Commonwealth of Kentucky
Cabinet for Health and Family Services

Cabinet for Health and Family Services (CHFS) Privacy Program

KENTUCKY
Cabinet *for* Health *and* Family Services

CHFS Privacy Program

Version 1.0
06/09/2021

Revision History

Date	Version	Description	Author
06/09/2021	1.0	Effective Date	CHFS Privacy Program

Sign-Off

Sign-off Level	Date	Name	Signature
CHFS Secretary	6/8/2021 | 8:55 PM EDT	Eric Friedlander	DocuSigned by: Eric Friedlander 0AEA1D8C15D0431...
OHDA Executive Director (or delegate)	6/8/2021 | 9:31 AM EDT	Robert Putt	DocuSigned by: Robert E. Putt 4BBBFF0DFCEC461...
CHFS Chief Privacy Officer (or delegate)	6/8/2021 | 10:07 AM EDT	Kathleen Hines	DocuSigned by: Kathleen Hines E27E1B3456DA43D...

Table of Contents

1 Program 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, but are not limited to, data not releasable under the Kentucky State Law (Kentucky Revised Statute 61.878); 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 of 1996 (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 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 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 NIST SP 800-53 as an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.
- **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 chip0, 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 with final approval and appointment by the Kentucky Personnel Cabinet.
- **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 provide temporary work for CHFS.

2 Program Overview

2.1 Purpose

The Cabinet for Health and Family Services (CHFS) must establish a comprehensive privacy program to maintain compliance with the applicable laws and regulations, and to outline roles and responsibilities of Cabinet stakeholders responsible for the implementation and maintenance of privacy-related functions. This Program serves as the foundational element in the process of creating a privacy culture within CHFS and will convey CHFS' expectations and initiatives regarding privacy. This document establishes the agency's privacy program that manages risks and provides guidelines for privacy practices regarding the management of privacy controls and requirements.

The Privacy Program is aligned with CHFS' existing policies, procedures, programs, processes, and other applicable documents that verify coverage of privacy requirements.

2.2 Scope

The scope of this program applies to all CHFS state, contract, and vendor staff/personnel, temporary personnel employees, third party providers under contract with a CHFS agency, and other entities that interact with CHFS information related resources.

2.3 Management Commitment

The Chief Privacy Officer (CPO) and Office of Health Data and Analytics (OHDA) Executive Director have reviewed and approved this program, and Senior Management supports the objective this program endeavors to achieve. Violations of policies that are part of the Privacy Program 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. CHFS allocates appropriate budget and personnel resources to implement and operationalize this program.

2.4 Coordination among Organizational Entities

OHDA coordinates with organizations and/or agencies that access applications, systems, and facilities. All organizational entities that interact with CHFS are subject to follow the requirements of this program.

2.5 Compliance

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

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 Privacy Subcommittee. These individuals are responsible for the decision making process alongside Executive Director, CPO, and Executive Advisor for matters related to privacy and data governance. They serve as liaisons between the members of the CHFS Data Governance Steering Committee, Privacy Subcommittee, and members of their respective agencies. These individuals are responsible for adherence to this program.

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 program.

3.3 Chief Legal Counsel / General Counsel

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

3.4 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.

3.5 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.

3.6 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 7 Program References 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).

3.7 OHDA Executive Director

Individual that oversees activities conducted by CPO and OHDA Executive Advisors. This individual is also responsible for overseeing OHDA 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.

3.8 OHDA Governance Program Manager

Individual who works with OHDA Executive Director to lead various programs within OHDA. This individual is responsible for analyzing health data, data-sharing agreements, and decision-making processes as part of the CHFS Data Governance Steering Committee. This position is responsible for adherence to this program.

4 Program Overview

4.1 Laws and Regulations

Federal laws, Executive Orders, agency regulations, Governor's Office Directives, and Commonwealth Statutes govern CHFS' mission, business, and Privacy Strategic Planning. The mission/business process for CHFS Privacy Program is reviewed and approved by executive management, including the CPO and Executive Director. Reviews and updates of the mission/business process are conducted when a major change occurs in the CHFS environment as a result of, but not limited to, Federal laws, Executive Orders, agency regulations, Governor Directives, Commonwealth Statutes, emerging information security threats/vulnerabilities, and the impact of new technologies.

CHFS has developed a CHFS Privacy Framework to provide a cross-walk of the CPO approved authoritative sources with NIST 800-53 Revision 4. This framework is designed to support the operationalization of future state privacy priorities and initiatives, including the development of policies, procedures, and processes.

The framework can be accessed using a governance tool or other comparable method and should be reviewed annually or when the CPO identifies additional authoritative sources. Updates to the framework should be reviewed by Privacy Subcommittee and obtain final approval from OHDA.

4.2 Privacy and Data Governance

Governance refers to the process of establishing rules, executing the organizational vision, and decision-making for the betterment of organizational goals. Within CHFS, privacy and data governance is a key component for the establishment of the Privacy

Program and consists of various executives and members from throughout the Cabinet. Privacy Governance includes, but is not limited to:

- **Organizational Privacy Strategy**: Overall strategy pertaining to data sensitivity and privacy within CHFS.
- **Policies & Procedures**: Establishment and implementation of policies and procedures for enhancing privacy considerations within CHFS, while complying with applicable laws and regulations to protect the privacy of users, employees, and vendors for whom CHFS has personal information.
- **Training & Awareness**: Privacy focused awareness materials such as flyers and posters, as well as dedicated privacy training for CHFS employees.
- **Metrics & Monitoring**: Risk-centric approach to privacy that involves the development of metrics to ensure the effectiveness of privacy governance efforts, conducting periodic privacy impact assessments, monitoring privacy risk controls, and reporting results to executives for insight and awareness.
- **Data Sharing & Data Sharing Agreements**: Process of identifying the sensitivity level of data, the ability to share that data with third-parties and internal CHFS agencies, and maintaining a data inventory. Additionally, determining the limitations on which data can be shared, the restrictions on how it can be used if it is shared, and validating if agreements are already in place or new agreements must be created. The Office of General Counsel, CPO, and Data Owners, and others, as designated are responsible for approving the data sharing agreements.

CHFS has integrated privacy governance activities within the overarching agency structure and activities by ensuring appropriate participation by officials to oversee the implementation of privacy controls throughout the agency.

Figure 1 below provides an illustrative view of the structure of the CHFS Data Governance Steering Committee.

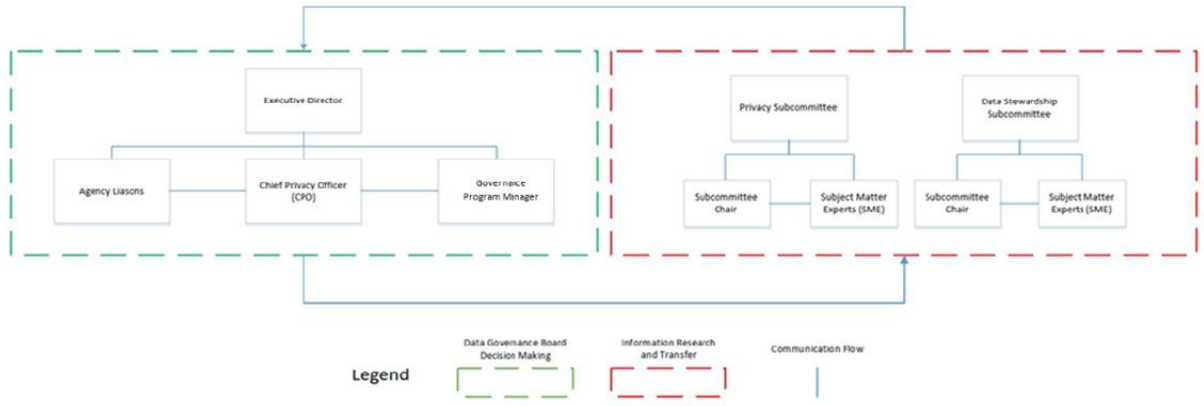

Figure 1 – CHFS Data Governance Steering Committee Structure

The OHDA is responsible for governing matters pertaining to privacy and data governance within CHFS. Agencies within CHFS interact with the CHFS Data Governance Steering Committee to implement privacy functions within their respective jurisdictions. The purpose of the CHFS Data Governance Steering Committee is to assist with data collection, restrictions, retention, stewardship, and consistency across CHFS.

The CHFS Data Governance Steering Committee has a collaborative model in which subcommittees, subject matter experts (SME's), and the subcommittee chair work with the CHFS Data Governance Steering Committee consisting of Executive Advisor, Agency Liaisons, and the CPO. The subcommittees are responsible for conducting research for their subject matter areas within CHFS and presenting this information to the decision-making board. The CHFS Data Governance Steering Committee considers this information during the decision-making process and ensure that all parties have contributed as applicable.

The CHFS Data Governance Steering Committee consists of the following:

- **CHFS Data Governance** Steering Committee**:** Responsible for making decisions pertaining to privacy functions and data governance within CHFS. Consists of Agency Liaisons, Executive Advisor, Executive Director, and CPO.
- **Data Stewardship Subcommittee:** Responsible for identifying technical aspects of data within CHFS, including but not limited to: Data Access, Storage, Interconnections, Security of Data, Stewardship, and Data Integrity.
- **Privacy Subcommittee:** Responsible for analyzing various regulations regarding the types of data within CHFS and is responsible for determining if CHFS should share that type of data. This subcommittee will also discuss privacy training requests and concerns communicated by agency liaisons. This subcommittee is also responsible for the development, review, approval, and update of Cabinet-level privacy policies and procedures.

4.3 Privacy Policies and Procedures

CHFS develops privacy policies and procedures to protect collected PII data and meet the requirements of various applicable laws and regulations, such as the HIPAA Privacy Rule. These policies and procedures define how CHFS, its employees, and vendors must interact with PII.

The CPO, delegates, and Privacy Subcommittee under the CHFS Data Governance Steering Committee, and the CHFS OATS, are collectively responsible for developing and maintaining Privacy Policies at the Cabinet level.

The CHFS Data Governance Steering Committee is responsible for developing the

CHFS Data Governance Policy, which will be made available upon its approval.

Agencies within CHFS follow cabinet-wide privacy policy requirements and develop procedures for their respective agencies to meet those requirements, at a minimum. Agencies may also develop procedures that enforce standards that are more restrictive than the cabinet-wide policy, as long as these are in-line with the requirements from the cabinet-wide policy. Agencies are responsible for maintaining and enforcing their respective procedures.

4.4 Privacy Impact Assessment

CHFS follows CIO-106 Enterprise Privacy Policy, and has developed a CHFS Monitoring, Oversight, and Audit Privacy Controls Policy and CHFS Risk Assessment Program Procedure, which helps to address the following:

- Privacy Risk Management: Assess privacy-related risks across the life cycles of organizational processes that collect, use, maintain, share, retain, and dispose of PII.
- Privacy Assessment: Assess information systems and associated programs and activities that pose a risk to the organization's possession of PII. A PIA should be conducted for every information system; after the initial PIA, reviews of information systems are required to be completed annually, and a PIA is conducted when a change is identified during annual review or when an information system or privacy program change occurs that may have an impact on the PII that is collected, created, used, or disclosed.

4.5 Third Party & Data Sharing Agreements

CHFS follows CIO-110 Enterprise Data Management Policy, CIO-106 Privacy Policy, and has developed a CHFS OATS Interconnection Security Agreement Review Process and CHFS Business Associates, Internal Sharing, and Third Party Agreements Policy, which help to address the following:

- Data Sharing Evaluation: OHDA conducts a tailored vetting process on third-parties and internal CHFS agencies which determines the type of data to be shared and regulatory sources that apply to that data. If data can be shared, OHDA evaluates if existing authorizations and privacy notices allow for data sharing or whether a change to the privacy notice is required prior to sharing.
- Data Sharing Agreements: Contracts developed by OHDA in collaboration with Division of Procurement Services and Grant Oversight and approved by OGC that establish permitted uses and disclosures of PII for third parties and internal CHFS agencies. The agreements shall also include but are not limited to: limitations and consequences for violations; requirements to implement appropriate safeguards to prevent unauthorized use or disclosure; and any further requirements as stated in the privacy notice.
- Vendor Staff Privacy Requirements: Ensures that all third parties and internal CHFS agencies with whom CHFS shares data follow, at a minimum, the privacy requirements to maintain the same standards as CHFS and protect

information.

4.6 Monitoring and Auditing

CHFS follows CIO-106 Privacy Policy and has developed a CHFS Monitoring, Oversight, and Audit Privacy Controls Policy, CHFS 040.201- Internal Risk Assessment Policy, 065.015- Application Audit and Accountability and 020.206 Certification and Accreditation Policy which helps to address the following:

- Monitoring: Continuous monitoring of privacy controls; changes to applicable privacy laws and regulations; tracking programs, systems, and applications that collect and maintain PII; ensuring that PII is used only in accordance with the privacy notice.
- Auditing: Conducting regular assessments (e.g. privacy impact assessments) to identify and address gaps in privacy controls, implement technology to audit for security, appropriate use, and loss of PII, and assess contractor compliance
- Plan of Action and Milestones (POA&M): Findings and corresponding corrective action plans, based on audits, assessments, security impact analyses, monitoring activities or other review types, shall be documented and tracked in the Agency's POA&M. CHFS shall utilize a governance tool or other comparable method for POA&Ms management.

4.7 Privacy Awareness and Training

CHFS follows CIO-106 Enterprise Privacy Policy, and has developed a 050.101 Privacy and Security Awareness Program Policy and CHFS OATS Role-Based Security Training Procedure, which helps to address the following:

- Awareness and Training: Identifying, categorizing, and training those individuals who have various levels of privacy responsibility.
- PII Awareness: Personnel shall be made aware of the various categories of PII within CHFS (e.g. PHI, FTI). understand the need for privacy functions, and how privacy incidents should be handled through posters, emails, or awareness events.
- Role-Based Training: Ensures that personnel understands privacy roles, responsibilities, and procedures as related to their job area responsibilities.
- Training on Monitoring and Auditing of Shared PII: Continuous monitoring of PII shared with third parties and enforcing the consequences if said PII is used for any unauthorized purpose.

4.8 Metrics and Reporting

CHFS has developed CHFS Privacy Metrics to ensure accountability and transparency in privacy operations. These metrics shall be tracked using a governance tool or other comparable method. These metrics help CHFS address the following:

- Effectiveness: Determine progress in meeting privacy compliance requirements and controls; compare performance across the Agency; identify gaps in policy and implementation; and, identify models for success

- Management Reporting: Provides an overview to the Executive Director, CPO, Executive Advisor, and other applicable personnel on the status of privacy program compliance and efficiency.

4.9 Individual Consent, Access, Redress, and Disclosure

CHFS follows CIO-106 Enterprise Privacy Policy, and has developed a CHFS Accounting of Disclosures and Retention Policy, CHFS Privacy Notice Development Policy, CHFS Collection, Use, Access, and Retention of Personal Information Policy and CHFS Individual Rights to Personal Information Policy which help to address the following:

- Accounting of Disclosures: Maintaining a proper system of records for disclosures that CHFS makes involving PII and providing access to those records for the individuals whose information was disclosed.
- Privacy Notices: Emplacement of a comprehensive and transparent public notice at the point of collection that informs individuals about organizational activities pertaining to the use, storage, sharing, and retention/destruction of collected PII data, as well as the user's privacy rights.
- Individual Choice/Consent: Describing the rights individuals have regarding the collection, use, and disclosure of their PII. This includes obtaining consent for the collection and processing of their PII as required by law or regulation.
- Individual Access: Ensuring individuals have the ability to access their individual PII collected by the organization within the maintained systems of records.
- Redress: Supports the right for individuals to ensure the accuracy of PII held by organizations. This includes providing information to individuals upon request, the timeframe in which to respond to a request, and the user's ability to amend incorrect PII.

4.10 Data Quality and Integrity

CHFS follows CIO-106 Enterprise Privacy Policy, CIO-110 Enterprise Data Management Policy, and is developing the CHFS Data Governance Policy and CHFS Information Technology Policies, which help to address the following.

- Data Quality: Ensuring the relevance, accuracy, and completeness of collected PII before and after processing. This includes correcting PII that is inaccurate, incomplete, or outdated.
- Data Integrity: Ensuring processes are documented to describe the privacy controls in place to maintain the integrity of PII.
- Data Safeguarding: Ensuring proper security controls are in place for data at rest, data in transit, and data in use.

4.11 Data Minimization, Retention, and Disposal

CHFS follows Kentucky Department for Library and Archives (KDLA) Record Retention Schedule, CIO-106 Enterprise Privacy Policy, CIO-092 Media Protection Policy, and has developed CHFS 010.102 Data/Media Security, CHFS Collection, Use, Access, and Retention of Personal Information Policy, and is developing the CHFS Data

Governance Policy, which help to address the following:

- Data Minimization: Defining the appropriate steps to ensure the collection of PII elements are relevant and necessary to accomplish the purpose authorized by law or regulation.
- Data Retention: Defining the retention of each collection of PII for the minimum allowable time-period necessary to fulfill the purpose(s) identified in the consent notice or as required by law.
- Data Disposal: Defining the methods used to ensure secure deletion or disposal of PII (including originals, copies, and archived records).

4.12 Incident Response and Breach Notification

CHFS follows CIO-106 Enterprise Privacy Policy, and has developed CHFS 050.102-Information Systems Incident Response and Reporting and CHFS OATS Incident Response Plan, which help to address the following:

- Incident Response: Containing, mitigating, and resolving incidents and/or breaches of data, including security and privacy incidents.
- Breach Notification: Defining the coordination among various organizational and non-organization entities including all regulatory requirements regarding the investigation, management and reporting of suspected or actual information security incidents, and/or security breaches.

5 Program Maintenance Responsibility

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

6 Program Review Cycle

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

7 Program References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS 010.102 Data/Media Security
- CHFS 040.201- Internal Risk Assessment Policy
- CHFS 050.101 Privacy and Security Awareness Program Policy
- CHFS 050.102- Information Systems Incident Response and Reporting
- CHFS Accounting of Disclosures and Retention Policy
- CHFS Business Associates and Third Party Agreements Policy
- CHFS Collection, Use, Access, and Retention of Personal Information Policy
- CHFS Contractor Privacy and Security of Protected Health, Confidential and Sensitive Information Agreement Form for External Vendors (CHFS-219V)
- CHFS Individual Rights Policy
- CHFS Information Technology Policies
- CHFS Monitoring, Oversight, and Audit Privacy Controls Policy
- CHFS OATS Incident Response Plan

- CHFS OATS Role-Based Security Training Procedure
- CHFS Organizational Structure
- CHFS Privacy Notice Development Policy
- CHFS Risk Assessment Program Procedure
- CIO-092 Media Protection Policy
- CIO-106 Enterprise Privacy Policy
- CIO-106 Privacy Policy
- CIO-110 Enterprise Data Management Policy
- Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule
- Information Systems Incident Response and Reporting Policy
- Internal Revenue Services (IRS) Publications 1075
- Kentucky Department for Library and Archives (KDLA) Record Retention Schedule
- Kentucky Information Technology Standards (KITS): 4080 Data Classification Standard
- 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 Statute (KRS) Chapter 61: House Bill 5 (HB5)
- Kentucky Revised Statutes (KRS) Chapter 194A.060 Confidentiality of records and reports
- Kentucky Revised Statutes (KRS) Chapter 61.884 Person's access to record relating to him
- 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