

## PURPOSE

---

To provide guidance for the de-identification of PHI, the re-identification of de-identified Information, and to outline the process for reviewing and responding to requests for de-identification of Protected Health Information (PHI) for University of Arizona (UA) Health Care Components (HCCs) in accordance with 45 CFR §§ 164.502 and 164.514.

## REVIEW/REVISIONS

---

- 06/2015

## REFERENCES AND RELATED FORMS

---

- HIPAA Privacy Program Form P (Request for De-Identification of PHI)
- HIPAA Privacy Program Form Q (Is it PHI?)
- HIPAA Privacy Program Procedure 220 (Uses and Disclosures of Protected Health Information—Authorization Required)

## GUIDANCE

---

1. Uses and Disclosures of De-identified Information:
  - a. When possible or practical, HCCs should use and disclose de-identified information when conducting health care operations; however, HCCs are not required to de-identify PHI for health care operations.
  - b. Only HCC personnel, and third party Business Associates with whom the HCC has contracted, may de-identify health information or use the health information to create Limited Data Sets. If a third-party Business Associate is used for this purpose, then there must be a Business Associate Agreement in place with such third-party.
  - c. HCCs may use de-identified Information for a number of purposes, including, but not limited to research purposes.
  - d. HCCs may use PHI to create de-identified information, or disclose PHI to a Business Associate to create de-identified information, for use by:
    - i. UA;
    - ii. A Business Associate; or
    - iii. Another valid requestor.
  - e. If HCCs cannot use or disclose PHI for a particular purpose and believes that removing identifiers is excessively burdensome, it can:
    - i. Choose not to release the PHI;
    - ii. Consider use of a Limited Data Set (see HIPAA Privacy Program Procedure 180 (Limited Data Sets and Data Use Agreements); or
    - iii. Seek an Authorization from the individual for the use and disclosure of PHI including some or all of the identifiers (see HIPAA Privacy Program

Procedure 220 (Uses and Disclosures of Protected Health Information— Authorization Required)).

2. Creating De-identified Information:

- a. Statistical Method: a person with appropriate knowledge and experience applying generally accepted statistical and scientific principles and methods for rendering information not individually identifiable makes a determination that the risk is very small that the information could be used, either by itself or in combination with other reasonably available information, by anticipated recipients to identify a subject of the information; and documents the methods and results that justify this determination.
- b. Safe Harbor Method: all of the following identifiers of the patient, relatives, employers, or household members of the patient, are removed;
  - i. Names (special note: in order to meet the Safe Harbor method for de-identification, the following may not be used: patient initials, first name or last name);
  - ii. Address: street address, city, county, precinct, ZIP code, and their equivalent geocodes. Exception for ZIP codes: The initial three digits of the ZIP Code may be used, if according to current publicly available data from the Bureau of the Census: The geographic unity 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'. (Note: The 17 currently restricted 3-digit ZIP codes to be replaced with '000' include: 036, 059, 063, 102, 203, 556, 692, 790, 821, 823, 830, 831, 878, 879, 884, 890, and 893.)
  - iii. All elements of dates (except year) for dates directly related to an individual including:
    1. Birth date;
    2. Admission date;
    3. Discharge date;
    4. Date of death; and
    5. All ages over 89 and all elements of dates (including year) indicative of such age. Such ages and elements may be aggregated into a single category of age 90 or older.
  - iv. Telephone numbers;
  - v. Facsimile numbers;
  - vi. Electronic mail addresses;
  - vii. Social security numbers;
  - viii. Medical record numbers;
  - ix. Health plan beneficiary numbers;
  - x. Account numbers;
  - xi. Certificate/license numbers;

- xii. Vehicle identifiers and serial numbers, including license plate numbers;
  - xiii. Device identifiers and serial numbers;
  - xiv. Web Universal Resource Locators (URL's);
  - xv. Internet Protocol (IP) address numbers;
  - xvi. Biometric identifiers, including finger and voice prints;
  - xvii. Full face photographic images and any comparable images; and
  - xviii. Any other unique identifying number, characteristic, or code; except a code used for re-identification purposes;
  - xix. And the HCC does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is the subject of the information.
3. Software: If a HCC uses specialized software to de-identify PHI or re-identify information, access by Workforce members to the software will be governed by UA policies and procedures on information security and privacy, including, but not limited to:
- a. Access Controls;
  - b. Password management;
  - c. Media Controls;
  - d. Physical safeguards; and
  - e. Confidentiality and privacy of PHI.
4. Processing Requests for De-identified Information: Requests for De-identified Information must be in writing and submitted to the AHSC Data Warehouse and/or the HIPAA Privacy Officer or his/her designee. The request for de-identified Information must be reviewed, approved or denied by the appropriate personnel designated by the HCC. See Form P: Request for De-identified Information for a form the HCC may use for implementing this policy. Written requests must include the following information:
- a. Requestor information (name, address, telephone numbers, title, organization or department);
  - b. Date of request;
  - c. Purpose of the request;
  - d. Names of all anticipated recipients of the de-identified Information;
  - e. Record parameters or selection criteria (time period included, minimum number of patient records, type of patient records);
  - f. Date the recipient requires the de-identified Information;
  - g. A statement assuring the recipient will not give, sell, loan, show or disseminate the de-identified Information to any other parties without the express written permission of the HCC;
  - h. A statement assuring the recipient will not link de-identified data to any other data the recipient may have access to, where the linked data identifies individual patients. For example, linking de-identified data from the HCC with publicly available census data and the linking reveals the identity of individual patients; and

- i. A statement assuring the recipient will not contact any patient, or their relatives, employers, or other household members that may accidentally be identified by the recipient.
5. Denials: The request for de-identified Information may be denied if:
  - a. The HCC cannot de-identify the PHI;
  - b. The requestor refuses to agree to the required statements on the request form;
  - c. The recipient refuses to compensate the HCC for generating the de-identified Information; or
  - d. It is an imposition to the operations of the HCC.
6. Approvals: HCCs must designate appropriate personnel to whom approved requests should be routed for creating the de-identified Information.
  - a. The designated personnel must use one of the approved methods for de-identifying PHI. The de-identified Information must be accompanied by a statement certifying that either:
    - i. The risk is very small that the information could be used, either by itself or in combination with other reasonably available information, by anticipated recipients to identify a subject of the information; **or**
    - ii. All identifiers of the patient, or relatives, employers, or household members of the patient, are removed; **and**
    - iii. The HCC does not have actual knowledge that the de-identified Information could be used alone or in combination with other reasonably available information to identify an individual who is subject of the information.
  - b. The de-identified Information must be delivered to the approved recipient upon approval of the HIPAA Privacy Officer or other designated person.