
Title:	DPH Privacy and Security Manual
Chapter:	III. Use and Disclosure Policies, De-Identification of Health Information and Limited Data Sets
Current Effective Date:	November 1, 2004
Original Effective Date:	April 14, 2003
Revision History:	October 15, 2004

Purpose

The purpose of the Division of Public Health (DPH) de-identification of health information and limited data sets is to define the methods by which Divisions covered components may remove specific elements from health information so the resulting information will not be considered individually identifiable health information (IIHI). De-identified information can be used or disclosed without being subject to the protections specified for IIHI. This policy is in compliance with the [DHHS Policy and Procedure Manual, Section VIII, Security and Privacy](#), that establishes the NC Department of Health and Human Services (DHHS) de-identification of health information and limited data sets requirements.

Policy Scope:

- ***HIPAA covered health care components***
- ***Internal Business Associates***

Background

An individual identifier is information that could reasonably enable the identification of a specific DPH client or a relative, guardian, employer, or household members of that client. The Health Insurance Portability and Accountability Act (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 IIHI.

The HIPAA definition of completely de-identified health information is not the same as what many providers, program managers, and researchers have been familiar with as de-identified data. The HIPAA de-identification strips out all geographical subdivision smaller than a state, including zip codes, and as such, HIPAA de-identified data may not be sufficient for many research studies nor for public health data analysis and reporting.

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 that authorize when IHI 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).

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

DPH covered components and internal business associates shall de-identify health information whenever IHI is not necessary to accomplish the intended purpose for the use or disclosure of health information or when the use or disclosure of IHI is not permitted by federal or state laws. The Division will establish an oversight committee to review the method(s) used to de-identify health information, to provide guidelines for de-identification, and to review periodically the practices used for de-identification.

Division work groups that are not HIPAA covered components or internal business associates should continue to follow their guidelines and protocols for de-identifying data according to the NC statutory and administrative rule requirements. To further protect IHI, division work groups may enter into data use agreements with other organizations to provide assurances to the data sources regarding the use and disclosure of their Protected Health Information

In situations where a provider or research entity requests a DUA, the DPH work group can use HIPAA-compliant [DPH Data Use Agreement Template](#) as the basis for developing the DUA. The DPH work group can also use a standard HIPAA-compliant DUA provided by the covered entity. These DUAs should be reviewed by the DPH HIPAA Office before entering into the DUA.

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 Division covered component 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, DPH covered components shall enter into a data use agreement with the recipient of the information. The Division has developed a [DPH Data Use Agreement Template](#) that conforms to the DHHS Data Use Agreement template.

DPH covered components 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 DPH work group 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 Division work group 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, DPH covered components shall ensure that disclosure of the health information is permitted by law and is in accordance with DHHS and DPH Privacy Policies. Exceptions to this policy should be referred to the Division Privacy Officer for help in resolving de-identification issues.

Implementation

The following section provides details about HIPAA-defined individual identifiers, limited data sets, data use agreements, and the data elements that can and cannot be included in limited data sets.

Individual Identifiers

For the purposes of DPH Privacy Policies, the following elements are considered individual identifiers if they apply to DPH clients or relatives, guardians, employers, or household members of DPH clients. If the elements below are associated with health information, the information becomes IHI 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 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 initial digits contains more than 20,000 people; and
 - The initial three 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
- 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
- Any other unique identifying number, characteristic, or code that can be re-identified

"Limited Data Sets and De-Identified Data Sets", by NCHICA provides a quick reference guide.

De-Identification

IIHI 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 a covered components' work, unless federal or state laws otherwise restrict the information.

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

- 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 methods* and scientific principles 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**
- **All** identifiers (listed above) of the client or relatives, guardians, employer, or household members of that client are removed.

A covered component may engage an internal or external business associate (such as the State Center for Health Statistics) to serve as the qualified person with “appropriate knowledge and experience with generally accepted statistical and scientific principles and methods” to de-identify information. 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 these de-identification criteria shall develop a procedure to verify that the individual adequately meets the knowledge and experience criteria.

The Division will establish an oversight committee to review, when necessary, the methods covered components and internal business associates use to de-identify data. This committee will establish general guidelines for de-identification and will review periodically the de-identification methods used with the Division.

At a minimum, the committee will consist of representatives from the following:

- State Center for Health Statistics, including Cancer Registry and Birth Defects Monitoring Program
- Epidemiology, including General Communicable Disease
- Office of Legal and Regulatory Affairs
- DPH HIPAA Office

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

DPH work groups may use or disclose IHHI 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, DPH work groups will enter into a data use agreement, using the [DPH Data Use Agreement Template](#), 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 DPH clients or relatives, guardians, employers, or household members of those clients **can** be associated with health information:

- State, county, city or town, ZIP Code;
- Birth date, admission date, discharge date, date of death;
- Age; and/or
- Unique identifying number, characteristic, or code exclusive of identifiers such as Social Security Numbers, 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 IHI in order to consider the information as de-identified or as a limited data set.

DATA ELEMENTS THAT MUST BE EXCLUDED TO BE CONSIDERED DE-IDENTIFIED DATA OR A LIMITED DATA SET		
ELEMENTS	DE-IDENTIFIED ELEMENTS	LIMITED DATA SET ELEMENTS
Names of clients or employers, household members, guardians, or relatives of clients	X	X
Street address or post office box number of clients or employers, household members, guardians, or relatives of clients	X	X
County, city, town, or precinct of clients or employers, household members, guardians, or relatives of clients	X	
State of clients or employers, household members, guardians, or relatives of clients		
First three digits of the ZIP Code of clients or employers, household members, guardians or relatives of clients if, according to the Bureau of Census, the population of all ZIP Codes with the same first three digits is greater than 20,000 people. 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.		
First three digits of the five digit ZIP Code of clients or employers, household members, guardians or relatives of clients if, according to the Bureau of Census, the population of the all ZIP Codes with the first three digits is less than 20,000 people. 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 digits of the ZIP Code in de-identified health information.	X	
Last two digits of the ZIP Code of clients or employers, household members, guardians or relatives of clients	X	
Five digit ZIP Code of clients or employers, household members, guardians, or relatives of clients. E.g., the five digit ZIP Code of 27603 must be excluded from de-identified data, but can be included in a limited data set.	X	
Dates exclusive of year (e.g., Month/Day) directly related to a	X	

DATA ELEMENTS THAT MUST BE EXCLUDED TO BE CONSIDERED DE-IDENTIFIED DATA OR A LIMITED DATA SET		
ELEMENTS	DE-IDENTIFIED ELEMENTS	LIMITED DATA SET ELEMENTS
client including admission date, discharge date, date of death		
Birth date exclusive of year (e.g., Month/Day) for clients age 89 and under	X	
Birth date inclusive of year (e.g., Month/Day/Year) for clients age 90 and above (not aggregated – e.g., 1880-1913)	X	
Age 89 and under		
Specified Ages 90 or above (not aggregated – e.g., 90+)	X	
Telephone numbers of clients or employers, household members, guardians, or relatives of clients	X	X
Fax numbers of clients or employers, household members, guardians, or relatives of clients	X	X
Electronic mail addresses of clients or employers, household members, guardians, or relatives of clients	X	X
Social Security Numbers of clients or employers, household members, guardians, or relatives of clients	X	X
Medical record numbers of clients or employers, household members, guardians, or relatives of clients	X	X
Health plan beneficiary numbers of clients or employers, household members, guardians, or relatives of clients	X	X
Account numbers of clients or employers, household members, guardians, or relatives of clients	X	X
Certificate/license numbers of clients or employers, household members, guardians, or relatives of clients	X	X
Vehicle identifiers and serial numbers , including license plate numbers, of clients or employers, household members, guardians, or relatives of clients	X	X
Medical device identifiers and serial numbers of clients or employers, household members, guardians, or relatives of clients	X	X
Web Universal Resource Locators (URLs) of clients or employers, household members, guardians, or relatives of clients	X	X
Internet Protocol (IP) address numbers of clients or employers, household members, guardians, or relatives of clients	X	X
Biometric identifiers , including finger and voice prints of clients or employers, household members, guardians, or relatives of clients	X	X

Title: Privacy and Security Manual

Page 8 of 13

Chapter: III. Use and Disclosure Policies, De-Identification of Health Information and Limited Data Sets

Current Effective Date: February 10, 2004

DATA ELEMENTS THAT MUST BE <u>EXCLUDED</u> TO BE CONSIDERED DE-IDENTIFIED DATA OR A LIMITED DATA SET		
ELEMENTS	DE- IDENTIFIED ELEMENTS	LIMITED DATA SET ELEMENTS
Full face photographic images and any comparable images of clients or employers, household members, guardians, or relatives of clients	X	X
Any other unique identifying number, characteristic, or code (unless such code is developed in accordance with the <i>Re-Identification</i> section of this policy)	X	
Gender, race, ethnicity, or marital status		

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.

IDENTIFYING DATA ELEMENTS THAT CAN BE INCLUDED IN DE-IDENTIFIED DATA OR A LIMITED DATA SET (‘X’ indicates that the element can be included)		
ELEMENTS	DE- IDENTIFIED ELEMENTS	LIMITED DATA SET ELEMENTS
ADDRESS		
County, city, town, or precinct of clients or employers, household members, guardians, or relatives of clients		X
State of clients or employers, household members, guardians, or relatives of clients	X	X
First three digits of the ZIP Code of clients or employers, household members, guardians or relatives of clients if, according to the Bureau of Census, the combined population of all ZIP Codes with the same first three digits is greater than 20,000 people	X	X
First three digits of the five digit ZIP Code of clients or employers, household members, guardians or relatives of clients if, according to the Bureau of Census, the combined population of the all ZIP Codes with the first three digits is less than 20,000 people		X
Five digit ZIP Code of clients or employers, household members, guardians, or relatives of clients		X
DATES		
Year of client-related dates , including admission date, discharge date, and date of death	X	X
Dates exclusive of year (Month/Day) directly related to a client, including admission date, discharge date, and date of death		X
Year of birth for clients age 89 and under	X	X
Year of birth for clients age 90 and above		X
Aggregated years of birth for clients age 90 and over (e.g., 1880-1913)	X	X

IDENTIFYING DATA ELEMENTS THAT CAN BE INCLUDED IN DE-IDENTIFIED DATA OR A LIMITED DATA SET (‘X’ indicates that the element can be included)		
ELEMENTS	DE- IDENTIFIED ELEMENTS	LIMITED DATA SET ELEMENTS
AGE		
Age 89 and under	X	X
Ages 90 or above (not aggregated – e.g., 90 or 98)		X
Aggregated ages , including ages 90 and over (e.g., 5-15 or 90-105)	X	X
OTHER		
Any other unique identifying number, characteristic, or code (unless such code is developed in accordance with the <i>Re-Identification</i> section of this policy) that is not one of the following: Social Security Number Medical record number Account numbers Certificate/license numbers IP address numbers Telephone number Vehicle IDs/serial numbers Medical device IDs/serial numbers Health plan beneficiary number Fax numbers		X
Gender, race, ethnicity, or marital status	X	X

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 Division work group*, 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
- The DPH work groups does not use or disclose the code (or other means of identification) for any purpose other than that originally intended; and
- The DPH work group does not disclose any methods that can be used to re-identify information that has been de-identified.

Data Use Agreement

Division work groups that use or disclose a limited data set, wherein state or federal law does not permit the use or disclosure, the work group shall enter into a data use agreement with the limited data set recipient(s) consistent with the [DPH Data Use Agreement Template](#) 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 [DPH Data Use Agreement Template](#);
- 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 a DPH 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 the DPH Privacy Official who shall take reasonable steps to cure the breach or end the violation. If unsuccessful, the DPH Privacy Official shall ensure that disclosure of limited data sets to the recipient is discontinued. The DPH 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.

Processing Data Requests

The DHHS HIPAA Office and the North Carolina Healthcare Information Alliance (NCHICA) Privacy Workgroup have prepared quick reference guidelines to follow when reviewing requests for data. This material includes a flow chart with narrative describing the decision process and a table that lists the data elements that can included in and must be excluded from a limited data set.

The guidelines are *Guidelines for Processing Data Requests*, *Processing Data Requests* (flow chart), and *Limited Data Sets and De-Identified Data Sets*.

Relevant Forms: [DPH Data Use Agreement Template](#)

These documents can be accessed on the DPH HIPAA website at <http://www.schs.state.nc.us/hipaa/>.

References: DHHS Directive Number III-11; DHHS Policy and Procedure Manual, Section VIII, Security and Privacy, DPH HIPAA Compliance Statement, 45 CFR 164.514, NC General Statutes 130A-131.17, NC General Statutes 130A-143, NC General Statutes 130A-374, NC General Statutes 130A-9310A, NC General Statutes-130A-212, 10A NCAC 46C.0106, 10A NCAC 41A.0104, 10A NCAC 47A.0102, 10A NCAC 41H0702, 10A NCAC 47B.0106, 10A NCAC 43G.0409

For questions or clarification on any of the information contained in this policy, please contact the DPH Privacy Office at <mailto:HIPAA.DPH@ncmail.net>.