

## DHHS POLICIES AND PROCEDURES

---

<b>Section VIII:</b>	<b>Privacy and Security</b>
<b>Title:</b>	<b>Privacy Manual</b>
<b>Chapter:</b>	<b>Use and Disclosure Policies, De-Identification of Health Information and Limited Data Sets</b>
<b>Current Effective Date:</b>	<b>5/1/05</b>
<b>Revision History:</b>	<b>6/27/03</b>
<b>Original Effective Date:</b>	<b>4/14/03</b>

---

### **Purpose**

The purpose of this policy is to define methods by which the North Carolina Department of Health and Human Services (NC DHHS) agencies may remove specific elements from health information so the resulting information will not be considered individually identifying health information. De-identified information can be used or disclosed without employing privacy protections.

***This policy shall apply to the following DHHS agencies:***

- *The Health Insurance Portability and Accountability Act (HIPAA) covered health care components and*
- *Internal business associates*

### **Background**

An individual identifier is information that could reasonably enable the identification of a specific DHHS client or a relative, guardian, employer, or household members of that client. HIPAA Privacy Rule primarily addresses the protection of individually identifiable health information and specifies when such information can be used or disclosed. HIPAA allows a covered entity to de-identify health information by removing all identifying elements so that the remaining information cannot identify an individual and therefore is not subject to the protections specified for individually identifiable health information.

In addition to de-identifying health information, HIPAA permits the creation of a “limited data set” that can contain specific individual identifiers when such information is needed for public health, research, or health care operations activities and a “data use agreement” (DUA) has been executed. There are provisions in HIPAA, state laws, and other federal laws when individually identifying health information can be used and disclosed for public health, research, and health care operations without the necessity for a limited data set or data use agreement (e.g., public health disclosures required by law, licensure surveys). Therefore, data use agreements would only be needed for those public health, research, or health care operation uses and disclosures that are not otherwise permitted by federal or state laws.

## Policy

DHHS agencies shall de-identify health information whenever individually identifying health information is not necessary to accomplish the intended purpose for the use or disclosure of health information or when use or disclosure of individually identifying health information is not permitted by federal or state laws.

When use or disclosure of individually identifying health information is necessary for public health, research, or health care operation activities, and the particular instance of use or disclosure is not permitted by federal or state laws, each DHHS agency will determine if a limited data set would meet the intended purpose of the use or disclosure. When a limited data set is deemed appropriate, DHHS agencies shall enter into a data use agreement with the recipient of the information. Data use agreements that do not conform to the [DHHS Data Use Agreement](#) must be submitted for review/approval by the DHHS Privacy Officer, after which any DUAs that substantially deviate from the template will be forwarded to the attorney general's office for review and approval.

DHHS agencies shall comply with all conditions in this policy regarding the creation, use, and disclosure of health information for which the elements that could reasonably be expected to identify a specific individual have been removed or restricted to a limited data set. Each DHHS agency that is a recipient of a limited data set must sign a data use agreement and shall comply with the conditions of that agreement. A DHHS agency may use the limited data set for its own activities or operations provided that the information used is the minimum necessary to accomplish the intended purpose.

This policy shall apply to *paper* documents as well as *electronic* data in any form (e.g., paper or electronic records, system data, tape, disc, etc.)

When information cannot be de-identified or included in a limited data set, the agency shall ensure that disclosure of the health information is permitted by law and is in accordance with DHHS Privacy Policies.

## Implementation

### Individual Identifiers

For the purposes of DHHS Privacy Policies, the following elements are considered individual identifiers if they apply to DHHS clients or relatives, guardians, employers, or household members of DHHS clients. If the elements below are associated with health information, the information becomes individually identifying health information that must be protected from improper use or disclosure:

- Names

- All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geo codes, except for the initial three (3) digits of a zip code if, according to the current publicly available data from the bureau of the census:
  - The geographic unit formed by combining all zip codes with the same three (3) initial digits contains more than 20,000 people; and
  - The initial three (3) digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
- 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;
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social Security Numbers (SSN);
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code that can be re-identified.

## De-Identification

Individually identifiable health information is de-identified when elements have been removed that could identify an individual and there can be no reasonable basis to believe that the information may be used, with or without other available information, to identify an individual. De-identified health information may be used and shared as necessary in the performance of an agency's work, unless the information is otherwise restricted by federal or state laws.

Such health information may be considered de-identified only if the following criteria are met:

---

<b>Section VIII:</b>	<b>Privacy and Security</b>	<b>Page 3 of 11</b>
<b>Title:</b>	<b>Privacy Manual</b>	
<b>Chapter:</b>	<b>Use and Disclosure Policies, De-Identification of Health Information and Limited Data Sets</b>	
<b>Current Effective Date:</b>	<b>5/1/05</b>	

---

- The agency is unaware of a means by which the information could be used alone or in combination with other information to identify an individual who is the subject of the information; **and** a person with appropriate knowledge and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable (e.g., statistician I or II):
  - Determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is the subject of the information; and
  - Documents the methods and results of the analysis that justify such determination; **or**
- The identifiers (listed above) of the client or relatives, guardians, employer, or household members of that client are removed.

An agency may engage an internal or external business associate to serve as the qualified person with “appropriate knowledge and experience with generally accepted statistical and scientific principles and methods” to de-identify information. (Note: Several DHHS divisions, facilities and schools employ individuals with statistical background/experience who may be able to provide this type of service.) The use of the disclosed data and the recipients of the data shall be considered in the risk assessment conducted by the qualified person. An agency that uses an internal or external person to satisfy this de-identification criteria shall develop a procedure to verify that the individual adequately meets the knowledge and experience criteria.

Health information that has been considered de-identified does not meet the de-identification criteria if either of the following is true:

- A code or other means of record identification designed to enable coded or otherwise de-identified information to be re-identified is provided; or
- De-identified information is re-identified.

#### Limited Data Set

DHHS agencies may use or disclose individually identifying health information that contains a limited number of identifiers (i.e., *limited data set*) for public health, research, or health care operation activities whenever the limited data set will meet the intended purpose for the use or disclosure. When a limited data set is deemed appropriate for a use or disclosure, DHHS agencies will enter into a data use agreement, using the [DHHS Data Use Agreement](#), with the recipient of the information unless the use or disclosure is permitted by state or federal law, which negates the need for such an agreement.

When limited data sets are used or disclosed with an appropriate data use agreement executed:

- An authorization is not required for the use or disclosure of a limited data set; and
- Limited data sets do not need to be included in an accounting of disclosures.

To qualify as a limited data set, the following identifiers for DHHS clients or relatives, guardians, employers, or household members of those clients can be associated with health information:

- State, county, city or town, zip code, SSN;
- Birth date, admission date, discharge date, date of death;
- Age; and/or
- Unique identifying number, characteristic, or code exclusive of identifiers such as SSN, account numbers, medical record numbers, etc., as listed in the *Exclusion of Data Elements* section below.

Exclusion of Data Elements Considered to be Identifying Elements

The table below outlines the identifiers that must be **excluded** from individually identifying health information in order to consider the information as de-identified or as a limited data set. (See [Appendix A](#) for a list of all elements that can be **included** in de-identified information or a limited data set.)

<b>DATA ELEMENTS THAT MUST BE <u>EXCLUDED</u> TO BE CONSIDERED DE-IDENTIFIED DATA OR A LIMITED DATA SET</b>		
<b>ELEMENTS</b>	<b>DE-IDENTIFIED ELEMENTS</b>	<b>LIMITED DATA SET ELEMENTS</b>
<b>Names</b> of clients or employers, household members, guardians or relatives of clients.	X	X
<b>Street address or post office box number</b> of clients or employers, household members, guardians or relatives of clients.	X	X
<b>County, city, town or precinct</b> of clients or employers, household members, guardians or relatives of clients	X	
<b>State</b> of clients or employers, household members, guardians or relatives of clients.		
<b>First three (3) digits of the zip code</b> of clients or employers, household members, guardians or relatives of clients <b>if, according to the bureau of census, the population of all zip codes with the same first three (3) digits is greater than</b>		

<b>DATA ELEMENTS THAT MUST BE <u>EXCLUDED</u> TO BE CONSIDERED DE-IDENTIFIED DATA OR A LIMITED DATA SET</b>		
<b>ELEMENTS</b>	<b>DE-IDENTIFIED ELEMENTS</b>	<b>LIMITED DATA SET ELEMENTS</b>
<b>20,000 people</b> e.g., if the population of all zip codes that begin with 276 is more than 150,000, you can include 276 in de-identified health information.		
<b>First three (3) digits of the five (5) digit zip code</b> of clients or employers, household members, guardians or relatives of clients <b>if, according to the bureau of census, the population of the all zip codes with the first three (3) digits is less than 20,000 people</b> e.g., the total population for all zip codes starting with 211 – say 21101 and 21104 – is 19,200 people. In this case, you could not use the first three (3) digits of the zip code in de-identified health information.	X	
<b>Last two (2) digits of the zip code</b> of clients or employers, household members, guardians or relatives of clients.	X	
<b>Five (5) digit zip code</b> of clients or employers, household members, guardians, or relatives of clients e.g., the five (5) digit zip code of 27603 must be excluded from de-identified data, but can be included in a limited data set.	X	
<b>Dates exclusive of year</b> (e.g., month/day) directly related to a client including admission date, discharge date, date of death.	X	
<b>Birth date exclusive of year</b> (e.g., month/day) for clients age 89 and under.	X	
<b>Birth date inclusive of year</b> (e.g., month/day/year) for clients age 90 and above (not aggregated – e.g., 1880-1913).	X	
<b>Age 89 and under.</b>		
<b>Specified ages 90 or above</b> (not aggregated – e.g., 90+).	X	
<b>Telephone numbers</b> of clients or employers, household members, guardians, or relatives of clients.	X	X
<b>Fax numbers</b> of clients or employers, household members, guardians, or relatives of clients.	X	X
<b>Electronic mail addresses</b> of clients or employers, household members, guardians, or relatives of clients.	X	X
<b>SSN</b> of clients or employers, household members, guardians, or relatives of clients.	X	X
<b>Medical record numbers</b> of clients or employers, household members, guardians, or relatives of clients.	X	X
<b>Health plan beneficiary numbers</b> of clients or employers, household members, guardians or relatives of clients.	X	X
<b>Account numbers</b> of clients or employers, household members, guardians or relatives of clients.	X	X

<b>DATA ELEMENTS THAT MUST BE <u>EXCLUDED</u> TO BE CONSIDERED DE-IDENTIFIED DATA OR A LIMITED DATA SET</b>		
<b>ELEMENTS</b>	<b>DE-IDENTIFIED ELEMENTS</b>	<b>LIMITED DATA SET ELEMENTS</b>
<b>Certificate/license numbers</b> of clients or employers, household members, guardians or relatives of clients.	X	X
<b>Vehicle identifiers and serial numbers</b> , including license plate numbers, of clients or employers, household members, guardians or relatives of clients.	X	X
<b>Medical device identifiers and serial numbers</b> of clients or employers, household members, guardians or relatives of clients.	X	X
<b>Web Universal Resource Locators (URLs)</b> of clients or employers, household members, guardians or relatives of clients.	X	X
<b>Internet Protocol (IP) address numbers</b> of clients or employers, household members, guardians or relatives of clients.	X	X
<b>Biometric identifiers</b> , including finger and voice prints of clients or employers, household members, guardians or relatives of clients.	X	X
<b>Full face photographic images</b> and any comparable images of clients or employers, household members, guardians or relatives of clients.	X	X
<b>Any other unique identifying number, characteristic or code</b> (unless such code is developed in accordance with the <i>Re-Identification</i> section of this policy).	X	
<b>Gender, race, ethnicity or marital status</b>		

### Re-Identification

An agency may assign a code or other means of identification to allow information that has been de-identified to be re-identified *within the agency*, provided that:

- The code or other means of identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual (examples would be codes containing a SSN or the unique ID algorithm assigned to clients served in facilities operated by the Division of Mental Health, Developmental Disabilities, and Substance Abuse Services);
- The agency does not use or disclose the code (or other means of identification) for any purpose other than that originally intended; and

- The agency does not disclose any methods that can be used to re-identify information that has been de-identified.

### Data Use Agreement

DHHS agencies that use or disclose a limited data set, wherein the use or disclosure is not permitted by state or federal law, the agency shall enter into a data use agreement with the limited data set recipient(s) consistent with the [DHHS Data Use Agreement](#) provided by the department. The data use agreement must contain the following:

- A requirement to use or disclose such information only for the purposes of research, public health or health care operation activities;
- Specifications regarding who can use or receive the limited data set;
- Specifications of the permitted uses and disclosures;
- A stipulation that the recipient will not use or disclose the limited data set for any purposes other than those specified in the data use agreement or as otherwise required by law;
- Adequate assurances that the recipient will use appropriate safeguards to prevent the use or disclosure of the limited data set for any purposes other than those specified in the data use agreement. These assurances may be addressed through language similar to that provided in the [DHHS Data Use Agreement](#) ;
- Commitment by the recipient to report to the agency any use or disclosure of the information not provided for by the data use agreement of which it becomes aware;
- Assurance that any agent, including a subcontractor, to whom the recipient provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and
- A commitment by the recipient that they will not re-identify the information or contact any of the individuals whose data is being disclosed.

If an agency staff member becomes aware of a pattern of activity or practice of the limited data set recipient that constitutes a material breach or violation of the recipient’s obligation under the data use agreement, the staff member shall notify that agency’s privacy official who shall take reasonable steps to cure the breach or end the violation. If unsuccessful, the agency privacy official shall ensure that disclosure of limited data sets to the recipient is discontinued. The agency privacy official shall report the problem to the DHHS Privacy Officer, who will determine if further actions are warranted which could include reporting the material breach to the Secretary of the US Department of Health and Human Services.

The minimum necessary rule shall apply to limited data sets; therefore, only data elements that are necessary to perform the purpose(s) specified in the data use agreement should be included in the limited data set released to the recipient.

## Implementation Activities

Each agency shall identify those areas within the agency that may use or disclose health information that includes any of the identifiers specified in this policy for purposes other than treatment or payment or when authorized by the client. Each agency shall ensure that staff in these areas understand:

- The elements that constitute identifiers;
- The potential for use or disclosure of limited data sets when data use agreements are in place; and
- That there are specific laws that must be adhered to when using or disclosing individually identifying health information.

A business associate who has entered into an approved Business Associate Agreement with the DHHS agency may be engaged for the purpose of converting individually identifiable health information into de-identified health information or a limited data set.

Each agency shall develop a procedure to ensure compliance with this policy regarding de-identified health information and limited data sets. This procedure shall include oversight, which may be centralized and/or may include a committee review, as well as procedures for coding and re-identifying individually identifying health information that are in accordance with the coding requirements in this policy.

If time constraints prohibit the immediate creation of de-identified health information, these circumstances shall be documented and provided to the agency privacy official. When practicable, these issues shall be resolved to enable de-identification for future comparable occurrences.

## Reference

DHHS Directive Number III-11; 45 CFR 164.514

**Relevant Document:** [DHHS Data Use Agreement](#)

*For questions or clarification on any of the information contained in this policy, please contact [DHHS Privacy Officer](#). For general questions about department-wide policies and procedures, contact the [DHHS Policy Coordinator](#).*

## Appendix A – Elements Permitted in De-identified Health Information and Limited Data Sets

The table below lists the elements that **can** be included in de-identified health information. The table also identifies those data elements, including some individual identifiers that are allowed to be included in a limited data set. Note that the individual identifiers that can be included in a limited data set are not likely to identify an individual if no additional individual identifiers are used.

<b>IDENTIFYING DATA ELEMENTS THAT CAN BE INCLUDED IN DE-IDENTIFIED DATA OR A LIMITED DATA SET</b> (“X” indicates that the element can be included)		
<b>ELEMENTS</b>	<b>DE-IDENTIFIED ELEMENTS</b>	<b>LIMITED DATA SET ELEMENTS</b>
<b>ADDRESS</b>		
<b>County, city, town or precinct</b> of clients or employers, household members, guardians or relatives of clients.		X
<b>State</b> of clients or employers, household members, guardian or relatives of clients.	X	X
<b>First three (3) digits of the zip code</b> of clients or employers, household members, guardians or relatives of clients <b>if, according to the bureau of census, the combined population of all zip codes with the same first three (3) digits is <u>greater than</u> 20,000 people.</b>	X	X
<b>First three (3) digits of the five (5) digit zip code</b> of clients or employers, household members, guardians or relatives of clients <b>if, according to the bureau of census, the combined population of the all zip codes with the first three (3) digits is <u>less than</u> 20,000 people.</b>		X
<b>Five (5) digit zip code</b> of clients or employers, household members, guardians, or relatives of clients.		X
<b>DATES</b>		
<b>Year of client-related dates</b> , including admission date, discharge date and date of death.	X	X
<b>Dates exclusive of year (month/day)</b> directly related to a client, including admission date, discharge date and date of death.		X
<b>Year of birth</b> for clients age 89 and under.	X	X
<b>Year of birth</b> for clients age 90 and above.		X

