Commonwealth of Kentucky
Cabinet for Health and Family Services

Cabinet for Health and Family Services (CHFS) Privacy Policy

KENTUCKY CABINET FOR HEALTH AND FAMILY SERVICES

CHFS Monitoring, Oversight and Audit Privacy Controls Policy

Version 1.2
10/29/2020

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

Sign-Off

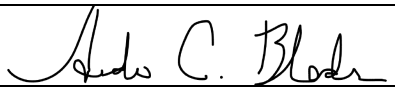
Sign-off Level	Date	Name	Signature
Executive Advisor (or delegate)	01/14/2022	Andrew Bledsoe	
CHFS Chief Privacy Officer (or delegate)	01/14/2022	Kathleen Hines	

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 6

3.1 CHIEF INFORMATION SECURITY OFFICER (CISO) 6
3.2 CHFS OATS INFORMATION SECURITY (IS) TEAM 7
3.3 CHIEF PRIVACY OFFICER (CPO) 7
3.4 SECURITY/PRIVACY LEAD 7
3.5 CHFS STAFF AND CONTRACTOR EMPLOYEES 7
3.6 SYSTEM DATA OWNER 7

4 POLICY REQUIREMENTS 7

4.1 MONITORING 7
4.2 PRIVACY IMPACT ASSESSMENT (PIA) 8
4.3 THIRD-PARTY OVERSIGHT AND AUDITS 8

5 POLICY MAINTENANCE RESPONSIBILITY 9

6 POLICY REVIEW CYCLE 9

7 POLICY REFERENCES 9

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 (HIPPA) 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. The 18 individually identifiable health information includes 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 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 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 provide temporary work for CHFS.

2 Policy Overview

2.1 Purpose

The Cabinet for Health and Family Services (CHFS) Office of Health Data and Analytics (OHDA) must establish a comprehensive level of privacy controls provided by State and Federal regulations and available in the CHFS Privacy Framework (accessible in RSA Archer enterprise governance and compliance application or other comparable method), to implement through an Oversight, Monitoring, and Audit Privacy Controls Policy. This document establishes the agency's Oversight, Monitoring, and Audit Privacy Controls, to manage privacy related risks and provide guidelines for security best practices regarding monitoring and auditing privacy controls and internal privacy plan.

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 OHDA Executive Director 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

OHDA coordinates 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).

3 Roles and Responsibilities

3.1 Chief Information Security Officer (CISO)

The 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.

3.2 CHFS OATS Information Security (IS) Team

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

3.3 Chief Privacy Officer (CPO)

An individual responsible for overseeing activities related to the development, implementation, maintenance of, and adherence to the Cabinet's and Commonwealth's information privacy and confidentiality policies and procedures in compliance with federal and state laws. This individual will conduct Health Insurance Portability and Accountability Act (HIPAA) self-assessments through coordination with the Information Security Agency Representative, the CISO, or CHFS OATS IS Team, and other CHFS agencies, and will ensure compliance with HIPAA notification and reporting requirements in the event of an identified breach. This position is responsible to adhere to this policy.

3.4 Security/Privacy Lead

Individuals are designated by the division leadership to coordinate privacy and/or security issues and incidents with all appropriate personnel. The individual is responsible for providing security and privacy guidance for protection of PII, PCI, ePHI, FTI and other sensitive information to all CHFS staff and contractor personnel. This role along with the CHFS OATS IS Team is responsible for the adherence of this policy.

3.5 CHFS Staff and Contractor Employees

All CHFS contract, state, and vendor staff/personnel must adhere to this policy. All staff/personnel must comply with referenced documents, found in Section 7 Policy 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).

3.6 System Data Owner

The System Data Owner, or appointed delegate, is responsible for preparing the annual risk assessment as mandated by the HIPAA Security Rule 45CFR164.308(a)(1)(ii)(A). System Data Owners, or appointed delegate, are also responsible for performing the various steps related to identifying potential risks and threats and are required to ensure that identification of risks is properly categorized and documented in terms of their potential threat to their program area. All information regarding risks to the business systems will be the responsibility of the System Data Owner, or appointed delegate, to document, track and respond whenever appropriate.

4 Policy Requirements

4.1 Monitoring

CHFS CPO or designee shall coordinate with other CHFS agencies to monitor all agencies privacy related controls, policies, and procedures to ensure that they reflect

state and federal regulations. CHFS CPO or designee shall also monitor for changes to applicable privacy laws, regulations, and policies. Privacy policies, procedures, programs, and other applicable documents shall be revised and updated as needed to reflect new regulations. The CPO will maintain a record of privacy controls which are not currently being met or implemented and shall follow the CHFS POA&M procedure to remediate the gap.

As part of CHFS Continuous Monitoring Program, the CHFS OATS IS Team shall track information systems, and applications that collect, use, maintain, or share PII to ensure compliance with state and federal regulations and laws.

CHFS agency personnel will ensure that PII is on a need-to-know basis and it is only used for legally authorized purposes. KRS Chapter 61.878 states that "public records containing information of a personal nature" are exempt from inspection except on order of court. Additionally, KRS Chapter 61.884 states that "any person shall have access to any public record relating to him."

CHFS agency personnel will follow the 065.015 Application Audit and Accountability (AU) Policy to audit for the security, appropriate use, and loss of PII. CHFS agency personnel will continuously monitor systems which use sensitive and confidential information and will follow 050.102- Information Systems Incident Response and Reporting in case of an incident.

CHFS will ensure contractor compliance with privacy requirements by requiring contractors to sign a CHFS Contractor Privacy and Security of Protected Health, Confidential and Sensitive Information Agreement Form for External Vendors (CHFS-219-V) prior to receiving any CHFS computing asset.

4.2 Privacy Impact Assessment (PIA)

The CPO or designee will coordinate with other CHFS agencies to conduct PIA's. These may either be conducted periodically based on state or federal requirements, or as per discretion from CPO or management.

Assessment activity, including but not limited to conducting assessments, gap identification, gap remediation, will be tracked using the RSA Archer enterprise governance and compliance application or other comparable method. If using Archer, notifications are sent to the System Data Owners to start the process of mitigating the risk identified by the PIA. The final assessment report is formally documented and shared with management and is stored at a secure CHFS site.

4.3 Third-Party Oversight and Audits

The CPO or designee shall coordinate with other agencies to conduct third-party audits based on regulatory requirements or as per discretion from CPO or management. The audit findings shall be documented, and corrective actions will be identified and tracked.

As per IRS Publication 1075, CHFS shall conduct an internal inspection to ensure physical security of documents containing FTI. The report of the inspection shall be submitted to IRS.

CHFS agencies shall comply with US Department of Health and Human Services (HHS) privacy oversight and audit policies and procedures. CHFS agencies shall follow HHS requirements as determined by HIPAA Privacy Rule and may be subject to HHS audits on an ad-hoc basis as requested.

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 2.0
- CHFS Continuous Monitoring Metrics
- 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 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
- 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