



**Office of the Victorian
Information Commissioner**

IPP 7 – Unique Identifiers



IPP 7 – Unique Identifiers

On this page

‘Unique identifiers’	3
How to determine whether an identifier is a ‘unique identifier’	3
Distinguishing unique identifiers under the IPPs from other identifiers.....	4
Examples of unique identifiers	4
Restrictions on the use and disclosure of unique identifiers	5
IPP 7.1: Assignment of a unique identifier	5
IPP 7.2: Adoption of another organisation’s unique identifier	6
Adoption versus recording of unique identifiers.....	6
IPP 7.2(a): Necessary to efficiently carry out functions.....	7
IPP 7.2(b): Consent.....	7
IPP 7.2(c): Outsourcing	7
IPP 7.3: Use or disclosure of a unique identifier.....	8
IPP 7.3(a): Necessary to fulfil obligations to the other organisation.....	8
IPP 7.3(b): Use or disclosure in certain public interests	9
IPP 7.3(c): Use or disclosure by consent	9
IPP 7.4: Requiring identifiers to be provided in order to obtain a service	10
IPP 7 in practice.....	12
Is an email address a unique identifier?	12
Data matching and the IPPs.....	12
Is a code assigned to de-identify an individual a unique identifier?	12
Version control table.....	13

Document version: IPP 7 (Unique Identifiers) 2019.B, 14 November 2019.

- 7.1 IPP 7 deals with the assignment, adoption, use and sharing of unique identifiers. IPP 7 is intended to prevent pervasive data matching across government. This is reflected in the Explanatory Memorandum for the PDP Act which states IPP 7 ‘provides a safeguard against the creation of a single identifier that could be used to cross match data across all Government Departments’.¹
- 7.2 The use of unique identifiers also increases the risk of ‘function creep’ because the use of an identifier can lead to more personal information becoming linked over time to that identifier. For more discussion on [function creep](#), see the Key Concepts chapter.

‘Unique identifiers’

7.3 A ‘unique identifier’ is defined under Schedule 1 of the PDP Act to mean:

an identifier (usually a number) assigned by an organisation to an individual uniquely to identify that individual for the purposes of the operations of the organisation but does not include an identifier that consists only of the individual's name and does not include an identifier within the meaning of the Health Records Act 2001.

- 7.4 An identifier can be a sequence of numbers, letters or characters. An individual’s name is not considered a unique identifier under the PDP Act. However, an identifier that includes part of a person’s name or uses their initials may be regarded as a unique identifier. For example, a statistical linkage key comprised of a person’s initials and date of birth (JWH-26071939) is likely to be a unique identifier.
- 7.5 IPP 7 does not apply to unique identifiers that fall within the meaning of an ‘identifier’ under the Health Records Act 2001 (Vic) (**HR Act**). Instead, Health Privacy Principle (**HPP**) 7 applies to the assignment, adoption, use and disclosure of identifiers under the HR Act. For example, a patient identifier assigned to a person undergoing medical treatment is regulated by the HR Act not the PDP Act. The exclusion of health identifiers from the definition of unique identifier under the PDP Act was expressly intended to avoid duplication in the regulation and handling of personal information under both laws.²

How to determine whether an identifier is a ‘unique identifier’

- 7.6 There are three steps to determine whether a particular sequence of numbers, letters or symbols is a ‘unique identifier’ for the purposes of the PDP Act:
1. Was the identifier assigned by an organisation to an individual?
 2. Was the identifier assigned with the aim, purpose or intention of uniquely identifying that individual?
 3. Was the assignment of the identifier to uniquely identify the individual for the purposes of the organisation’s operations?
- 7.7 When applying the test to determine whether an identifier is a unique identifier for the purposes of the PDP Act, organisations should keep in mind the aim of IPP 7: to ‘safeguard against the creation of

¹ Explanatory Memorandum, Privacy and Data Protection Bill 2014, 36.

² Explanatory Memorandum, Health Records Bill 2001, 23.

a single identifier that could be used to cross match data across all Government Departments'.³ This approach may help organisations with the second limb of the test in particular as it may provide helpful context for determining the intention for assigning a unique identifier to an individual.

- 7.8 Individuals interacting with organisations will sometimes be linked to numbers or codes that could be used to identify them. These kinds of identifiers may include serial numbers of equipment assigned to an individual, desk numbers, position numbers, titles and email addresses. Importantly, these identifiers are not assigned to identify that individual, but for some other reason, such as to keep track of transactions and equipment or to manage accommodation or facilitate communication. Importantly, these identifiers are not assigned to an individual to identify that individual, but for some other reason. Unless a number, letter, symbol or combination of these is assigned to an individual for the purpose of uniquely identifying them, it will not attract the additional protections of IPP 7.
- 7.9 This interpretation of 'unique identifier' means an identifier not initially assigned to identify an individual can later become a unique identifier. What matters is the purpose for which a label, name or other identifier is used. An identifier that is later used for the purpose of uniquely identifying an individual can be a unique identifier for IPP 7.

Distinguishing unique identifiers under the IPPs from other identifiers

- 7.10 Information that uniquely identifies a person in a general sense should be distinguished from 'unique identifiers' as defined under Schedule 1 of the PDP Act. In some cases, information may uniquely identify a person, however, that information will not necessarily constitute a unique identifier for the purposes of IPP 7. For example, an individual's identity is often apparent from their email address, and, as email addresses have to be unique, they can uniquely identify that individual. However, an email address is not likely to be a unique identifier for the purposes of Part 3 of the PDP Act. Email addresses and unique identifiers are considered in more detail below under [IPP 7 in practice](#) at [7.49]-[7.50].
- 7.11 Where an organisation holds information that uniquely identifies an individual, but that falls outside the scope of the definition of unique identifiers under Schedule 1 of the PDP Act, this does not prevent the organisation from giving that information a higher standard of protection. In accordance with [IPP 4](#), organisations will need to put in place security controls that are proportionate to the possible harm to an individual if that information is compromised.

Examples of unique identifiers

- 7.12 The most common example of a unique identifier in Victoria is a driver's licence number issued by VicRoads. Identifiers are often found on identity or entitlement documents issued by public sector organisations. Other examples of documents that may contain unique identifiers include:

- student identity cards issued by universities;
- health care and concession cards;
- birth and marriage certificates;
- attainment of citizenship documents;
- library cards;
- membership cards;
- credit cards; and
- passports.

³ Explanatory Memorandum, Privacy and Data Protection Bill 2014, 36.

- 7.13 Identifiers are also used in conjunction with registration schemes for professionals, police and others who must obtain permission to work in the community. For example, volunteers who work with children in Victoria must have a valid Working With Children Check.
- 7.14 TFNs are also a good example of unique identifiers. However, TFNs are treated differently from most other unique identifiers. TFNs are subject to purpose-built legislation that specifically prohibits collection, use or disclosure except for limited purposes.⁴ The handling of TFNs is also subject to specific, [binding rules](#) issued by the Australian Privacy Commissioner under s 17 of the *Privacy Act 1988* (Cth).
- 7.15 Biometric characteristics, which encompass unique patterns of bodily features such as a person's fingerprint or iris, may also constitute a unique identifier. While a biometric characteristic itself is not 'assigned' to individuals in the same way a number is, an organisation may assign individuals with a unique identifier based on a biometric characteristic. As they are unique to individuals and can be more reliable and effective than an ID card or password, organisations often use biometric data for authentication or identification. For example, a prison may use a combination of fingerprint and iris scanning to verify the identity of visitors and staff.

Restrictions on the use and disclosure of unique identifiers

- 7.16 IPP 7 restricts the assignment, adoption and use and disclosure of unique identifiers by Victorian public sector organisations, except where specific requirements are met. The requirements permitting unique identifiers vary if the organisation assigns its own unique identifier (IPP 7.1), adopt another organisation's unique identifier (IPP 7.2) or use or disclose another organisation's unique identifier (IPP 7.3). The specific requirements are explained below.

IPP 7.1: Assignment of a unique identifier

- 7.17 IPP 7.1 states an organisation must not assign unique identifiers to individuals unless that assignment is necessary to enable the organisation to carry out any of its functions efficiently.
- 7.18 An organisation should be clear about the need for the unique identifier. Assigning unique identifiers should not occur simply because the organisation wants to use them, or it is convenient. [Ng v Department of Education](#)⁵ suggests an organisation should ask whether assigning a unique identifier is reasonably required or ancillary to the achievement of the organisation's functions.
- 7.19 Organisations should also be clear and specific about the functions for which it is necessary to assign unique identifiers to individuals. It is important to be clear about whose functions are being carried out as IPP 7.1 does not allow organisations to assign identifiers to assist in the efficient conduct of another organisation's functions. Unique identifiers should only be assigned where they are relevant to the functions of the organisation assigning the identifier.
- 7.20 An organisation should also consider whether assigning a unique identifier is necessary to enable it

⁴ For example, under the [Taxation Administration Act 1953](#) (Cth). Also, the [Data-matching Program \(Assistance and Tax\) Act 1990](#) (Cth) authorises the use of TFNs in data matching between the Australian Taxation Office (ATO) and certain Commonwealth agencies that provide welfare and assistance. In addition, the *Budget Savings (Omnibus) Act 2016* (Cth) requires organisations to implement Single Touch Payroll (STP) which means organisations must send payroll data (including TFNs) to the ATO each pay cycle.

⁵ [Ng v Department of Education](#) [2005] VCAT 1054 [84].

to carry out its functions 'efficiently'. 'Efficiently' for the purpose of IPP 7 means with minimum waste or effort. Whether a function is being carried out 'efficiently' requires an assessment from the perspectives of both the organisation and its stakeholders. 'Necessary' means reasonably proportionate and is discussed in greater detail in the Key Concepts chapter. When considering assigning unique identifiers to individuals, organisations should always maintain a sense of proportionality. Needing to distinguish between a few similar names should not automatically lead to the conclusion that everyone dealing with the organisation needs a unique identifier.

Case Study 7A: Avoiding assigning a unique identifier where possible

An organisation deals with two Jane Smiths from the same suburb. Rather than assigning a unique identifier to each individual in the organisation's entire database, it adopts a more proportionate response. The organisation decides to refer to the two individuals as Jane Smith A and Jane Smith B in its database, removing the need for unique identifiers.

Another approach may be to confirm the integrity of the information. The two Janes may actually be the same person appearing twice in the database or one may no longer a client or employee of the organisation and should be removed.

7.21 Case Study 7A suggests organisations avoid assigning unique identifiers where possible. However, where there are many, many people with the same names, a unique identifier might be the most (or only) practicable option. For example, prisoners are assigned Criminal Reference Numbers.

IPP 7.2: Adoption of another organisation's unique identifier

7.22 The potential privacy risks associated with profiling and data matching increase when a unique identifier assigned by one organisation is adopted by other organisations. To minimise these risks, IPP 7.2 limits the adoption of identifiers across multiple agencies.

7.23 IPP 7.2 prohibits an organisation from adopting as its own unique identifier of an individual a unique identifier assigned by another organisation, unless:

1. it is necessary to enable the organisation to carry out any of its functions efficiently; or
2. it has obtained the consent of the individual to the use of the unique identifier; or
3. it is an outsourcing organisation adopting the unique identifier created by a contracted service provider in the performance of its obligations to the organisation under a State contract.

7.24 Limiting the adoption of particular identifiers across different organisations may reduce the extent of harm where identity theft occurs. If a unique identifier is inappropriately accessed or disclosed, whether inadvertently or by theft, it can potentially be used to obtain access to, and to misuse, other information.

Adoption versus recording of unique identifiers

7.25 Unique identifiers and identity documents are commonly requested by organisations to establish or

verify identity. If anonymity is not a lawful and practicable option, sometimes it may be sufficient for an organisation to simply sight an identity document and perhaps note that it was sighted. In this instance, the PDP Act would not apply as the information is not recorded. At other times, it may be necessary to keep a copy of the identity document or make a note of the unique identifier, in which case the PDP Act will apply.

- 7.26 IPP 7.2 does not prevent an organisation from recording unique identifiers as evidence of identity, nor does it prevent an organisation from requesting identification as required by law. However, the organisation is not permitted to adopt those identifiers assigned by other organisations as its own unless IPP 7.2(a), (b) or (c) applies.

IPP 7.2(a): Necessary to efficiently carry out functions

- 7.27 Under IPP 7.2(a), an organisation may adopt another organisation's unique identifier where it is necessary to carry out any of their functions *efficiently*. See the discussion of 'necessity' and 'efficiency' under IPP 7.1 for more information.

IPP 7.2(b): Consent

- 7.28 Under IPP 7.2(b), an organisation is permitted to adopt as its own a unique identifier assigned by another organisation if that organisation has the consent of the individual to whom the unique identifier was assigned. It is the organisation seeking to adopt the unique identifier which must seek the individual's consent, not the organisation that originally assigned it.
- 7.29 Seeking meaningful consent promotes transparency and gives individuals an opportunity to assess the risks and benefits of the proposed adoption of their identifier. Consent should be specific, informed, voluntary, current and given by someone with the capacity to do so. Consent for the adoption of another organisation's unique identifier should not be part of 'bundled' consent. More information on meaningful [consent](#) is in the Key Concepts chapter.

IPP 7.2(c): Outsourcing

- 7.30 An organisation may adopt as its own a unique identifier assigned to individuals by a contracted service provider (CSP) if the unique identifier was created by the CSP in the performance of its obligations to the outsourcing organisation under a State Contract.
- 7.31 IPP 7.2(c) does not operate in reverse. A CSP may, in the course of performing obligations to the outsourcing organisation under a State Contract, become aware of an organisation's unique identifiers for individuals.⁶ However, the CSP cannot adopt the unique identifier as its own.
- 7.32 Organisations should ensure contracts with CSPs deal appropriately with the security and return or disposal of unique identifiers CSPs may acquire in the course of the contract. For more information on the obligations of organisations in an outsourcing arrangement, see OVIC's [Guidelines for outsourcing in the Victorian public sector](#).

Case Study 7B: Outsourcing party adopting the unique identifier of a contracted service provider

An organisation engaged a contracted service provider (CSP) to undertake debt recovery

⁶ This may be a use or disclosure by the outsourcing organisation under IPP 7.3(a), where the contracted service provider is itself an organisation under 13 of the PDP Act.

services on its behalf. The CSP was bound to the IPPs under a specific provision in its State contract with the outsourcing organisation.

In the course of performing its obligations under the State contract, the CSP assigned a reference number to individuals it had pursued regarding outstanding debt. The CSP used these identifiers in its communications with the outsourcing organisation to uniquely identify individuals.

The outsourcing organisation adopted the CSP's unique identifiers for the purposes of managing its own database of clients that it had referred to the CSP for debt recovery. In this case, the outsourcing organisation was able to adopt the CSP's unique identifiers to use as its own, under IPP 7.2(c).

IPP 7.3: Use or disclosure of a unique identifier

7.33 IPP 7.3 prohibits an organisation from using or disclosing a unique identifier assigned by another organisation, unless one of the following applies:

1. the use or disclosure is necessary for the organisation to fulfil its obligations to the other organisation; or
2. one or more of IPP 2.1(d) to (g) applies to the use or disclosure; or
3. it has obtained the consent of the individual to the use or disclosure.

7.34 While IPP 7.2 restricts an organisation from adopting other organisations' unique identifiers as its own, IPP 7.3 limits an organisation's ability to use and disclose unique identifiers assigned by other organisations. For example, if an organisation conducts an identity check and records a driver's licence number, IPP 7.2 prevents the organisation using that identifier to refer to that individual or their information, while IPP 7.3 restricts the organisation from using or disclosing the driver's licence number either for its own purposes or to other organisations.

7.35 However, IPP 7.3(a) to (c) outlines three particular exceptions which permit organisations to use and disclose other organisations' unique identifiers.

IPP 7.3(a): Necessary to fulfil obligations to the other organisation

7.36 IPP 7.3(a) allows an organisation to use or disclose a unique identifier assigned by another organisation where it is necessary for the organisation to fulfil its obligations to the organisation that originally assigned the identifier. The meaning of 'necessary' is discussed in the [Key Concepts](#) chapter. 'Obligations' means more than an understanding, habit, arrangement, course of conduct or administrative practice. It includes statutory and contractual obligations.

Case Study 7C: Disclosure necessary for statutory obligations

For example, a school collects certain information from a teacher when they are first employed, including a teacher registration number issued by the Victorian Institute of

Teaching (VIT). The school has a statutory obligation to inform VIT if any action is taken against the teacher in response to an allegation of serious misconduct. The school's disclosure of the teacher's registration number in communication with VIT about a disciplinary action taken is in accordance with IPP 7.3(a) because the school's statutory obligations make the use and disclosure necessary.

IPP 7.3(b): Use or disclosure in certain public interests

7.37 IPP 7.3(b) allows an organisation to use or disclose another organisation's unique identifier for certain public interest purposes listed in [IPP 2.1\(d\) to \(g\)](#), namely where:

- IPP 2.1(d) – the organisation reasonably believes the use or disclosure is necessary to lessen or prevent a serious threat to life, health, safety or welfare;
- IPP 2.1(e) – the use or disclosure is a necessary part of the organisation's own investigation into reasonably suspected unlawful activity, or in reporting its concerns to relevant persons or authorities;
- IPP 2.1(f) – the use or disclosure is required or authorised by or under law;
- IPP 2.1(g) – the organisation reasonably believes the use or disclosure is reasonably necessary to assist a law enforcement agency to carry out certain law enforcement functions.

7.38 IPP 7.3(b) is narrower in scope than IPP 2.1 as only some of the exceptions contained in IPP 2.1 apply to IPP 7.3(b). Notably, use and disclosure under IPP 2.1(a), (b) and (h) are not included in IPP 7.3(b). If a unique identifier is sought by ASIO and ASIS (under IPP 2.1(h)), organisations should consider if another exception under IPP 7.3(b) applies, for example, the investigation of unlawful activity under IPP 2.1(g) or as permitted by law under IPP 2.1(f).

7.39 The use and disclosure of a unique identifier assigned by another organisation, without the consent of the individual to whom the identifier relates, is not otherwise permitted, whether for public interest research (IPP 2.1(c)) or for reasonably expected related secondary purposes (IPP 2.1(a)). If an organisation wishes to use or disclose another organisation's identifier outside of the law enforcement and public safety context or without authority of law, then it should seek individuals' consent.

IPP 7.3(c): Use or disclosure by consent

7.40 IPP 7.3(c) allows an organisation to use or disclose a unique identifier assigned by another organisation, where it has the consent of the individual to whom the identifier was assigned.

7.41 As with IPP 7.2(b), it is the organisation that wants to use or disclose the identifier that must obtain the individual's consent, not the organisation that assigned the identifier. Similarly, consent must be voluntary, informed, specific, current and given by someone with the capacity to do so. In addition, the individual's consent must be to the particular proposed use or disclosure. General consent for unspecified uses or disclosures is not sufficient.

Case Study 7D: Disclosure of unique identifier with individual's consent

As part of its recruitment process, an organisation conducted police checks on job applicants. To do so, the organisation was required to collect a copy of applicants' driver's licences, which contained a unique identifier issued to the individual by another organisation (the licencing body).

When collecting this information, the organisation sought the applicants' consent for the licence information – including the unique identifier – to be disclosed to other parties for the purpose of conducting the police check.

The organisation engaged an external party to undertake the police checks on its behalf. This meant the organisation was required to disclose the unique identifier assigned to the individual (i.e., the applicant) by the licencing body to the third party undertaking the police check.

The disclosure of the unique identifiers assigned to the individuals by another organisation (the licencing body) was permitted under IPP 7.3 because the organisation had obtained the individuals' consent to disclose the information for the specific purpose of conducting a police check.

IPP 7.4: Requiring identifiers to be provided in order to obtain a service

7.42 IPP 7.4 states an organisation must not require an individual to provide a unique identifier to obtain a service unless:

- the provision of the unique identifier is required or authorised by law; or
- the provision is in connection with the purpose (or a directly related purpose) for which the unique identifier was assigned.

7.43 Like other sections in IPP 7, IPP 7.4 aims to prevent a particular unique identifier being adopted across government and becoming a de facto universal identity number. More specifically, IPP 7.4 seeks to prevent organisations from forcing individuals to provide their identifiers by threatening to otherwise withhold services. Organisations must not make service delivery conditional upon individuals providing a unique identifier unless they have authority under law, or the identifier is relevant to the purpose for which it was assigned.

7.44 For example, a university may require a student to provide their student identity number to access various student services such as library borrowing, a sports facility or counselling services. In this case, the identity number is relevant to establishing the student's eligibility to access services provided by or on behalf of the university. However, making services such as library borrowing or use of gym facilities conditional on a student providing their driver's licence number is likely to be prohibited by IPP 7 because a driver's licence number is not assigned for these purposes.

7.45 Organisations that require individuals using or accessing a service to provide a unique identifier should consider whether the organisation's service is connected to the reason for which the identifier was assigned, and if so, how. For example, how is the organisation's service related to

being eligible to drive (in the case of a drivers' licence), to travel (in the case of a passport) or to receive health benefits (in the case of Medicare or health care cards)? If there is no connection, organisations should consider whether they have authority under law to require individuals to provide a unique identifier in exchange for a service.

Case Study 7E: Demanding residents provide identity card numbers to obtain electronic access cards unnecessary and excessive⁷

A property management company in a private housing estate installed electronic readers that required residents to have a door access card or door key to enter the building. Residents applying for a door access card had to register their names, telephone numbers, and Hong Kong Identity Card numbers with the management company. One resident objected to the collection of his identity number and complained to the Hong Kong Privacy Commissioner.

The property management company argued it was necessary to collect the number to prevent any harm to residents and damage or loss on the part of the company in case the access card fell into the wrong hands. If that occurred, the company would be able to identify the resident and seek an indemnity for any claims that might be made by a victim of some crime.

The Hong Kong Privacy Commissioner found the possibility and extent of damage or loss speculated by the management company should be realistically justified. If an access card were misused for criminal purposes, the management company would be able to identify or trace the responsible cardholder through the original flat owner who had applied for the card or take action directly against the flat owner where appropriate. The Privacy Commissioner considered it was unnecessary and excessive to collect the identity card numbers of all residents simply because an electronic door access system was installed.

- 7.46 If the provision of a unique identifier is not relevant or legally authorised, organisations should not require individuals seeking to use or access a service to produce such identification. This includes situations where an organisation uses identity documents as 'security' while someone is using a service. IPP 7.4 prohibits an organisation from demanding identifiers be provided regardless of whether the organisation subsequently records the information.
- 7.47 The excessive and unnecessary collection of unique identifiers may also be contrary to an organisation's obligations under IPP 1 which requires the collection of personal information be minimised to what is necessary, fair and not unreasonably intrusive. Also, in some cases, requiring the provision of a unique identifier in exchange for a service may also be contrary to [IPP 8 \(Anonymity\)](#).

⁷ Collection of identity card numbers of residents applying for electronic entrance cards by property management company, Case No. ar0405-2 [2004] HKPrivCmr 2.

IPP 7 in practice

Is an email address a unique identifier?

- 7.48 In practice, email addresses assigned by Victorian public sector organisations are not ordinarily be ‘unique identifiers’ for the purposes of Part 3 of the PDP Act. Although an email address can reveal an individual’s identity, they are usually assigned to individuals by organisations to manage and facilitate electronic communications.
- 7.49 However, like any other piece of information about an individual, an email address may become a unique identifier if it is assigned by an organisation with this purpose. A single identifier may be assigned multiple times and for multiple purposes. An email address may be assigned initially to facilitate communication but if an organisation later uses that email address as a unique identifier, for example to identify an individual when cross matching data, then IPP 7 may apply. This applies to other identifiers, not only email addresses. Organisations should avoid using email addresses as unique identifiers, so they do not subsequently need to handle those email addresses in accordance with IPP 7.

Data matching and the IPPs

- 7.50 Organisations considering data matching should think about the potential for obligations under IPP 7 to arise. Often, an obligation under the IPPs will not arise in isolation. In the context of data matching, organisations should consider how their obligations under IPP 7 will interact with other obligations under other IPPs.⁸
- 7.51 Transparency and notice will be essential in any data matching exercise. Organisations should consider their obligations under IPPs 1.3, 1.5, 5.1 and 5.2. Further, where data matching is likely to lead to the aggregation of information or profiles of individuals, IPP 1 requires the collection of data is minimised to what is necessary, fair and not unreasonably intrusive. The reason for data matching should be communicated clearly to affected individuals in terms that are not overly technical or legalistic and any collection or re-use of data should be lawful and clearly authorised (under IPP 1.2 and IPP 2).
- 7.52 IPP 7 aims to balance the potential privacy invasiveness of data matching, linking and profiling with the clear benefits to organisations in assigning or adopting identifiers to efficiently administer their functions. An individual may consent to the adoption, use or disclosure of a unique identifier under IPPs 7.2 and 7.3 respectively. Seeking the meaningful consent of an individual before adopting or using or disclosing unique identifiers promotes transparency and gives individuals greater control over their personal information in data matching. The potential for agencies to unnecessarily collect identity documents or identifiers is reduced by the necessity tests in IPPs 7.1, 7.2 and 7.3 and the requirement of relevant or separate legislative authority in IPP 7.4. Where appropriate, organisations should refer to the discussion of ‘consent’ and ‘necessary’ in the [Key Concepts chapter](#).

Is a code assigned to de-identify an individual a unique identifier?

- 7.53 In some contexts, identifiers may be used instead of names to de-identify individuals. For example, an individual’s file may be assigned a number or other unique identifier so it can be shared with others in the organisation while allowing the individual to remain unnamed. In this situation, the number assigned is not a ‘unique identifier’ because it is not assigned for the purpose of identifying the individual. On the contrary, it is assigned to obscure the individual’s identity. An assigned code

⁸ For more information see [‘Unique Identifiers under the PDP Act’](#).

may have two purposes, for example, to uniquely identify an individual, and for administrative purposes. What matters is the purpose: a code used for the purpose of uniquely identifying an individual is a unique identifier.

Please send any queries or suggested changes to privacy@ovic.vic.gov.au. We will respond to privacy enquiries and consider your suggestions when we next update the Guidelines to the Information Privacy Principles.

Version control table

Version	Description	Date published
IPP 7 – Unique Identifiers 2019.B	Edits following consultation.	14 November 2019
IPP 7: Unique Identifiers 2019.A	Consultation draft.	16 May 2019
IPP 7: Unique Identifiers (2011)	2011 pdf version.	2011