

Guide to De-identifying Information

Privacy and Data Protection Act 2014

De-identified Information

Information Privacy Principle 4 of the *Privacy and Data Protection Act 2014* (PDPA), requires that personal information be securely destroyed or de-identified if it is “no longer required for any purpose”. The following sets out guidance regarding how to de-identify information which needs to be retained.

De-identified information or de-identified data, is information that cannot be linked to any individual and is therefore not regulated by the PDPA or the *Health Records Act 2001* (HRA).

The difference between “anonymous” and “de-identified” information

“Anonymous information” does not contain an individual’s name, however, the individual it relates to, may still be indirectly identified. For example, the anonymous information may contain very detailed descriptions that allow the person’s identity to be guessed, or, include information that can be linked to a particular person.

Separate pieces of information, when linked together, may describe an individual, such as eye colour, height, telephone number, postcode or job position. This full “data set” would fall within the definition of ‘personal information’ for the purposes of the PDPA and the HRA.

“De-identified information” has had all the identifying data, such as, name, pin number, address, images etc., removed from it. It can be aggregated into statistical information but does not provide any clues or links to an individual (see below).

What is de-identification?

The process of de-identification consists of modifying and/or manipulating information or recorded opinion about an individual, so that, the individual’s identity is no longer apparent and cannot “reasonably be ascertained” from the information or opinion.

How to assess whether a person’s identity can reasonably be ascertained

The following questions help in deciding whether an individual’s identity can ‘reasonably be ascertained’:

- Is the information about a group of people or one specific individual?
- Is the group of individuals large enough to afford obscurity?
- Are there any obvious identifying details contained in the information such as name, photo or physical description?
- Does the information contain any unique identifiers, assigned specifically to the individual, such as client identification number?
- Does the information include data that, when combined, will allow the individual to be recognised, such as name, address and telephone number?
- Is it likely, that people who have access to the information will know, or know about, the person, it relates to?
- Is it likely that the information, when combined with publically available information will identify a person?

The more personal characteristics present in the information under consideration, the more ‘identifying’ the information is likely to be, and so, the greater the risk of the person’s identity being “reasonably ascertained”.

Guide to De-identifying information

Minimising the possibility of identification from information

The risk that a person can be identified through a particular record, or description, can vary depending on a number of factors:

- Who has access to the information – are they likely to know the individual personally?
- Do any of the people in the information have a high public profile, so are more likely to be recognisable by others, who do not know them personally?
- Can a person be identified by combining the information with other easily obtained data items, or using other sources, such as unique identifiers, publicly available telephone numbers or email addresses?
- Does the information contain a lot of detail?
- Is the information accumulated over time, thereby becoming more detailed and potentially identifying?
- How many people have access to an index that connects names to any unique identifiers (numbers or codes assigned to an individual such as a “Pin”).

Further advice

For further information about de-identifying personal information or data, please contact:

INSERT FOR YOUR AGENCY