Potential (x) Client Data Privacy Policy

|  |  |
| --- | --- |
| **Policy Title** | **Data Privacy Policy** |
| Person Responsible | Hagan Slattery  | Effective: April 2016 |
| Date Last Updated | 26 April 2016 | Status: Approved |
| File Name | QMS-POL-07-DataPrivacyPolicy |   |
| Folder Name | G:\My Drive\HRT Drive\HRT & Potential (x) Policies & Procedures\Policies\Potential (x)\Information Technology |   |

**Version History**

|  |  |  |
| --- | --- | --- |
| **#** | **Updater** | **Notes** |
| 1.1 | Hagan Slattery | Draft |
| 1.2 | John Menzies | Reviewed/Amended/Approved |
| 1.3 | Rachel Plumbe | Reviewed/Amended |
| 1.4 | David Dean | Reviewed/Approved |
| 1.5 | Hagan Slattery | Updated with “bound by confidentiality agreements” |
| 1.6 | Cheryl Duffy | Rebranded |

# Contents

[Contents](#h.f4c617x785w2)

[Introduction](#h.vd5zehi0kdl6)

[Collection of Information](#h.4285qlravanq)

[Data Submitted for Analysis](#h.8atq7krlol)

[Unsolicited Personal Information](#h.7gc8a1egzoa)

[Use and Disclosure of Information](#h.7see0dwh6vlj)

[Cross Border Disclosure of Information](#h.pk37yf4ueidu)

[Access to and Correction of Information](#h.dqyoyyt2xu0p)

[Quality of Information](#h.9yzrkthspwew)

[Access to Information](#h.szyn1x41h0lf)

[Correction of Information](#h.dbjoz9a2tray)

[Destruction of Information](#h.3eajm5ro7j3f)

[Data Breach Response Policy](#h.coevtobovfrb)

[Updates To This Policy](#h.1y958ysr6se)

[Further Information, Enquiries or Complaints](#h.tk265jggufrm)

#

#

# Introduction

In its day to day operations Potential (x) Pty Ltd provides commercial health data analysis services to major Australasian healthcare providers. Given the potentially personal and sensitive nature of information provided by clients for analysis, Potential (x) maintains this client Data Privacy Policy to outline the responsibilities and obligations of both Potential (x) and its clients when engaging in data analysis.

The handling of personal data within Australia is governed by the Privacy Act 1988. This act requires organisations that hold personal information to obey certain restrictions and requirements when dealing with personal information. These are collectively known as the Australian Privacy Principles (APPs), and place certain requirements on organisations holding personal data in the areas of collection, disclosure and access.

The Privacy Act 1988 defines personal information as:

*“Information or an opinion (including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can be reasonably ascertained, from the information or opinion.”*

In 2002, Privacy Commissioner Malcolm Crompton further clarified this stating:

*“... In practice, identifying an individual generally involves focusing on those things that distinguish that individual from others, including legal name, date of birth, location or address and symbolic identifiers such as a driver's license number.“*

Many of the APPs’ requirements are impractical to execute for data of the volume typically held by Potential (x) for analysis. Therefore:

**Potential (x) will only accept, retain and analyse client data that has been anonymised to such a degree that it can no longer be considered personal information**.

This vastly simplifies the legal requirements placed on the submission, holding, analysis and disclosure of client data by Potential (x). That said, Potential (x) will comply with the Privacy Act and APPs with regard to client data wherever practical. In doing so, Potential (x) will treat the client as a proxy to the owner of the information. This ensures that Potential (x) is meeting or exceeding privacy expectations and requirements at all times.

#

#

# Collection of Information

## Data Submitted for Analysis

Potential (x) will only collect personal information via bulk data provision by clients. Potential (x) will only solicit data from the client required to perform the analysis requested, and will only work with the data provided by the client when performing that analysis. Potential (x) requires clients to state that they have a legal right to disclose any data provided to Potential (x), and that the data has been anonymised.

Potential (x) requires that all data submitted for analysis be anonymised so as not to be considered personal information. The following table describes which information Potential (x) can accept from clients as being unidentifiable or anonymous, and which must be rejected due to its potential to reasonably identify a person.

|  |  |
| --- | --- |
| **Anonymous Information** | **Identifying Information** |
| Date of Birth / Date of Death | Legal Name |
| Indigenous Status / Ethnic Origin | Government Identifier (TFN, Medicare # etc) |
| Gender | Residential Address |
| Postcode / SLA / Domicile Code |  |

Potential (x) allows clients to anonymise any other entities (such as organisation or facility names) within their submitted data. If Potential (x) is aware of the actual names for entities represented by a pseudonym, it will not disclose this information to any party other than the submitting client unless authorised by the client to do so.

## Unsolicited Personal Information

If Potential (x) receives identifying information as part of a client data submission (residential addresses for example), Potential (x) will immediately destroy the identifying information and advise the client. It will then be the client’s responsibility to inform individuals that their personal information has been disclosed if required. Potential (x) may also request that the client re-submit anonymised data to complete any analysis.

#

#

# Use and Disclosure of Information

Client data will only be used by Potential (x) for the purpose for which it was submitted by the client. Potential (x) will not use the data for any other purpose without first seeking approval by the client. Potential (x) will not release client data, or results of client data analysis to any party other than the client without first seeking approval by the client.

Potential (x) may disclose data or the results of data analysis to other organisations when requested to do by the client in the service agreement. This may include research groups, member organisations of the client and other related entities. In these cases, Potential (x) will follow any disclosure requirements or limitations imposed by the client.

Potential (x) may, in exceptional circumstances, release client data to law enforcement agencies, courts of law and regulatory bodies as required by law. In this event, data will only be disclosed that is within the jurisdiction of the organisation requesting the information.

It should be noted that in the course of normal operations, Potential (x) may disclose client data to other service providers such as web hosting and data backup providers. When negotiating contracts with service providers, Potential (x) will make every effort to select providers who are compliant with the Australian Privacy Act.

## Cross Border Disclosure of Information

In the event that an international client provides data to Potential (x) for analysis, Potential (x) will apply the APPs to the data for as long as it is held. When client data, data analysis or aggregate information is released back to an international client, a reference to the APPs will be included with the data alongside a requirement that the information continue to be treated in accordance with the Australian Privacy Principles.

The Australian Privacy Act 1988 is considered to be equivalent legislation to the New Zealand Privacy Act 1993, and the UK Data Protection Act 1988. These pieces of legislation are largely similar in the protections they offer individuals. It can be assumed that an international entity abiding by one of these equivalent pieces of legislation would satisfy the Australian Privacy Principles, and vice versa.

#

#

# Access to and Correction of Information

The APPs state that organisations must provide a pathway for individuals to access and update the information held about them by that organisation. It would be highly impractical (and inappropriate) for Potential (x) to interact with individuals about anonymised data submitted by a Potential (x) client. Potential (x) therefore extends the right of access and correction of data to the client providing the data. It is the responsibility of the client to extend that right to individuals.

## Quality of Information

It is the responsibility of the client to ensure that data submitted to Potential (x) for analysis is accurate, up to date and complete. Potential (x) will provide a best effort audit process to check the quality of data being submitted.

## Access to Information

Potential (x) clients may request a copy of any data held by Potential (x) that they have provided. Potential (x) will provide a copy of the data held by Potential (x) within 30 days.

## Correction of Information

Potential (x) clients may update data held by Potential (x) via resubmission or direct update request. Potential (x) will process any such request or re-submission within 120 days.

## Destruction of Information

Potential (x) retains client data indefinitely to allow further analysis of data at a future date if requested. Data will only be destroyed at the specific request of a client.

# Protection of Data

Potential (x) limits access to customer data to staff and contractors with a legitimate need to use it for the purpose for which it was collected. All employees and contractors of Chappel Dean are bound by confidentiality agreements. Potential (x) also employs technical security measures to prevent unauthorised access or modification of personal information from outside the organisation.

# Data Breach Response Policy

In the event that Potential (x) believes client data has been disclosed in a way that breaches the Australian Privacy Act or the contractual agreement with the client, Potential (x) will inform the client as soon as possible and keep them updated on any subsequent investigation.

If the breach is determined to originate from a Potential (x) employee, contractor service providers, Potential (x) will be responsible for taking the appropriate action (up to and including immediate termination of contract). If the breach is determined to originate from a client organisation, Potential (x) will communicate these findings to the client, and follow any changes to collection and disclosure that the client wishes to implement.

#

# Updates To This Policy

This policy is reviewed annually to ensure continuing compliance with Australian Privacy legislation. The most recent review date can be found on the document title page.

# Further Information, Enquiries or Complaints

If you have any further questions about how Potential (x) handles client data, or would like to make a complaint, please contact us.

Potential (x)

40 Port Jackson Road, Terrigal NSW 2260

Tel: +61 (0) 2 8006 4834

Email: privacy@chappelldean.com

ABN 21 062 345 117