

**Commonwealth of Kentucky**  
Cabinet for Health and Family Services



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



**CHFS Collection, Use, and Retention of Personal  
Information Policy**

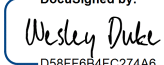

**Version 2.1  
05/13/2024**

CHFS Collection, Use, and Retention of Personal Information Policy	Current Version: 2.1
Category: Policy	Review Date: 05/13/2024

## Revision History

Date	Version	Description	Author
06/08/2021	1.0	Original Document	CHFS Privacy Program- OHDA
05/13/2024	2.1	Review	CHFS Privacy Program- OLS
05/13/2024	2.1	Revision	CHFS Privacy Program- OLS

## Sign-Off

Sign-off Level	Date	Name	Signature
CHFS General Counsel (or delegate)	5/24/2024	Wesley Duke	DocuSigned by:  D58FF6B4FC274A6...
CHFS Chief Privacy Officer (or delegate)	5/28/2024	Kathleen Hines	DocuSigned by:  E27E1B3456DA43D...

CHFS Collection, Use, and Retention of Personal Information Policy	Current Version: 2.1
Category: Policy	Review Date: 05/13/2024

# Table of Contents

## Table of Contents

- 1 POLICY DEFINITIONS.....4**
- 2 POLICY OVERVIEW.....6**
  - 2.1 PURPOSE .....6
  - 2.2 SCOPE .....6
  - 2.3 MANAGEMENT COMMITMENT.....6
  - 2.4 COORDINATION AMONG ORGANIZATIONAL ENTITIES .....6
  - 2.5 COMPLIANCE .....6
- 3 ROLES AND RESPONSIBILITIES .....7**
  - 3.1 AGENCY LIAISONS .....7
  - 3.2 CHIEF INFORMATION SECURITY OFFICER (CISO) .....7
  - 3.1 CHIEF LEGAL COUNSEL / GENERAL COUNSEL .....7
  - 3.2 CHIEF PRIVACY OFFICER (CPO) .....7
  - 3.3 CHFS OATS INFORMATION SECURITY (IS) TEAM .....7
  - 3.4 CHFS CONTRACT, STATE, AND VENDOR STAFF/PERSONNEL .....7
  - 3.5 OHDA EXECUTIVE DIRECTOR .....8
  - 3.6 OHDA GOVERNANCE PROGRAM MANAGER .....**ERROR! BOOKMARK NOT DEFINED.**
- 4 POLICY REQUIREMENTS .....8**
  - 4.1 COLLECTION AND USE OF PERSONALLY IDENTIFIABLE INFORMATION .....8
  - 4.2 ACCESS TO PII .....9
    - 4.2.1. *Workforce Access: CHFS will identify people or classes of people in its workforce who need access to PII, the type of information that is needed, and the conditions for such access. CHFS will limit access to the information which is required for workforce members to carry out their duties, based on the specific needs and roles.....9*
  - 4.3 RETENTION AND DISPOSAL OF PII.....9
    - 4.3.1. *Retention of PII: CHFS will retain each collection of PII for the time period required to fulfill the purpose(s) identified in the notice or as required by law.....9*
- 5 POLICY MAINTENANCE RESPONSIBILITY .....10**
- 6 POLICY REVIEW CYCLE.....10**
- 7 POLICY REFERENCES .....10**



CHFS Collection, Use, and Retention of Personal Information Policy	Current Version: 2.1
Category: Policy	Review Date: 05/13/2024

# 1 Policy Definitions

- **Confidential Data:** Defined by the Commonwealth Office of Technology (COT) Standards Data of which the Commonwealth has a legal obligation not to disclose. This data requires the highest levels of restrictions, because of the risk or impact that will result from disclosure, modifications, breach, or destruction of that data. Examples include: Data not releasable under the Kentucky State Law; Protected Health Information; Federal Tax Information; Social Security and Credit Card numbers.
- **Contract Staff/Personnel:** Defined by CHFS as an employee hired through a state approved (i.e. System Design/Development Services {SDS} Vendor Agreement/Company) vendor who has a master agreement with the state.
- **Electronic Protected Health Information (ePHI):** Defined by the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule as individually identifiable health information, including demographic data, that relates to: the individual's past, present or future physical or mental health or condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual. Personally identifiable health information items include many common identifiers (e.g., name, address, birth date, Social Security Number). The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g.
- **Federal Tax Information (FTI):** Defined by Internal Revenue Service (IRS) Publication 1075 as federal tax returns and return information (and information derived from it) that is in the agency's possession or control which is covered by the confidentiality protections of the Internal Revenue Code (IRC) and subject to the IRC 6103(p) (4) safeguarding requirements including IRS oversight. FTI is categorized as Sensitive but Unclassified information and may contain personally identifiable information (PII). FTI includes return or return information received directly from the IRS or obtained through an authorized secondary source, such as Social Security Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS), or Centers for Medicare and Medicaid Services (CMS), or another entity acting on behalf of the IRS pursuant to an IRC 6103(p) (2) (B) Agreement. FTI includes any information created by the recipient that is derived from federal return or return information received from the IRS or obtained through a secondary source.
- **Personally Identifiable Information (PII):** Defined by Kentucky Revised Statute (KRS) Chapter 61 House Bill 5 (HB5) and in accordance with NIST 800-53 Revision 4 as information which can be used to distinguish or trace the identity of an individual; person's first name or first initial and last name, personal mark, or unique biometric or genetic print or image, in combination with one or more of the following

CHFS Collection, Use, and Retention of Personal Information Policy	Current Version: 2.1
Category: Policy	Review Date: 05/13/2024

data elements: account number, credit card number or debit card number that in combination with any required security code, access code or password would permit access to an account; social security number, taxpayer ID number, driver's license number, state ID number, passport number or other ID number issued by the United States government, or individually identifiable health information, except for education records covered by The Family Educational Rights and Privacy Act of 1974 (FERPA). In addition, HIPAA identifies an individual's full name, date of birth, street or email address, biometric data, and other common identifiers as direct PII that can be used alone, as well as combined with additional fields of information, to uniquely identify an individual.

- Privacy Impact Assessment (PIA):** Defined by CMS Minimum Acceptable Risk Standards for Exchanges (MARS-E) 2.2 as the process and document that is the outcome of the process of identifying privacy risks and methods to mitigate them. PIAs are performed before developing or procuring information systems, or initiating programs or projects that collect, use, maintain, or share PII, and they are updated when changes create new privacy risks. PIAs also are conducted to ensure that programs and information systems comply with applicable legal, regulatory, and policy requirements.
- Sensitive Data:** Defined by COT standards as data that is not legally protected but should not be considered public information and only be disclosed under limited circumstances. Only authorized users should be granted access to sensitive data. Examples include: All information identifiable to an individual including staff, employees, and contractors but not limited to dates of birth, driver's license numbers, employee ID numbers, license plate numbers, and compensation information. The Commonwealth proprietary information including but not limited to intellectual property, financial data and more.
- Sensitive Financial Data (Including PCI):** Defined by Payment Card Industry (PCI) Data Security Standards (DSS) as cardholder and sensitive authentication data including Primary Account Number (PAN), cardholder name, expiration date, service code, full track data (magnetic stripe data or equivalent on a chip), Card Security Codes such as CAV2/CVC2/CVV2/CID, and PIN(s). CHFS also defines sensitive financial data as anything that is inclusive of bank identification/information (i.e. bank routing number, account number, etc.).
- State Staff/Personnel:** Defined by CHFS as an employee hired directly through the state within the CHFS.
- Third Party:** Defined by CHFS as any contracted or government organization that is not a part of the agency's organizational structure. This may include state or federal auditing agencies, state approved security contract vendors or other external organization whose capabilities can be determined sufficient to conduct assessment needs.
- Vendor Staff/Personnel:** Defined by CHFS as an employee contracted through an approved Master Business Associate Agreement, or other formal agreement, to

CHFS Collection, Use, and Retention of Personal Information Policy	Current Version: 2.1
Category: Policy	Review Date: 05/13/2024

provide temporary work for CHFS.

## 2 Policy Overview

### 2.1 Purpose

The CHFS must establish a comprehensive level of privacy controls provided by state and federal regulations to implement through an Accounting of Disclosures and Retention Policy. This document establishes the agency's Accounting of Disclosures and Retention, to manage privacy related risks and provide guidelines for practices regarding accounting of disclosures and retention of disclosures of PII.

### 2.2 Scope

The scope of this policy applies to all internal CHFS state, contract, and vendor staff/personnel, temporary personnel, third party providers under contract with a CHFS agency, and other entities that interact with CHFS information related resources. This policy covers applicable computer hardware, software, application, configuration, business data, and data communication systems.

### 2.3 Management Commitment

Chief Privacy Officer (CPO) and Office of Legal Services General Counsel have reviewed and approved this policy. Senior Management supports the objective put into place by this policy. Violations of not abiding by this policy may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. CHFS shall report illegal activities or theft of CHFS property (physical or intellectual) to the appropriate authorities.

### 2.4 Coordination among Organizational Entities

Office of Legal Services (OLS), Office of Data Analytics (ODA), and Office of Application Technology Services (OATS) coordinate with CHFS organizations and/or agencies that access applications, systems, and facilities. All organizational entities that interact with CHFS are subject to follow requirements outlined within this policy.

### 2.5 Compliance

As official guidance domain for this policy, CHFS agencies abide by the security and privacy requirements established in state laws and regulations as well as federal guidelines outlined in the National Institute of Standards and Technology (NIST). Applicable agencies additionally follow security and privacy frameworks outlined within the Centers for Medicare and Medicaid Services (CMS), the Internal Revenue Services (IRS), and the Social Security Administration (SSA).

CHFS Collection, Use, and Retention of Personal Information Policy	Current Version: 2.1
Category: Policy	Review Date: 05/13/2024

## 3 Roles and Responsibilities

### 3.1 Agency Liaisons

Individuals that serve as representatives of their agencies as members of the CHFS Data Governance Steering Committee and the CHFS Privacy Advisory Council . These individuals are responsible for the decision making process alongside General Counsel, CPO, and ODA for matters related to privacy and data governance. They serve as liaisons between the members of the CHFS Data Governance Steering Committee, Privacy Advisory Council, and members of their respective agencies. These individuals are responsible for adherence to this policy.

### 3.2 Chief Information Security Officer (CISO)

Individual responsible for providing guidance and direction in assessment, planning, and implementation of all security standards, practices, and commitments required. This individual is responsible for adherence to this policy.

### 3.1 Chief Legal Counsel / General Counsel

Individual(s) from the CHFS Office of General Counsel (OGC) responsible for providing legal services at the discretion of the CPO, as well as serving in a legal advisory capacity.

### 3.2 Chief Privacy Officer (CPO)

Individual responsible for overseeing activities related to the development, implementation, maintenance of, and adherence to CHFS and Commonwealth's information privacy and confidentiality policies and procedures in compliance with federal and state laws. This includes continuously analyzing the impact of new and updated regulations and evaluating the organization's privacy compliance status. This individual will conduct HIPAA self-assessments through coordination with the Information Security Agency Representative, the CISO or CHFS Office of Application Technology Services (OATS) Information Security (IS) Team, and other CHFS agencies, and will ensure compliance with HIPAA notification and reporting requirements in the event of an identified incident. The CPO works in conjunction with the Executive Advisor to lead efforts of the privacy subcommittee within the CHFS Data Governance Steering Committee. This position is responsible for adherence to CHFS Privacy Program.

### 3.3 CHFS OATS Information Security (IS) Team

CHFS OATS IS team is responsible for conducting the assessment, planning, and implementation of all security standards, practices, and commitments required.

### 3.4 CHFS Contract, State, and Vendor Staff/Personnel

All CHFS contract, state, and vendor staff/personnel must adhere to this program. All named in this subsection must comply with referenced documents, found in Section



CHFS Collection, Use, and Retention of Personal Information Policy	Current Version: 2.1
Category: Policy	Review Date: 05/13/2024

**Error! Reference source not found. Error! Reference source not found.** below that pertain to the agency's applications, application servers, appliances, operating systems, web servers, network components, and database (server or components) that reside on CHFS/OATS information system(s).

### 3.5 ODA Executive Director

Individual that oversees activities conducted by OHDA Executive Advisor(s). This individual is also responsible for overseeing ODA as a whole, including its functions and ongoing activities. Additionally, this individual is responsible for final approval in any work product of the CHFS Data Governance Steering Committee. This position is responsible for adherence to this program.

## 4 Policy Requirements

CHFS will only collect, use, and disclose Personally Identifiable Information (PII) as authorized by statute, regulation, or Executive Order. Collection of PII will be in accordance with the minimum amount necessary according to applicable laws and regulations, and in accordance with any notice provided to an individual for that purpose. CHFS will limit use of PII to the authorized purposes for which it was collected, and will not use PII in a manner incompatible with those purposes. Any unauthorized collection, use, access, retention, or disclosure of an individual's PII is strictly prohibited and is a violation of CHFS policy.

### 4.1 Collection and Use of Personally Identifiable Information

CHFS will take appropriate steps to limit the collection and use of PII to the minimum amount necessary that CHFS is authorized to collect under law or regulation.

- 4.1.1. Authority and Purpose to Collect: CHFS will identify and document the legal authority and purpose that permits the collection, use, and disclosure of PII, either generally or in support of specific programs and/or needs of information systems.

CHFS will document the purpose for which data will be collected, used, and disclosed in any required privacy notices or compliance documents (for example Privacy Act Notices, Privacy Impact Assessments(PIA), Notices of Privacy Practices (NPP), etc.).

- 4.1.2. Limitation on Collection and Use: CHFS programs that collect PII will identify and document the minimum PII elements that are relevant and necessary to accomplish the purpose of collection.



CHFS Collection, Use, and Retention of Personal Information Policy	Current Version: 2.1
Category: Policy	Review Date: 05/13/2024

Collection and retention of PII will be limited to the minimum elements as referenced in any CHFS Privacy Notice and for which the individual has provided consent, if required.

- 4.1.3. Review of PII Collection: CHFS will conduct a review at least every two years, or more frequently if required by law, to reduce or eliminate unnecessary collection of PII.

## 4.2 Access to PII

- 4.2.1. Workforce Access: CHFS will identify people or classes of people in its workforce who need access to PII, the type of information that is needed, and the conditions for such access. CHFS will limit access to the information which is required for workforce members to carry out their duties, based on the specific needs and roles.

- 4.2.2. Third Party Access: CHFS may share PII externally only for the authorized purposes for which it was collected, as described in the agency's privacy notice(s), or for a purpose authorized by statute or regulation.

Before sharing PII with third parties, CHFS will assess whether sharing is authorized and whether additional or new public notice(s) are required.

- 4.2.3. Third Party Agreements: Where appropriate, CHFS will enter into agreements with third parties to allow access to PII. The agreements will describe the PII involved, and specifically enumerate the purposes for which the PII may be used. These agreements must also comply with all requirements as outlined in the CHFS Business Associates and Third Party Agreements Policy.

## 4.3 Retention and Disposal of PII

- 4.3.1. Retention of PII: CHFS will retain each collection of PII for the time period required to fulfill the purpose(s) identified in the notice or as required by law.

CHFS will follow the Kentucky Department for Library and Archives (KDLA) Record Retention Schedule. Per the schedule, all state government should use the General Schedule for State Agencies which outline scheduling and retention guidelines. CHFS agencies will also use a retention schedule specific to their agency or program if the agency is

CHFS Collection, Use, and Retention of Personal Information Policy	Current Version: 2.1
Category: Policy	Review Date: 05/13/2024

required to keep records for a longer period than required on the General Schedule.

- 4.3.2. Disposal of PII: CHFS will dispose of PII in accordance with the retention schedule as defined by Section 4.3.1 of this policy.

CHFS will use security standards defined by the Commonwealth Office of Technology (COT) and the CHFS Office of Administration and Technology Services (OATS) to ensure secure deletion or destruction of all PII, and in a manner that prevents loss, theft, misuse, or unauthorized access.

## 5 Policy Maintenance Responsibility

The CHFS CPO or designee is responsible for the maintenance of this policy.

## 6 Policy Review Cycle

This policy is reviewed at least biennially and revised on an as needed basis.

## 7 Policy References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.2
- CHFS Business Associates and Third Party Agreements Policy
- CHFS Contractor Privacy and Security of Protected Health, Confidential and Sensitive Information Agreement Form for External Vendors (CHFS-219V)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule
- Internal Revenue Services (IRS) Publications 1075
- Kentucky Information Technology Standards (KITS): 4080 Data Classification Standard
- Kentucky Revised Statue (KRS) Chapter 61.931 *et seq.*
- Kentucky Revised Statute (KRS) Chapter 61.878 Certain public records exempted from inspection except on order of court – Restriction of state employees to inspect personnel files prohibited
- Kentucky Revised Statutes (KRS) Chapter 61.884 Person's access to record relating to him
- Kentucky Revised Statutes (KRS) Chapter 194A.060 Confidentiality of records and reports
- National institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- Social Security Administration (SSA) Security Information