Commonwealth of Kentucky
Cabinet for Health and Family Services

Cabinet for Health and Family Services (CHFS) Privacy Plan

CHFS Privacy Plan

Version 2.0
04/3/2023

Revision History

Date	Version	Description	Author
10/28/2019	1.0	Effective Date	Privacy Policy Team
10/29/2020	1.1	Effective Date	Privacy Policy Team
01/14/2022	1.2	Review Date	Privacy Policy Team
04/3/2023	2.0	Revision Date	Privacy Program

Sign-Off

Sign-off Level	Date	Name	Signature
General Counsel (or delegate)	4/3/2023	Wesley Duke	DocuSigned by: Wesley Duke D58FF6B4FC274A6...
CHFS Chief Privacy Officer (or delegate)	4/10/2023	Kathleen Hines	DocuSigned by: Kathleen Hines E27E1B3456DA43D...

Table of Contents

Table of Contents

1 DEFINITIONS 4

2 PLAN OVERVIEW 6

3 PRIVACY CONTROLS AND PLAN OF ACTION & MILESTONES (POA&M) 6

4 POLICIES AND PROCEDURES DEVELOPMENT 7

5 PRIVACY IMPLEMENTATION STRATEGY 7

6 PRIVACY IMPACT ASSESSMENTS (PIA) 7

7 PLAN MAINTENANCE RESPONSIBILITY 7

8 REVIEW CYCLE 8

9 POLICY REFERENCES 8

1 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) maintaining current master services agreement with the Commonwealth.
- **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. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number). 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 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 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).

- **Privacy Impact Assessment (PIA):** Defined by CMS Minimum Acceptable Risk Standards for Exchanges (MARS-E) 2.0 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.
- **State Staff/Personnel:** Defined by CHFS as an employee hired directly through the state by CHFS.
- **System Security Plan (SSP):** Defined by NIST Special Publication 800-37, an SSP is a formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.
- **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 Plan Overview

Privacy Plan outlines the Cabinet for Health and Family Services (CHFS) program to strategically develop and implement privacy-related policies and procedures including a summary of how State and Federal security and privacy requirements, for example CMS, are incorporated into the overall organization.

3 Privacy Controls and Plan of Action & Milestones (POA&M)

Privacy controls are requirements that CHFS agencies within the cabinet must follow. These controls are determined by different federal and state regulatory laws and may vary within each agency. Examples of sources include, but are not limited to, the following which are defined in an excel sheet called the “Privacy Requirements Framework”. This is also available on RSA Archer application:

- NIST Special Publication (SP) 800-53
- CMS MARS-E v2.0
- Health Insurance Portability and Accountability Act (HIPAA) of 1996
- IRS Publication 1075
- Social Security Administration Privacy requirements
- Patient Protection and Affordable Care Act (PPACA)
- Kentucky Revised Statutes (61.931, 61.932, 61.933, 61.934,194A.060, 209.140, 216.530, 214.420, 214.625, 214.181, 222.271, 216.2927, 202A.091, 202B.180 210.235, 211.902, 211.670, 213.131, 199.570, 205.175, 205.730(6), 205.735, 205.796, 434.850, 610.340, 620.050, 625.045, 625.108)
- Privacy Act of 1974
- Health Information Technology for Economic and Clinical Health (HITECH) Act, Subtitle D

CHFS Chief Privacy Officer (CPO) or designee monitors and audits privacy controls for the cabinet as required by applicable privacy requirements and as determined by the CPO. CHFS follows the requirements listed in the framework with an endeavor to protect PII during its complete lifecycle and to ensure that PII is used for limited purpose(s) as required.

A weakness is created if privacy control requirements exist, but its control implementation status is not implemented. CPO coordinates with various agencies to address the outstanding gap/weakness and implement the privacy control, which is not currently in place. The framework can serve as a reference guidance for this control implementation. CHFS CPO will follow the CHFS POA&M procedure to remediate the gap/ weakness.

4 Policies and Procedures Development

CHFS CPO develops privacy policies and procedures to enforce privacy requirements throughout the cabinet. CPO maintains an internal list of privacy policies and procedures, which either are currently in development or are anticipated for future development. This list may be changed as per discretion of CPO.

Privacy policies and procedures are accessible through a website once they are approved.

5 Privacy Implementation Strategy

CHFS CPO works with various agencies in the cabinet to develop and maintain a cabinet board to foster awareness of privacy policies and procedures. The board is generally responsible for the following, but not limited to:

- Discerning vision of CPO to various agencies
- Providing privacy training to employees within their agencies
- Enforcing privacy policies and procedures

6 Privacy Impact Assessments (PIA)

For systems, which must be CMS MARS-E compliant, CHFS conducts PIAs on an annual basis. Additionally, PIAs must also be conducted 60 days before a major system change occurs. For other systems, a PIA may be conducted based on other regulatory requirements or as per discretion from CPO or CHFS management.

CHFS uses the following templates to conduct PIAs:

- CMS PIA Template; This template is used for systems (for example Integrated Eligibility & Enrollment System (IEES)) that must be compliant with CMS MARS-E requirements
- COT PIA Template; This template is used for systems (for example Kentucky Health Interactive Exchange (KHIE), etc.) which require a PIA but are not governed by CMS MARS-E requirements

CHFS is responsible for managing activities related to performing a PIA of IT systems, resources, or data-sets to endeavor to ensure privacy considerations and protections are incorporated into activities related to PII.

7 Plan Maintenance Responsibility

The CHFS CPO is responsible for the maintenance of this plan.

8 Review Cycle

CHFS CPO updates this plan, privacy policies and procedures at least biennially and on an as needed basis or as requirements change.

9 Policy References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS OATS IT Policies
- CHFS Plan of Action & Milestone Procedure
- Enterprise IT Policy: CIO-106 - Privacy Policy
- Health Information Technology for Economic and Clinical Health (HITECH) Act, Subtitle D
- 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 Statutes
- Kentucky Revised Statute (KRS) Chapter 61: House Bill 5 (HB5)
- 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
- National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- Patient Protection and Affordable Care Act (PPACA)
- Privacy Act of 1974
- Social Security Administration (SSA) Security Information