Commonwealth of Kentucky
Cabinet for Health and Family Services

Cabinet for Health and Family Services (CHFS) Privacy Policy

CHFS
KENTUCKY
Cabinet *for* Health *and* Family Services

CHFS Privacy Notice Development Policy

Version 1.1
10/30/2020

Revision History

Date	Version	Description	Author
10/28/2019	1.0	Effective Date	Privacy Policy Team
10/30/2020	1.1	Effective Date	Privacy Policy Team

Sign-Off

Sign-off Level	Date	Name	Signature
Executive Director (or delegate)	10/30/2020	Robert Putt	Robert E Putt
CHFS Chief Privacy Officer (or delegate)	10/30/2020	Kathleen Hines	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 INFORMATION OWNER 7

4 PRIVACY NOTICE POLICY 7

4.1 PRIVACY NOTICE DEVELOPMENT 7
4.2 PRIVACY NOTICE REVISION 9

5 MAINTENANCE RESPONSIBILITY 10

6 REVIEW CYCLE 10

7 POLICY REFERENCES 10

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. The 18 individually 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 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).

- **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 Privacy Notice Development Policy. This document establishes the agency's Privacy Notice Development, to manage privacy related risks and provide guidelines for practices regarding specific privacy notice policy requirements.

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 the 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)

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 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. Each individual is responsible for providing security and privacy guidance for protection of PII, PCI, ePHI, FTI and other confidential or 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 Information Owner

The Information Owner is responsible for assisting System Owners (SO) with implementing, maintaining and reviewing appropriate auditable events, for their information resources, that may need action or changes.

4 Privacy Notice Policy

4.1 Privacy Notice Development

Information Owners will develop a privacy notice which is provided to end users describing how their personal information will be collected, used, accessed, disclosed and protected where required by law. Notice may be provided in any number of different channels (e.g., electronic, paper).

The collection of personal information will be in accordance with applicable laws and regulations such as Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule. To accomplish this, the collection and use of personal information will be limited to what is required and relevant for legitimate purposes and is in accordance

with the privacy notice provided to the individual (i.e., individuals are informed as to what information is collected, for what purpose, and how it will be used).

As per applicable laws including CMS MARS-E 2.0, the privacy notice should address the following:

- Provide detail on the choices, if any, that individuals have for the collection, use, and disclosure of personal information, or otherwise obtain consent from individuals for the collection, use, and disclosure of personal information that the CHFS may have about them.
- Identify CHFS and the agency as the collector, processor, and handler of individuals' personal data (i.e., provide CHFS's official name and address) and, if applicable, identify the third parties that will handle personal information on CHFS's behalf (i.e., provide third parties' legal names and addresses).
- Identify the legal authority for CHFS to collect personal information.
- Inform users of any transfer and/or disclosure of personal information to third parties (including name of third parties' the information is being shared with and purpose for sharing information).
- Inform users of the purposes for which CHFS uses personal information internally.
- Identify and provide contact information which the individual may use to gain access to or request correction of personal information.
- Describe the categories of personal information being collected by CHFS and the purposes for collecting and processing this information where required by law.
- Inform users of the safeguards in place to protect personal information, such as reasonable administrative, technical, and/or physical security controls to prevent unauthorized or accidental loss, corruption, or disclosure of personal information related to individuals.
- Inform users if they have the choice to consent to specific uses or sharing of personal information, how to exercise any such consent, and the consequences of exercising or not exercising that choice.

Additional notice requirements may be required by law based on certain circumstances. Information owners must ensure that their notices meet these requirements as well, if applicable. Where required by law, [i.e. HIPAA 45 CFR 164.520(a)(1) Right to notice. Except as provided by paragraph (a)(2) or (3) of this section, an individual has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information], privacy notice may disclose additional information including:

- A description of the types of entities (e.g., federal agencies) to which personal information is disclosed.
- Whether requested information is required or voluntary, as well as the possible consequences of failure to provide information.
- The individual's rights and means of gaining access to personal information as

well as rectification (i.e., correction) of personal information held by CHFS.
- An explanation of the individual's right to opt out of the disclosure of personal information to third parties, including the method(s) by which the individual may exercise that right at that time.
- Assurance that personal information will only be kept for its required retention period and then securely destroyed, permanently deleted, made anonymous, in a manner that prevents loss, misuse, or unauthorized access.
- Any further information which is necessary, taking into account the specific circumstances.

CHFS CPO is responsible for reviewing privacy notice before it is finalized and provided to individuals.

HIPAA Notice of Privacy Practices

CHFS agencies that are covered components subject to the HIPAA Privacy Rule are required to provide individuals with a "Notice of Privacy Practices" that describes how the agency may use and disclose protected health information about the individual, as well as the individual's rights and the agency's obligations with respect to that information. All Notices of Privacy Practices must meet the requirements outlined in 45 CFR § 164.520.

A Notice of Privacy Practices must be in plain language and include:
- Information regarding uses and disclosures of PHI
- The individual's rights with respect to PHI, including how to make a complaint to the agency
- The agency's responsibilities, including the requirement to maintain the privacy of PHI
- Contact information for individuals to request more information about the agency's privacy practices
- The effective date of the notice

A Notice of Privacy Practices must be made available to any person who asks for it. An agency that maintains a website that provides information about its customer services or benefits must prominently post and make available its Notice of Privacy Practices on the web site.

4.2 Privacy Notice Revision

Whenever there is a change in applicable law or privacy practices and policies that may affect PII or changes in its activities that impact privacy, necessitates a change to the content of the privacy notice.

If the privacy notice is revised and/or updated by CHFS information owner, CHFS CPO will review the updated notice before it is finalized. The respective CHFS information owner will make the appropriate revisions to the notice in accordance with legal and

regulatory requirements and see that the revised notice is distributed appropriately.

5 Maintenance Responsibility

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

6 Review Cycle

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

7 Policy References

- 45 CFR 155.260 Privacy and Security of personally identifiable information
- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS Contractor Privacy and Security of Protected Health, Confidential and Sensitive Information Agreement Form for External Vendors (CHFS-219V)
- Enterprise IT Policy: CIO-106 - Privacy Policy
- 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 194A.060 Confidentiality of records and reports
- 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