Administrative Policies & Procedures

Subject: **De-identification and Re-identification of Protected Health Information**	Section: **Health Information**	**Policy #:**
Cross Reference:	**Issued For:** ☒ Mayo Clinic, Jacksonville ☒ St. Luke's Hospital	
Content Manager: **Approved by Mayo Jacksonville Administrative Committee Date:** _____	**Effective Date: January 2003** **Next Review Date:** **Revision Dates:**	

PURPOSE:
To provide guidance for workforce members at Mayo Clinic Jacksonville, St. Luke's Hospital and Mayo Primary Care Centers (collectively referred to as "Mayo") regarding the appropriate de-identification and re-identification methods.

POLICY:
If records are de-identified, they are no longer considered individually identifiable health information and can be used or disclosed freely without a patient's authorization

DEFINITION:
Patient information is "de-identified" if sufficient key items have been removed such that it is no longer individually identifiable and cannot be used, alone or in combination with other reasonably available information, to identify the individual patient.

PROCEDURE:

A. De-identification

To de-identify records, all of the following information must be removed:

(A) Names;

(B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

(*1*) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and

(*2*) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

(C) 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;

(D) Telephone numbers;

(E) Fax numbers;

(F) Electronic mail addresses;

(G) Social security numbers;

(H) Medical record numbers;

(I) Health plan beneficiary numbers;

(J) Account numbers;

(K) Certificate/license numbers;

(L) Vehicle identifiers and serial numbers, including license plate numbers;

(M) Device identifiers and serial numbers;

(N) Web Universal Resource Locators (URLs);

(O) Internet Protocol (IP) address numbers;

(P) Biometric identifiers, including finger and voice prints;

(Q) Full face photographic images and any comparable images; and

(R) Any other unique identifying number, characteristic, or code, except for an algorithmic derivation code or an encoded security code that could allow for the record to be re-identified using the key.

B. Statistical Evaluation

If a person with appropriate statistical knowledge concludes the risk is "very small" that the information could be used to identify an individual, it may be treated as not individually identifiable. Contact the Privacy Officer for guidance on statistical evaluation.

C. Limited Data Set

If the de-identification requirements render the data unusable for the intended purpose, a "limited data set" could be created for certain purposes. A limited data set can be used to disclose information for the purposes of research, public health, or health care operations provided a "Data Use Agreement" is put in place before the information is disclosed. For assistance with a Data Use Agreement, contact the Privacy Officer.

A limited data set is individually identifiable health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

(A) Names;

(B) Postal address information, other than town or city, State, and zip code;

(C) Telephone numbers;

(D) Fax numbers;

(E) Electronic mail addresses;

(F) Social security numbers;

(G) Medical record numbers;

(H) Health plan beneficiary numbers;

(I) Account numbers;

(J) Certificate/license numbers;

(K) Vehicle identifiers and serial numbers, including license plate numbers;

(L) Device identifiers and serial numbers;

(M) Web Universal Resource Locators (URLs);

(N) Internet Protocol (IP) address numbers;

(O) Biometric identifiers, including finger and voice prints; and

(P) Full face photographic images and any comparable images.

D. Data Use Agreement

A Data Use Agreement must:

(A) Establish the permitted uses and disclosures of the information by the limited data set recipient. The data use agreement may not authorize the limited data set recipient to use or further disclose the information in a manner that would jeopardize the confidentiality of the information.

(B) Establish who is permitted to use or receive the limited data set; and

(C) Provide that the limited data set recipient will:

(1) Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;

(2) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;

3) Report to Mayo any use or disclosure of the information not provided for by its data use agreement of which it becomes aware;

(4) Ensure that any agents, including a subcontractor, to whom it 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

(5) Not identify the information or contact the individuals.