PRIVACY POLICY

PURPOSE

Fight Parkinson's is committed to protecting the privacy and confidentiality of the personal information (including health information and other sensitive information) that it collects and uses.

Fight Parkinson's complies with its obligations under all applicable privacy laws, including the *Privacy Act 1988* (Cth) (and its Australian Privacy Principles). Where Fight Parkinson's provides services, those service arrangements may also require Fight Parkinson's to comply with other privacy obligations from time to time.

This Privacy Policy explains how Fight Parkinson's manages the personal information that we collect, use and disclose; it also describes how you may contact us if you have any questions or complaints about your privacy or would like to access the personal information, we hold about you.

WHAT INFORMATION DOES FIGHT PARKINSON'S COLLECT?

Fight Parkinson's collects personal information so that we can provide services to people living with and caring for people with Parkinson's. The personal information that we collect from you may include name, address, contact details, lifestyle history, family history, details regarding your current health issues.

We also collect personal information from other individuals, such as employees, volunteers, contractors, students, job, applicants, donors, and service providers, this information is collected to enable us to assess, work with or transact with them. The personal information we may collect from those individuals in those circumstances may include name, contact details, qualifications, education, and employment history.

HOW FIGHT PARKINSON'S COLLECTS PERSONAL INFORMATION

We will ordinarily collect personal information from you directly. Occasionally we may need to collect personal information about you from a third party such as your family or carer. However, we will only do so if you have given us your permission.

If we receive personal information about you from someone else that we have not requested and we determine that we would not have been permitted to collect that information under privacy law, we will ordinarily destroy or de-identify the information.

HOW FIGHT PARKINSON'S USES AND DISCLOSES PERSONAL INFORMATION

Fight Parkinson's will only use and disclose your personal information for the particular purpose for which we have collected it.

Generally, we will use and disclose your personal information for the purpose of providing services to you.

Fight Parkinson's will not transfer your personal information to any person or organisation outside Australia, without your permission. However, Fight Parkinson's may enter into arrangements with service providers who may store some of Fight Parkinson's data (which may include personal information) overseas. If we do, we will ensure we comply with any privacy law requirements that relate to cross border disclosures of personal information.

We may collect information in the following manner:

- directly, in person (face to face or by telephone) in documents, by email or via Fight Parkinson's website;
- from third parties, such as strategic research partners; and
- from Fight Parkinson's members register

If we collect personal information from an agent acting on your behalf, we will seek some indication that the party contacting us is your authorised agent

PROTECTION OF YOUR PERSONAL INFORMATION

Fight Parkinson's has adopted the National Data Breach (NDB) scheme.

Fight Parkinson's has implemented measures to protect your personal information from misuse, interference, loss, unauthorised access, modification and disclosure. The information we collect is stored in either hard copy or electronic format.

We use access control procedures, audit trails, email and web network firewalls as well as physical security to protect your privacy. Only staff or contractors that have the appropriate authorisation have access to your records and we monitor any access to these records.

Where we no longer require the personal information, you have supplied for the purpose for which we collected it, Fight Parkinson's will destroy or permanently de-identify any of your information which, provided we are not required under law to retain the information.

CORRECTION OF YOUR PERSONAL INFORMATION

You may access your personal information by viewing it or by requesting a copy of your personal information. You may request access to the personal information we hold about you by contacting us at the details set out below. You may also request that we correct the personal information we hold about you if you believe that it is inaccurate by contacting us at the details set out below.

We will not ordinarily charge you for giving you access to your personal information, however excessive requests or the volume of information requested may incur a charge which are in accordance with the fees and charges we are permitted to charge under the applicable laws.

Fight Parkinson's will consider your request for access or correction and respond within the time required by law.

COMPLAINTS OR QUERIES REGARDING YOUR PRIVACY

If you have any queries or wish to make a complaint regarding how Fight Parkinson's has handled your personal information, you may contact us at the details set out below. We will consider your complaint promptly and provide a written response on the outcome.

CONTACT DETAILS

You may contact us in any of the following ways:

- By telephone: 03 8809 0400
- By letter: Privacy Officer, Fight Parkinson's 03 8809 0400
- Online: Through our website info@fightparkinsons.org.au.

If you would prefer to make your complaint to an external complaint body, or you are not satisfied with the handling or outcome of the Fight Parkinson's complaints process, you may contact the following organisations to lodge a complaint:

Australian Information Commissioner
By telephone: 1300 363 992
By email: enquiries@oaic.gov.au
Online: https://forms.business.gov.au/aba/oaic/privacy-complaint-/

YOUR USE OF OUR WEBSITE

When using Fight Parkinson's website you may voluntarily disclose personal information to us. Our server may automatically record details such as your internet address, domain name if applicable, and the date and time of your visit to our website. This information is used for internal purposes only, including statistical purposes.

We use cookies. A cookie is a small data file that is stored on your browser or device and allows our computer server to identify your computer or device. This information allows our website content to load and function as intended when you access it and to monitor various statistics on use of our website. Most browsers will allow you to control whether the browser will accept or reject all, or certain, cookies. Further, you should be able to delete most cookies – you should check your browser for instructions on how to do this.
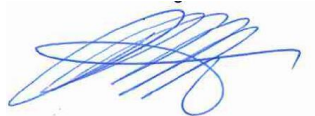
When you access our website, we will keep a record of your visit. We may collect the following information that does not identify you in relation to your use of our website: your computer address, the date and time of your visit, the type of browser you use, the pages you visit, the information you request and the country from which you request information. We collect this information for statistical purposes and to monitor and improve our web site and services. We will not try to identify users or their browsing activities except as necessary to investigate or report any suspected unlawful activity, as required or authorised by law or as reasonably necessary for the activity of an enforcement body

Our website may contain links to third party websites unrelated to Fight Parkinson's. This Privacy Policy has no application to third party websites. Fight Parkinson's makes no representation regarding, and is not responsible for, the content or the privacy practices of third party websites and has no knowledge of whether cookies or other tracking devices may be used by those sites.

Fight Parkinson's cannot ensure that any information transmitted over the internet is secure and you transmit such information at your own risk. However, once we receive a transmission of personal information, we take all reasonable steps to ensure that the information is secure on our systems.

APPROVED BY THE BOARD

Signed:

Date: 10 June 2021

Chair, Fight Parkinson's

Appendix 1

APP entities

The National Data Breach (NDB) scheme applies to entities that have an obligation under the Australian Privacy Principals (APP) 11 of the Privacy Act to protect the personal information they hold. Entities include Australian Government agencies and private sector and not-for-profit organisations with an annual turnover of more than $3 million. This includes all entities of any size that trade in personal information and organisations that provide a health service to, and hold health information about individuals.

Eligible data breach

An eligible data breach arises when the following three criteria are satisfied:

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

1. **What is a 'data breach'?**

The first step in deciding whether an eligible data breach has occurred involves considering whether there has been a data breach; that is, unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information. The *Privacy Act 1988* (Cth) (Privacy Act) does not define these terms.

- *Unauthorised access* of personal information occurs when personal information that an entity holds is accessed by someone who is not permitted to have access. This includes unauthorised access by an employee of the entity, or an independent contractor, as well as unauthorised access by an external third party (such as by hacking).
- *Unauthorised disclosure* occurs when an entity, whether intentionally or unintentionally, makes personal information accessible or visible to others outside the entity, and releases that information from its effective control in a way that is not permitted by the Privacy Act. This includes an unauthorised disclosure by an employee of the entity.
- *Loss* refers to the accidental or inadvertent loss of personal information held by an entity, in circumstances where is it is likely to result in unauthorised access or disclosure.

Under the NDB scheme, if personal information is lost in circumstances where subsequent unauthorised access to or disclosure of the information is unlikely, there is no eligible data breach.

The type or types of personal information involved in the data breach

Examples of the kinds of information that may increase the risk of serious harm if there is a data breach include:

- 'sensitive information', such as information about an individual's health,
- documents commonly used for identity fraud (including Medicare card, driver licence, and passport details),
- financial information,
- a combination of types of personal information (rather than a single piece of personal information) that allows more to be known about the individuals the information is about.

The nature of the harm

Entities should consider the broad range of potential kinds of harms that may follow a data breach. Examples may include:

- identity theft
- significant financial loss by the individual
- threats to an individual's physical safety
- loss of business or employment opportunities
- humiliation, damage to reputation or relationships
- workplace or social bullying or marginalisation.

The likelihood of a particular harm occurring, as well as the anticipated consequences for individuals, are relevant.

How to notify

When an agency or organisation is aware of reasonable grounds to believe an eligible data breach has occurred, they are obligated to promptly notify individuals at likely risk of serious harm. The Commissioner must also be notified as soon as practicable through a statement about the eligible data breach.

Who needs to be notified?

Once an entity has reasonable grounds to believe there has been an eligible data breach, the entity must, as soon as practicable, make a decision about which individuals to notify, prepare a statement for the Commissioner and notify individuals of the contents of this statement.

The NDB scheme provides flexibility — there are three options for notifying individuals at risk of serious harm, depending on what is 'practicable' for the entity.

Whether a particular option is practicable involves a consideration of the time, effort, and cost of notifying individuals at risk of serious harm in a particular manner.

Option 1 — Notify all individuals

If it is practicable, an entity can notify each of the individuals to whom the relevant information relates. That is, all individuals whose personal information was part of the eligible data breach.

This option may be appropriate, and the simplest method, if an entity cannot reasonably assess which particular individuals are at risk of serious harm from an eligible data breach.

Option 2 — Notify only those individuals at risk of serious harm

If it is practicable, an entity can notify only those individuals who are at risk of serious harm from the eligible data breach.

Option 3 (Publish notification)

Option 3, which can only be used if Options 1 or 2 are not practicable, requires an entity to publish a copy of the statement prepared for the Commissioner on its website, and take reasonable steps to publicise the contents of that statement.

Timing of notification

Entities must notify individuals as soon as practicable after completing the statement prepared for notifying the Commissioner.

Considerations of cost, time, and effort may be relevant in an entity's decision about when to notify individuals. However, the Commissioner generally expects entities to expeditiously notify individuals at risk of serious harm about an eligible data breach unless cost, time, and effort are excessively prohibitive in all the circumstances.