**Cabinet for Health and Family Services (CHFS)**

**Office of Application & Technology Services (OATS) Standards:**

**Category: 5000 Controls Domain**

**5200- Data Masking and De-Identification**

**Scope:**

[CHFS Privacy Policy: CHFS Personally Identifiable Information (PII) used in Testing, Training, and Research](https://www.chfs.ky.gov/agencies/os/oats/polstand/Privacy-%20PII%20in%20Testing%20Training%20and%20Research.pdf) requires PII and PHI data used outside the production environment to be de-identified.

**Definitions**

**De-Identification:** The process by which records have had enough PII or PHI removed or obscured such that the remaining information does not identify an individual, and there is no reasonable basis to believe that the information can be used to identify an individual. De-identification is a technique or process applied to a dataset to prevent or limit certain types of privacy risks to individuals, protected groups, and establishments while still allowing for the production of aggregate statistics if needed. This can be achieved by data masking or obscuring the data. De-identified data cannot be re-identified.

**Data Masking:** The process of systematically removing a field and replacing it with a value in a way that does not preserve the analytic utility of the value, such as replacing a phone number with asterisks or a randomly generated pseudonym, or replacing a person's name with a unique identifier, thereby making it difficult to link data to specific individuals directly. If data masking is used and a key or table is kept for re-identification purposes, the data is not de-identified.

**Obscured Data:** The process in which the data has been distorted by cryptographic or other means to hide information. It is also referred to as being obfuscated. An example could be transforming an email address into a non-decipherable string of characters, preserving data structure while eliminating the actual sensitive data. If data can be decrypted, either intentionally or because of a weak algorithm or encryption key, it is not de-identified.

**Re-Identification:** The process by which data is rendered distinguishable by using a code, algorithm, or pseudonym that is assigned to individual records.

**Approved Standard for Data De-Identification(s):**

Personally Identifiable Information (PII)

* [NIST Special Publication 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)](https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-122.pdf) (April 2010)

Protected Health Information (PHI) and Electronic Protected Health Information (ePHI)

* [Guidance on De-identification of Protected Health Information](https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf) (November 2012)

**Exceptions**:

If the PII or PHI data did not achieve a full de-identification, or if de-identified data can be re-identified and will be used in a non-production environment, an exception must be submitted and follow [070.203 Security Exceptions and Exemptions to CHFS OATS Policies and Security Controls Policy](https://www.chfs.ky.gov/agencies/os/oats/polstand/070203SecurityExceptionsandExemptions.pdf).

If data is being de-identified by masking or obscuring, CHFS Security must be informed to review and approve the method being used.

**Approved Product(s) for New Applications:**

IBM Optim

**Exceptions:**

Any exceptions to this standard must follow the procedures established in CHFS IT Policy #070.203.

**Review Cycle:**

Annually

**Timeline:**

Last reviewed: 01/31/2024

Next review: 01/02/2025

**Cross Reference:**

[CHFS Privacy Policy: CHFS Personally Identifiable Information (PII) used in Testing, Training, and Research](https://www.chfs.ky.gov/agencies/os/oats/polstand/Privacy-%20PII%20in%20Testing%20Training%20and%20Research.pdf)

[NIST Special Publication 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)](https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-122.pdf)

[Guidance on De-identification of Protected Health Information](https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf)

https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf

**Link to all COT Software Domain Standards:**

[KITS\_Report.pdf (ky.gov)](https://cgp.ky.gov/sites/COTPUBDOCS/Standards/KITS_Report.pdf)

**Link to all CHFS IT Standards:**

[CHFS IT Standards - Cabinet for Health and Family Services (ky.gov)](https://chfs.ky.gov/agencies/os/oats/Pages/itstandards.aspx)

**Link to all CHFS IT Policies:**

[CHFS IT Policies - Cabinet for Health and Family Services (ky.gov)](https://chfs.ky.gov/agencies/os/oats/Pages/ITpolicies.aspx)