or an opinion, that could identify an individual. What is personal information will vary, depending on whether a person can be identified or is reasonably identifiable in the circumstances; whether the information is true or not, and whether the information is recorded in a material form or not".

"Sensitive information is personal information that includes information or an opinion about an individual's:

- racial or ethnic origin;
- political opinions or associations;
- religious or philosophical beliefs;
- trade union membership or associations;
- sexual orientation or practices;
- criminal record;
- health or genetic information; and
- some aspects of biometric information." [1]

Responsibilities

NOR will:

- Maintain and update this *Privacy and Privacy Breach Policy & Procedure* and related documents;
- Provide staff with access and training in relation to the *Privacy and Privacy Breach Policy & Procedure*; and
- Incorporate relevant feedback into NOR's continuous improvement processes.

Process

1. Collection of personal information

NOR only collects and holds sensitive and/or personal information that is reasonably necessary for operating our business; the delivery of occupational rehabilitation services; injury prevention; and ADL assessment. NOR will give your sensitive information a greater level of protection from unnecessary disclosure and we will not share it unless you have consented.

The kinds of personal information NOR may collect and hold from individuals includes:

- name, date of birth, gender & contact details (Address – postal, residential, email; phone numbers – home, work, mobile);
- drivers' licence and passport information;
- injury details, health, and medical information;
- employment details (qualifications and work history, and other information from your resume);
- photographs or video relating to specific assessments conducted; and/or
- other sensitive information which is defined above.

NOR will collect personal information from individuals directly and depending on the service required, indirectly from additional parties. These parties may include but not be limited to: employers, insurers, doctors, treatment providers, union representatives, and legal representatives. If we receive an individual's personal information and we are not entitled to that information, we will destroy or de-identify that information as soon as practical (if it is lawful and reasonable to do so).

NOR collects personal information during assessment interviews, meetings, via telephone or fax and written correspondence (e.g. reports, letters, and emails (or over the internet or any other electronic medium) and documents provided to us or completed at the time of assessment. All assessments will be conducted in locations which ensure the privacy for all individuals and their medical information. When conducting client meetings in locations such as libraries, community centres, worksites and treatments centres, private rooms will be obtained to ensure privacy and confidentiality. Personal information is also collected through the completion of referral forms on our website.

Individuals are not required to disclose all your personal information to NOR, however NOR may not be able to provide the requested services or business-related activities, if the

information is not supplied. Similarly, an individual can choose to remain anonymous or use a pseudonym when dealing with NOR, however this might lead to the provision of services being impractical.

2. Use and disclosure of Personal Information

NOR only uses individuals' personal information for the purpose it was collected, or for related purposes. We collect, use, manage and disclosure individuals' personal information to carry out the services that have been referred. For example: the delivery of occupational rehabilitation services; injury prevention (manual handling assessment and training); and ADL assessment.

Personal information may be used for internal quality assurance (file review and file audits) or complaint and feedback purposes. Where data analysis is completed; all data would have any identifying information removed.

Personal information may be used for business operations in the following instances including, but not limited to recruitment and induction; staff management; work, health and safety; professional development and training; and customer marketing.

To effectively assist individuals and enable NOR to provide the services we are referred, the following situations may require us to disclose personal information:

- Consultation with an individual's treating doctors, treating allied health professionals, employer or insurer representatives, and other parties (this may include family, unions, service or community organisations) to assist with occupational rehabilitation services;
- In relation to NE services and assisting individuals finding a suitable job: submitting of resume to apply for specific jobs, assist to match individual details with job vacancies, and to host and training organisations if individuals are participating in their activities;
- To another service provider if the individual is being transferred;
- For NOR's business operations, such as administrative (contact with employer or insurer to confirm an individual's personal details for billing purposes); and
- Updating of IT system requirements to ensure secure storage and management of our records.

NOR will not use or disclose an individual's personal information to any third party other than for its intended primary purpose or administrative purposes, without the individual's prior written consent or knowledge. An individual's personal information may be disclosed in the event of exceptional circumstances including but not limited to; serious threat to life, legal reasons, the health, and safety of an individual, or conduct confidential alternative dispute resolution processes. NOR is also obliged to provide information from your file to relevant regulatory authorities upon their request; when the service provided is related to occupational rehabilitation services. Third parties must similarly comply with protecting an individual's privacy in relation to personal information. Where NOR shares an individual's sensitive information, we will require that third parties maintain the confidentiality of that information.

NOR does not intend to disclose your information to any overseas recipients. NOR also collects information through our website. The NOR website is hosted in Australia. We collect data about individuals' interaction with our website, to improve their experience when using our website. The types of data we collect IP addresses, browser information, device type and frequently visited pages.

A cookie is a small data file transferred onto computers or devices by websites for record keeping purposes, to enhance functionality on the website and to personalise online experience. Most browsers allow individuals to choose whether to accept cookies or not. If individuals do not wish to have cookies placed on their computer, then they need to set their browser preferences to reject all cookies before accessing our website.

NOR's website has links to other important websites we think individuals may be interested in; however we cannot ensure that an individual's privacy will be protected as per our *Privacy and Privacy Breach Policy & Procedure*. We encourage individuals to review these other websites' privacy policy, as they will also handle your personal information for their own purposes.

3. Security, storage and maintenance of Personal Information

NOR takes steps to protect the security of the personal information we hold from both internal and external threats by regularly assessing the risk of misuse, interference, loss, and unauthorised access, modification or disclosure of that information; regularly checking only authorised staff have access to specific records; and conducting audits to assess whether we have adequately complied with these measures.

Personal information may be collected and stored in hard copy form or electronic format on NOR's software and systems. We will hold hard copy records securely. Electronic records are held in databases with security safeguards. We destroy personal information in a secure manner when we no longer require. Working with children, criminal records and other checks are securely stored at all times or deleted when required to ensure confidentiality.

To effectively secure an individual's personal information NOR will maintain security by:

- Storing hard copy documents in areas that are only accessed by dual locking systems (lockable cabinets, within a locked room) and allowing only authorised access;
- Ensuring secure destruction of information and adequate de-identification when personal information is no longer needed or required to be kept by law;
- Keeping working files in the possession of the RC or in a secured location at all times when out of the office;
- Providing a private setting for confidential discussions;
- Providing all staff with the appropriate training regarding the secure and safe handling of personal information; and
- Restricting access to computer systems / software (e.g. via login / password protection, defining access rights in Case Manager software).

NOR also has a *Record Management Policy and Procedure* to support the security and storage of an individual's personal information.

4. Access to and correction of Personal Information

NOR aims to ensure individual's personal information is accurate, up to date, complete, relevant and not misleading. Individuals have the right to access and alter their personal information held by NOR in accordance with the Privacy Act (Australian Privacy Principles 12 and 13).

Any request to access, update or correct an individual's personal information should be completed in writing to NOR. We will ask individuals to verify their identity before we give access to or correct personal information. NOR will endeavour to make the process as simple as possible. We will process and respond within 30 days. If this timeframes cannot be meet, NOR will advise the individual of the anticipated timeframe. If requested, we can also notify relevant third parties to whom we have previously disclosed the individual's personal information (if it is practical and lawful to do so).

If we believe for some reason we cannot provide access to the individual, we will give them our reasons for refusing in writing and informed them what further steps can be taken, including the process involved to lodge a complaint, if required.

NOR utilizes detailed referral forms and data collection tools to obtain personal information which is necessary and relevant to provide referred services or business-related activities. During the course of service delivery or business activity, individuals may receive documentation from NOR containing personal information. It is important individuals review the information to ensure their personal information is correct, and if errors are identified, individuals contact NOR as soon as possible to make any corrections.

To ensure that the personal information we collect is accurate, up-to-date and complete we:

- record information in a consistent format;
- where necessary, confirm the accuracy of information we collect from a third party;
- promptly add updated or new personal information to existing records;
- review the quality of personal information before we use or disclose it; and
- complete internal quality assurance processes (file reviews and audits) to ensure accurate and up to date personal information is storage on our systems.

Individuals may also request that NOR cease using their information and contacting them. NOR will comply with the individual's request, however if this involves a request for deletion of your file, please be aware that we may not be required or able to do so, particularly where your file also holds information we are requested to retain under any government contract or where we are required by law or a court or tribunal order to retain your records. However, when we consider your information is no longer needed, we will remove any details that will identify you or we will securely destroy the records.

5. How to make a complaint

If individuals have a concern regarding the handling or a breach of their personal information, they can make a complaint in writing and address it to the Privacy Officer (see responsibilities and contact details below). If you need help lodging a complaint, you can contact us. We view breaches of individual's privacy very seriously and will comply with the notification of eligible data breaches as set out in the Privacy Act. We will inform the individual promptly that we have received their complaint and then respond to the complaint within 30 days.

If we receive a complaint from an individual, we will determine what (if any) action we should take to resolve the complaint. We will assess and handle complaints about the conduct of a NOR staff member using NOR's Values and Code of Conduct and the guidelines provided by the OAIC.

NOR's Privacy Officer is responsible for:

- processing requests for access to or correction of personal information;
- acknowledging your complaint in writing;
- conducting a preliminary assessment of your complaint;
- endeavouring to informally resolve all complaints;
- reviewing the NOR Privacy Policy every three years or when legislation changes; and
- training staff in relation to privacy legislation and process.

NOR will consider an individual's complaint to be resolved when they have expressed satisfaction with the resolution provided, NOR has determined that all avenues available to resolve the complaint has been exhausted or an external agency considers the complaint to be resolved.

Contact: Bianca Antoniolli

Privacy Officer

19 Earls Court,
Goonellabah, NSW 2480
Ph: 0404801074
Email: admin@northernoccrehab.com.au

If an individual is not satisfied with NOR's response or feel unable to discuss the complaint further, they can contact the Office of the Australian Information Commissioner (OAIC):

GPO Box 5218
Sydney, NSW 2001
Ph: 1300 363 992
Email: enquiries@oaic.gov.au

www.oaic.gov.au.

Supporting Documents

- Code of Conduct
- Record Management Policy & Procedure
- Complaint & Feedback Management Policy & Procedure
- Consent Form
- How NOR will handle your personal information
- Recruitment Policy & Procedure
- Induction Policy & Procedure
- Service Delivery & RTW Guidelines

Reference Documents

1. Your personal Information, Office of the Australian Information Commissioner, accessed 3 February 2020, https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/what-is-personal-information/#SensitiveInfo

2. Privacy for organisations, Office of the Australian Information Commissioner, accessed 3 February 2020, https://www.oaic.gov.au/privacy/privacy-for-organisations/small-business/

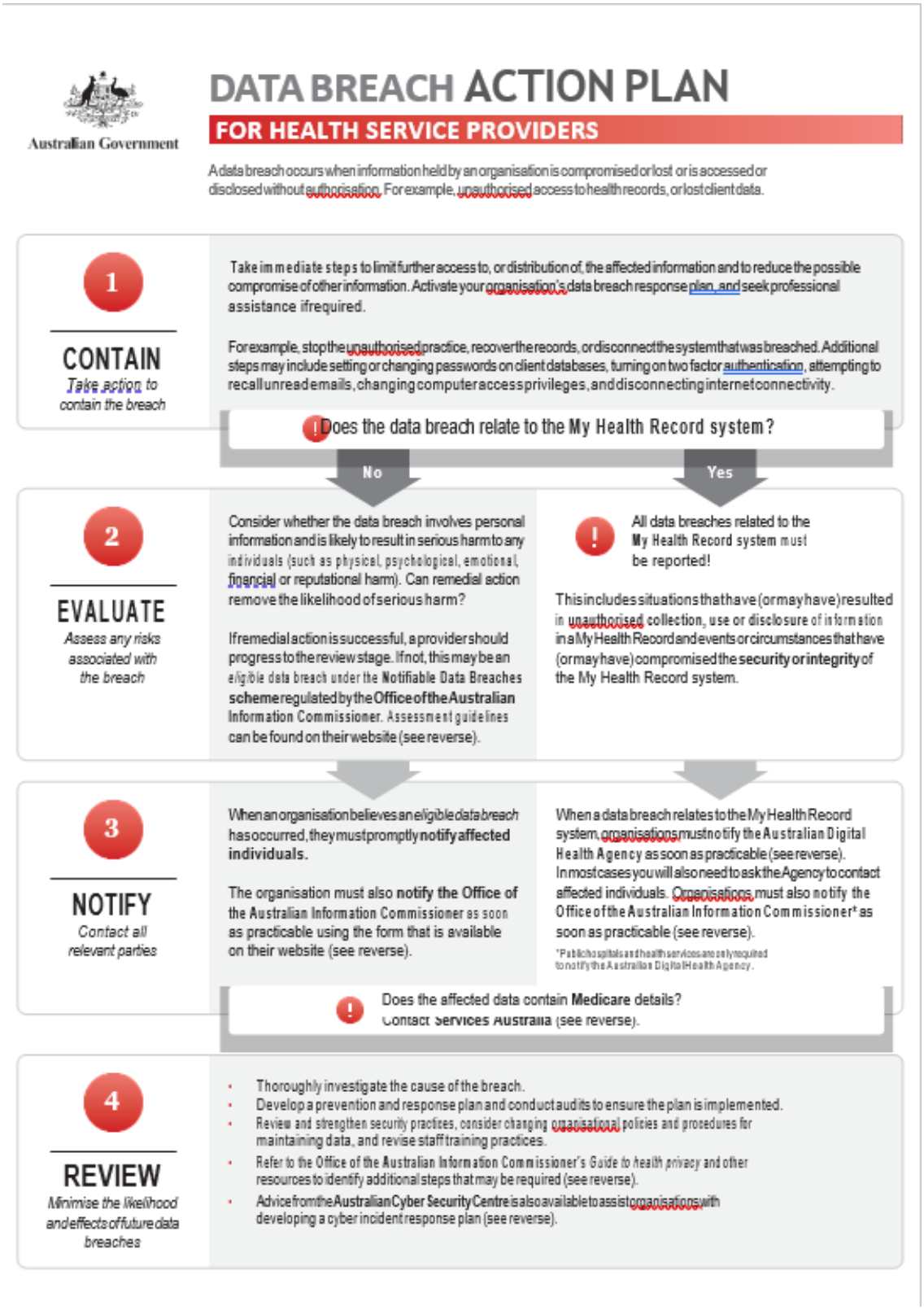
3. Protecting Customers Personal Information, Office of the Australian Information Commissioner, accessed 3 February 2020, https://www.oaic.gov.au/privacy/guidance-and-advice/protecting-customers-personal-information/

4. Guide to developing an APP privacy Principle, Office of the Australian Information Commissioner, accessed 3 February 2020, https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-developing-an-app-privacy-policy/

5. Privacy Act 1988 (Cth). Retrieved from https://www.oaic.gov.au/privacy/the-privacy-act/

Version No.	Author	Purpose/change	Date	Approved
2	Deb Smith	Updated contact information	16/02/21	

Appendix 1: Data Breach Action Plan



Australian Government

DATA BREACH ACTION PLAN

FOR HEALTH SERVICE PROVIDERS

A data breach occurs when information held by an organisation is compromised or lost or is accessed or disclosed without authorisation. For example, unauthorised access to health records, or lost client data.

1 CONTAIN

Take action to contain the breach

Take immediate steps to limit further access to, or distribution of, the affected information and to reduce the possible compromise of other information. Activate your organisation's data breach response plan, and seek professional assistance if required.

For example, stop the unauthorised practice, recover the records, or disconnect the system that was breached. Additional steps may include setting or changing passwords on client databases, turning on two factor authentication, attempting to recall unread emails, changing computer access privileges, and disconnecting internet connectivity.

! Does the data breach relate to the My Health Record system?

No

2 EVALUATE

Assess any risks associated with the breach

Consider whether the data breach involves personal information and is likely to result in serious harm to any individuals (such as physical, psychological, emotional, financial or reputational harm). Can remedial action remove the likelihood of serious harm?

If remedial action is successful, a provider should progress to the review stage. If not, this may be an eligible data breach under the **Notifiable Data Breaches scheme** regulated by the **Office of the Australian Information Commissioner**. Assessment guidelines can be found on their website (see reverse).

3 NOTIFY

Contact all relevant parties

When an organisation believes an eligible data breach has occurred, they must promptly **notify affected individuals.**

The organisation must also **notify the Office of the Australian Information Commissioner** as soon as practicable using the form that is available on their website (see reverse).

Yes

! All data breaches related to the **My Health Record system** must be reported!

This includes situations that have (or may have) resulted in unauthorised collection, use or disclosure of information in a My Health Record and events or circumstances that have (or may have) compromised the **security or integrity** of the My Health Record system.

When a data breach relates to the My Health Record system, organisations must notify the **Australian Digital Health Agency** as soon as practicable (see reverse). In most cases you will also need to ask the Agency to contact affected individuals. Organisations must also notify the **Office of the Australian Information Commissioner*** as soon as practicable (see reverse).

*Public hospitals and health services are only required to notify the Australian Digital Health Agency.

! Does the affected data contain **Medicare** details? Contact **Services Australia** (see reverse).

4 REVIEW

Minimise the likelihood and effects of future data breaches

- Thoroughly investigate the cause of the breach.
- Develop a prevention and response plan and conduct audits to ensure the plan is implemented.
- Review and strengthen security practices, consider changing organisational policies and procedures for maintaining data, and revise staff training practices.
- Refer to the Office of the Australian Information Commissioner's *Guide to health privacy* and other resources to identify additional steps that may be required (see reverse).
- Advice from the **Australian Cyber Security Centre** is also available to assist organisations with developing a cyber incident response plan (see reverse).

Northern Occ Rehab

CONTACT INFORMATION

Office of the Australian Information Commissioner (OAIC)

The OAIC oversees the Notifiable Data Breaches scheme and privacy aspects of the My Health Record system. For more information on notifiable data breaches:

Web: oaic.gov.au/data-breach-preparation-and-response

Assessing an eligible data breach
Web: oaic.gov.au/data-breach-response-steps

Report a notifiable data breach
Web: oaic.gov.au/report-a-data-breach

Report a My Health Record data breach
Web: oaic.gov.au/my-health-record-data-breach

Guide to health privacy
Web: oaic.gov.au/guide-to-health-privacy

Enquiries
Web: oaic.gov.au/contact-us
Phone: 1300 363 992

Services Australia (Medicare)

Services Australia can assist breached organisations by placing impacted customers on a watch list to monitor for any compromise or misuse of customers' Medicare records.

Email: protectyouridentity@servicesaustralia.gov.au

Phone: 1800 941 126

Australian Digital Health Agency (My Health Record system)

All data breaches related to the My Health Record system must be reported to the Australian Digital Health Agency. The Agency will contact affected healthcare recipients, when this is required under the *My Health Records Act 2012*. Where a significant number of people are affected, the general public will be notified.

Web:
myhealthrecord.gov.au/for-healthcare-professionals/howtos/manage-data-breach

Email: MyHealthRecord.Compliance@digitalhealth.gov.au

Phone: 1800 723 471

Australian Cyber Security Centre (ACSC)

The ACSC leads the Australian Government's efforts to improve cyber security, with the role of helping to make Australia the safest place to connect online. For advice on what to consider in developing an incident response plan:

Web: cyber.gov.au/advice/developing-an-incident-response-plan

Report a cyber security incident
Web: cyber.gov.au/report

Alert service: Sign up to the ACSC's Stay Smart Online free alert service on the latest online threats and how to respond at staysmartonline.gov.au

You can also seek support from Australia's national identity and cyber support service, IDCARE by calling 1300 432 273