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 Business Associates and Third Party Agreements Policy

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

- **Business Associate:** Defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule as a person or entity, other than a member of the workforce of a covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to protected health information. A "business associate" also is a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of another business associate.
- **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 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.13 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.

- **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).
- **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 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 security controls to implement through a Business Associate and Third Party Agreement(s) policy. This document establishes the agency's policy regarding Business Associate and Third Party Agreement(s), to manage risks and provide guidelines for security best practices.

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.

3.1 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.

3.2 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.

3.3 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.

3.4 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).

3.5 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.

3.6 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 may share PII externally only for the authorized purposes for which it was collected, as described in the agency's privacy notice(s) and agreements, or for a purpose authorized by statute or regulation. Before sharing PII with third parties, CHFS will assess whether sharing is authorized and if additional or a new public notice is required.

4.1 Third Party Agreements

Where appropriate or required by law, CHFS will enter into agreements with third parties that specifically describe the PII covered, and enumerate the purposes for which the PII may be used. These agreements will establish privacy roles, responsibilities, and access requirements for contractors and service providers, and will include privacy requirements in contracts and other acquisition-related documents.

4.2 Business Associate Agreements

4.2.1. Business Associate Agreements: The HIPAA Privacy Rule allows CHFS to disclose PHI to a "Business Associate" under certain conditions. In order to disclose PHI to a business associate, CHFS must receive satisfactory assurance that the business associate will appropriately safeguard the information. CHFS will ensure that before any third party receives or accesses PHI that the third party has signed a HIPAA-compliant Business Associate Agreement that contains satisfactory assurances.

4.2.2. Business Associate Agreement Requirements: A HIPAA-compliant Business Associate Agreement must include the following components:

1) Establish the permitted and required uses and disclosures of protected health information by the business associate;

2) Provide that the business associate will not use or further disclose the information other than as permitted or required by the agreement or as required by law;
3) Require the business associate to implement appropriate safeguards to prevent unauthorized use or disclosure of the information, including implementing requirements of the HIPAA Security Rule with regard to electronic protected health information;
4) Require the business associate to report to the covered entity within the time period specified in the agreement any use or disclosure of the information not provided for by its contract, including incidents that constitute breaches of unsecured protected health information;
5) Require the business associate to disclose protected health information as specified in its contract to satisfy a covered entity's obligation with respect to individuals' requests for copies of their protected health information, as well as make available protected health information for amendments (and incorporate any amendments, if required) and accountings;
6) To the extent the business associate is to carry out a covered entity's obligation under the Privacy Rule, require the business associate to comply with the requirements applicable to the obligation;
7) Require the business associate to make available to HHS its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity for purposes of HHS determining the covered entity's compliance with the HIPAA Privacy Rule;
8) At termination of the contract, if feasible, require the business associate to return or destroy all protected health information in a manner required within the agreement that was received from, or created or received by the business associate on behalf of, the covered entity;
9) Require the business associate to ensure that any subcontractors it may engage on its behalf that will have access to protected health information agree to the same restrictions and conditions that apply to the business associate with respect to such information; and
10) Authorize termination of the contract by the covered entity if the business associate violates a material term of the contract.

Contracts between business associates and business associates that are subcontractors are subject to these same requirements.

4.2.3. Compliance and Termination of Business Associate Agreement: If CHFS learns that a business associate has materially breached the agreement, CHFS will require the business associate to promptly cure the breach. If

the business associate fails to do so or is unsuccessful, CHFS will terminate the Agreement. If termination of the Agreement is not feasible, then at its discretion CHFS will report the breach of the agreement to the Secretary of HHS.

5 Policy Maintenance Responsibility

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

6 Policy Exceptions

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

7 Policy Review Cycle

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

8 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