HIPAA De-identification Checklist

See also Policy 3.12 De-identifying PHI

When is this used? To de-identify information that contains Protected Health Information (PHI).

Why is this used? UF staff may use or disclose health information that is de-identified without restriction under HIPAA’s Privacy Rule.

Identifiers to be Removed

- Names (including initials)
- Dates: All elements of dates (except year) for dates directly related to an individual
  - Birth date and Death Date
  - Admission and Discharge dates
  - Clinic Visit Dates
  - All ages over 89, unless aggregated into a single category of age 90 and older
- Addresses (All geographic subdivisions smaller than a state)
  - Street address
  - City
  - County
  - Zip code (May use first three digits of a ZIP Code if the geographic unit formed by combining all ZIP Codes with the same three initial digits contains more than 20,000 people. The initial three digits of a ZIP Code for all such geographic units containing 20,000 or fewer people are changed to 000.)
- Telephone numbers.
- Fax numbers.
- E-mail addresses.
- Social Security numbers.
- Medical record numbers.
- Account numbers.
- Health plan beneficiary numbers.
- Certificate/license numbers.
- Vehicle identifiers and serial numbers, including license plate numbers.
- Device identifiers and serial numbers.
- Web URLs.
- Internet protocol (IP) address.
- Biometric identifiers, including fingerprints and voiceprints.
- Full-face and other identifiable photographic images and any comparable images
- Any other unique identifying number, characteristic, or code (unless otherwise permitted by the Privacy Rule for re-identification) that could lead to the identification of the individual.
  - Some examples include clinical trial record number, barcode, revealing occupation, unique condition or publicized clinical event

Please contact the Privacy Office for help with de-identifying protected health information.