

TITLE NON-IDENTIFYING HEALTH INFORMATION	STANDARD # IPO-2013-0004
PARENT POLICY Delegation of Authority and Responsibilities for Compliance for HIA and FOIP Policy 1108	APPROVED August 6, 2014
APPROVING AUTHORITY Chief Privacy Officer	LAST UPDATE
DEPARTMENT/DIVISION Legal & Privacy	NEXT REVIEW
CONTACT Chief Privacy Officer	TELEPHONE

If you have any questions or comments regarding the information in this guideline please contact AHS Information & Privacy Office at Privacy@albertahealthservices.ca .

PURPOSE

- To provide guidance on what is non-identifying health information and when and how it may collected, used or disclosed.
- To ensure compliance with the *Health Information Act*

GUIDELINES

1. Alberta Health Services has a duty to collect, use or disclose health information with the highest degree of anonymity possible and in a limited manner as required to carry out the intended purpose. (HIA s.57, 58).
2. The principle of the highest degree of anonymity does not apply to the collection, use or disclosure of health information when it is for the purpose of providing health services, or determining or verifying the eligibility of an individual to receive a health service.
3. Affiliates of Alberta Health Services must limit the collection, use or disclosure of health information by applying the 'need to know principle', that is, the collection, use or disclosure is essential to provide access to the information to enable the affiliates to carry out their duties.



PRIVACY GUIDELINE	APPROVED / REVISED DATE	STANDARD #	PAGE
NON-IDENTIFYING HEALTH INFORMATION	August, 2014	IPO #2013- 0004	2 of 5

4. To consider health information as non-identifying it should be very difficult for the information owner or any other person to identify the person in question by using all means that are reasonably at their disposal. This includes using any existing technical means to be able to link aggregated data to the identity of the individual persons. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identify.
5. For purposes of this standard there are three types of non-identifying health information: anonymous, aggregate and de-identified.
6. Anonymous health information is where the identification of the individual was not collected in the first place; there are no identifiers held by Alberta Health Services. This may occur when Alberta Health Services conducts 'person on the street' surveys and does not collect identifiers. This information may be collected by, used by and disclosed to any person for any purpose.
7. Aggregate health information is information about groups of individual with common characteristics. This is often referred to as statistical information and is the kind of information from which it is very difficult to identify a single individual unless the cell or sample size is very small (less than 10) and some additional context is provided.
8. De-identified health information is where data elements that could identify an individual were initially collected but have been removed so that it would be very difficult to "re-identify" the patient.
9. When Alberta Health Services intends to collect, use or disclose health information, it must first consider whether collection, use or disclosure of aggregate health information is adequate for the intended purpose. If so, Alberta Health Services must collect, use, or disclose only aggregate health information.
10. If Alberta Health Services believes that collecting, using or disclosing aggregate information is not adequate for the intended purpose, Alberta Health Services must then consider whether collection, use, or disclosure of other non-identifying health information is adequate for the intended purpose. If so, Alberta Health Services may collect, use or disclose other non-identifying information.
11. Alberta Health Services may transform individually identifying health information into de-identified health information.

PRIVACY GUIDELINE	APPROVED / REVISED DATE	STANDARD #	PAGE
NON-IDENTIFYING HEALTH INFORMATION	August, 2014	IPO #2013- 0004	3 of 5

12. In compliance with the highest degree of anonymity principle under the *Health Information Act*, Alberta Health Services has a duty to change, strip, encode or otherwise transform individually identifying health information into de-identifying health information where its end use of the information does not require information about the identity about an individual.

13. Information may become de-identifying by stripping the identifying health information of its personal identifiers, by not providing contextual information, and by not undertaking data matching.

14. The following data elements are considered to be identifiers and all of these elements must be stripped from the identifying health information to convert it to non-identifying health information:
 1. Names (including initials).
 2. All geographic subdivisions smaller than a province, including street address, city, county, precinct, postal code, and their equivalent geographical codes, except for the initial three digits of a postal code if, according to the current publicly available data from the Census Bureau:
 - a. The geographic unit formed by combining all postal codes with the same three initial digits contains more than 20,000 people.
 - b. The initial three digits of a postal Code for all such geographic units containing 20,000 or fewer people are changed to 000.
 3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
 4. Telephone numbers.
 5. Fax numbers.
 6. Electronic mail addresses.
 7. Social insurance numbers.
 8. Medical record numbers.
 9. Health plan beneficiary numbers (i.e. PIN, ULI).
 10. Account numbers.
 11. Certificate/license numbers.
 12. Vehicle identifiers and serial numbers including license plate numbers.
 13. Device identifiers and serial numbers.
 14. Web universal resource locators (URLs).
 15. Internet protocol (IP) addresses.
 16. Biometric identifiers, including fingerprints and voice prints.
 17. Full-face photographic images and any comparable images.

PRIVACY GUIDELINE	APPROVED / REVISED DATE	STANDARD #	PAGE
NON-IDENTIFYING HEALTH INFORMATION	August, 2014	IPO #2013- 0004	4 of 5

15. Information may also be considered to be non-identifying if a person determines and certifies that the risk is very small that the information could be used by a recipient, alone or in combination with other reasonably available information, to identify an individual. The person making this determination must be someone with appropriate knowledge of, and experience with, generally accepted statistical and scientific principles and methods for rendering information not individually identifiable by using a statistical verification method. The person making this determination must document the basis for such determination. For use of a statistical verification method, please confer with AHS Information & Privacy Office.

16. When disclosure is to a researcher and where the information being disclosed is non-identifying health information, a researcher is allowed to apply a unique but meaningless number or code for control purposes as long as the code is not related to or derived from information about the individual and is not otherwise capable of being translated to identify the individual.

17. Health information which has been de-identified according to this standard may still be vulnerable to re-engineering of the identities of the individuals. As this information is still governed by the *Health Information Act*, this type of non-identified health information must be protected as confidential information. To mitigate this risk Alberta Health Services may undertake an agreement with the recipient which compels the recipient to protect the information as confidential, to promise not to re-engineer the identity of the patients or contact the patients and to use the information only for the purposes for which it is being disclosed.

18. If Alberta Health Services discloses non-identifying health information to a person that is not a custodian under the *Health Information Act*, then Alberta Health Services must inform the person that they must notify the Commissioner of the Office of the Information and Privacy of an intention to use the information for data matching before performing the data matching. This applies to all disclosures including disclosures to researchers.

CROSS-REFERENCES

- Delegation of Authority and Responsibilities for Compliance for HIA and FOIP Policy 1108
- *Health Information Act* (Alberta)

GLOSSARY (see Glossary standard for any other terms)

“Non-Identifying” means that the identity of the individual who is the subject of the information cannot be readily ascertained from the information. The *Health Information Act*

PRIVACY GUIDELINE	APPROVED / REVISED DATE	STANDARD #	PAGE
NON-IDENTIFYING HEALTH INFORMATION	August, 2014	IPO #2013- 0004	5 of 5

regulates information that identifies individuals. The *Health Information Act* contains a few basic provisions restricting the use of non-identifiable information.”

“**Aggregate Health Information**” means non-identifying health information about groups of individual with common characteristics. This is often referred to as statistical information and often is the kind of information from which it is virtually impossible to identify a single individual unless the cell or sample size is very small (less than 10).

“**Anonymity**” refers to the characteristic of being non-identifying. That is, the identity of the individual to whom it pertains cannot be readily ascertained.

“**Confidential**” “implies a trust relationship between the person supplying information and the individual or organization collecting it. The relationship is built on the assurance that the information will only be used by or disclosed to authorized persons or to others with the individual’s permission. Protecting the confidentiality of health information implies that individually identifying health information is concealed from all but authorized parties.”

“**Data Matching**” means the creation of individually identifying health information by combining individually identifying or non-identifying health information or other information from 2 or more electronic databases, without the consent of the individuals who are the subjects of the information.

“**De-identified Health Information**” means information where there is a very small probability of identifying an individual.