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: Individual Rights to Personal Information

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 0AEA1D6C15D6431...
OHDA Executive Director (or delegate)	6/8/2021 | 9:31 AM EDT	Robert Putt	DocuSigned by: Robert E. Putt 4BBBFF6DFCEC461...
CHFS Chief Privacy Officer (or delegate)	6/8/2021 | 10:07 AM EDT	Kathleen Hines	DocuSigned by: Kathleen Hines E27E1B3456DA43D...

Table of Contents

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.

- **Protected Health Information (ePHI):** Defined by the 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). 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 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.
- **Implied Consent:** Consent which is not expressly granted by a person, but rather implicitly granted by a person's actions and the facts and circumstances of a particular situation (or in some cases, by a person's silence or inaction).
- **Informed Consent:** The process by which an individual understands the purpose, benefits, and potential risks to make an informed decision to voluntarily share personal information.
- **Opt-in (consent):** Individuals shall give specific permission to contribute their data prior to primary and secondary use of personally identifiable information.
- **Opt-out (consent):** An individual's data is automatically added to a repository and an individual must explicitly request their data not be stored for the data to be removed.
- **Personally Identifiable Information (PII):** Defined by 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). 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.

- **Protected Health Information (PHI):** Defined by the HIPAA Privacy Rule as individually identifiable information relating to the past, present, or future health status of an individual that is created, received, stored, transmitted, or maintained by HIPAA covered entities and their business associates in relation to the provision of healthcare, healthcare services, and operations.
- **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 PCI DSS Security Standards 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, CAV2/CVC2/CVV2/CID, and PIN(s). CHFS also defines sensitive financial data 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 provide temporary work for CHFS.

2 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 security controls to implement through an Individual Rights to Personal Information Policy. This document establishes the agency's policy on an individual's rights to personal information, to manage risks and provide guidelines for security best practices regarding an individual and their rights to their own personal information.

2.2 Scope

Scope 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

The Chief Privacy Officer (CPO) and the Office of Health Data and Analytics (OHDA) Executive Director have reviewed and approved this program, and 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 organizations and/or agencies within the cabinet, which 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 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 **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).

3.7 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 Policy Requirements

CHFS is committed to protecting the integrity of the Personally Identifiable Information (PII), including Protected Health Information (PHI), that it collects by obtaining consent, providing individuals with access to their confidential information held by CHFS, and providing individuals a means for correcting the accuracy of their information unless otherwise restricted. Where feasible and appropriate, or when required by law or other authority, CHFS will provide the means for individuals to consent to the collection, use, maintenance, and dissemination of PII prior to its collection. CHFS will take appropriate measures to permit individuals to amend or restrict the disclosure of their confidential information, and an opportunity to request specific individual rights or to submit complaints related to confidential information held by CHFS.

4.1 Consent

When appropriate and possible, or when required by law or other authority, CHFS will provide the means for individuals to authorize the collection, use, maintenance, and dissemination of PII prior to its collection.

4.2.1. Method and Form of Consent: The method of providing authorization may be tailored as appropriate or as required by law. Authorization may be obtained through opt-in, opt-out, or implied consent. Opt-in consent is the preferred method, but is not always feasible. CHFS will ensure that opt-in consent is provided when it is required by law or other regulatory authority.

CHFS will provide appropriate means for individuals to understand the consequences of the decision to approve or decline authorization of the collection, use, dissemination, or retention of PII.

CHFS will obtain consent, where feasible and appropriate, or as required by statute or regulation, from individuals prior to new uses or disclosure of previously collected PII. CHFS will also ensure that individuals are aware of and, where feasible or as required by law, consent to uses of PII not initially described in the privacy notice that was in effect when the agency collected the PII.

Consent Documentation: CHFS will maintain proof of an individual's consent in a manner that clearly documents the individual's signed and/or verbal consent and the date when consent was granted. For opt-in consent, documentation shall contain at a minimum: name, date, signature, and authorized release of information. If opt-out consent is the primary method of disclosure, CHFS will maintain relevant documentation to reflect that the individual was given the right to opt-out, and the individual's choice.

When required by law, CHFS will create legally compliant consent and authorization forms.

4.2.2. Revocation of Consent: CHFS may allow an individual to revoke their consent where reasonably possible, if the individual agrees or requests to the revocation in writing, electronically, or if the individual orally agrees to the revocation and the oral agreement is documented.

4.2 Access

Access affords individuals the ability to review their own PII within CHFS records. Access must be reasonable and timely, provided in a format that the individual is able to understand, and provided as inexpensively as possible. Processes for allowing access to records may differ based on resources, legal requirements, and/or other factors. NOTE: Nothing in this policy is meant to replace or supersede requirements for access to records that is mandated by the Kentucky Open Records Act, contained in KRS 61.870 to KRS 61.884.

4.2.1. General Access: CHFS will provide individuals with reasonable access to their PII, in a readable form and format, and for a reasonable fee if permitted by law. CHFS agencies will make any processes and procedures available to individuals who wish to make a request for access to PII within the agency's records.

CHFS agency staff shall verify an individual's identity and the

authorization to disclose before releasing personal information.

4.2.2. HIPAA Designated Record Set: CHFS agencies that are covered components subject to the HIPAA Privacy Rule are required to provide individuals with access to the individual's designated record set. An individual has the right to access, inspect, and obtain a copy of PHI in a designated record set for as long as the information is maintained. (See 45 CFR § 164.524). Designated record set includes, at a minimum, the medical and billing records of individuals that are maintained by the agency, and other records used, in whole or in part, to make decisions about the individual.

The HIPAA Privacy Rule does not require the request to be in a specific format; therefore the agency may choose to accept both verbal and written requests. If the agency chooses to require individuals to make requests in writing, it must inform individuals of such a requirement, provided that this does not create a barrier or unreasonable delay for the individual to obtain his or her PHI.

The agency must respond to the request within thirty (30) days of receipt by either granting or denying the request. If the agency is unable to provide access within 30 days, the agency may extend the time for response by no more than 30 additional days, provided that the agency provides the individual with a written statement of the reason for the delay, and the date by which the agency will complete its action on the request. The agency is allowed only one such extension of time for action on a request for access.

If the agency grants the request, in whole or in part, it must inform the individual of the acceptance of the request and provide the access requested in accordance with 45 CFR 164.524(b)(2) and (c). If the agency denies the request, in whole or in part, it must provide the individual with a written denial, in accordance with 45 CFR 164.524(b)(2) and (d).

4.3 Correction or Amendment

CHFS will provide individuals with appropriate means to request correction of, or amendment to, their PII maintained by CHFS. To the extent possible, CHFS will make appropriate corrections or amendments upon request, and shall notify the individual and other authorized users of the PII of the change.

The Cabinet may deny a correction of, or amendment to PII if it is determined to be accurate and complete, not part of a designated record set, and would not be available under inspection per § 164.524, or was not created by CHFS originally and the Cabinet is no longer able to act upon the requested amendment (See 45

CFR 164.526 (a)).

4.4 Privacy Complaints and Redress

CHFS will shall provide appropriate means for individuals to submit complaints, concerns, or questions about organizational privacy practices.

CHFS will respond to complaints within 30 days of receipt. CHFS will document complaints and their disposition, if any, and retain these records for six years.

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 OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control 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 Statue (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
- Payment Card industry (PCI) data Security Standard (DSS) Requirements and Security Assessment Procedures Version 3.2.1
- Social Security Administration (SSA) Security Information