

Sec. 164.514 Other requirements relating to uses and disclosures of protected health information.

- (e) (1) Standard: Limited data set. A covered entity may use or disclose a limited data set that meets the requirements of paragraphs (e)(2) and (e)(3) of this section, if the covered entity enters into a data use agreement with the limited data set recipient, in accordance with paragraph (e)(4) of this section.
- (2) Implementation specification: Limited data set: A limited data set is protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:
  - (i) Names;
  - (ii) Postal address information, other than town or city, State, and zip code;
  - (iii) Telephone numbers;
  - (iv) Fax numbers;
  - (v) Electronic mail addresses;
  - (vi) Social security numbers;
  - (vii) Medical record numbers;
  - (viii) Health plan beneficiary numbers;
  - (ix) Account numbers;
  - (x) Certificate/license numbers;
  - (xi) Vehicle identifiers and serial numbers, including license plate numbers;
  - (xii) Device identifiers and serial numbers;
  - (xiii) Web Universal Resource Locators (URLs);
  - (xiv) Internet Protocol (IP) address numbers;
  - (xv) Biometric identifiers, including finger and voice prints; and
  - (xvi) Full face photographic images and any comparable images.
- (3) Implementation specification: Permitted purposes for uses and disclosures.
  - (i) A covered entity may use or disclose a limited data set under paragraph (e)(1) of this section only for the purposes of research, public health, or health care operations.
  - (ii) A covered entity may use protected health information to create a limited data set that meets the requirements of paragraph (e)(2) of this section, or disclose protected health information only to a business associate for such purpose, whether or not the limited data set is to be used by the covered entity.
- (4) Implementation specifications: Data use agreement.
  - (i) Agreement required. A covered entity may use or disclose a limited data set under paragraph (e)(1) of this section only if the covered entity obtains satisfactory assurance, in the form of a data use agreement that meets the requirements of this section, that the limited data set recipient will only use or disclose the protected health information for limited purposes.
  - (ii) Contents. A data use agreement between the covered entity and the limited data set recipient must:
    - (A) Establish the permitted uses and disclosures of such information by the limited data set recipient, consistent with paragraph (e)(3) of this section. The data use agreement may not

authorize the limited data set recipient to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity;

- (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 the covered entity 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.

(iii) Compliance.

- (A) A covered entity is not in compliance with the standards in paragraph (e) of this section if the covered entity knew of a pattern of activity or practice of the limited data set recipient that constituted a material breach or violation of the data use agreement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful:
  - (1) Discontinued disclosure of protected health information to the recipient; and
  - (2) Reported the problem to the Secretary.
- (B) A covered entity that is a limited data set recipient and violates a data use agreement will be in noncompliance with the standards, implementation specifications, and requirements of paragraph (e) of this section.