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 Personally Identifiable Information (PII) used in Testing, Training, and Research

Version 1.0
09/13/2021

Revision History

Date	Version	Description	Author
09/13/2021	1.0	Effective Date	CHFS Privacy Program

Sign-Off

Sign-off Level	Date	Name	Signature
CHFS Secretary	9/21/2021 | 8:40 AM EDT	Eric Friedlander	DocuSigned by: Eric Friedlander 0AEA1D6C15D6431...
Executive Director (or delegate)	9/16/2021 | 1:07 PM EDT	Robert E. Putt	DocuSigned by: Robert E. Putt 4B8BFF6DFCEC481...
CHFS Chief Privacy Officer (or delegate)	9/16/2021 | 12:37 PM EDT	Kathleen Hines	DocuSigned by: kathleen Hines E27E1B3458DA43D...

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.
- **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). 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.

- **Production (PROD):** Defined by CHFS as the system environment where the intended users will interact with the system and is updated only when testing on other environments is completed. Data within the system environment that may contain personal, identifiable, sensitive, and confidential information. All servers shall be labeled in the Information Technology Management Portal (ITMP) to reflect the system environment (i.e., Development, Test, Production, etc.). (This is the definition of Production that is in various CHFS IT Security policies. Since you are referencing Production, I thought it would be good to include the definition.)
- **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 Policy Overview

2.1 Purpose

The Cabinet for Health and Family Services (CHFS) must establish a comprehensive level of privacy and security controls pertaining to the use of Personally Identifiable Information (PII) in testing, training, and research. This document establishes the agency's Policy for Personally Identifiable Information (PII) used in testing, training, and research (above these words were not capitalized), to manage risks and provide guidelines for 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

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 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 7 Program 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).

3.7 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 follows NIST 800-53 Rev.4 which pertains to testing, training, and research and where applicable IRS Special Publication 1075, Centers for Medicare and Medicaid (CMS) Minimal Acceptable Risk Standards for Exchanges (MARS-E), HIPAA Privacy and Security Requirements, and Social Security Administration control requirements. When PII or PHI must be used for research, CHFS ensures minimal risk, authorization, and limited use of information for this purpose. The Chief Privacy Officer and Office of Legal Counsel will be consulted to ensure the use of PII and PHI are compatible with the original purpose for which data collection was intended. CHFS also follows all state laws pertaining to testing, training, and research as it relates to PII and PHI in addition to the CHFS OATS Policy: 010.102 Data/Media Security Policy.

4.1 Testing

CHFS is consistently developing, purchasing, and upgrading data systems. To ensure testing is effective, CHFS staff and contractors collaborate to create simulated “real” conditions as closely as possible to determine systems are operating correctly to keep PII and PHI safe. In User-Access Testing (UAT) environments, CHFS works with staff and contractors to implement role-based access control, enabling systems to be configured allowing each user to access only the data necessary for the user‘s role. CHFS uses anonymized or obfuscated data, also known as created data to test real conditions in order to protect CHFS data.

Production data shall not be used in a test environment. As a last resort, if PII or PHI in

production data must be used in a test environment, an exception must be submitted and approved following CHFS OATS Policy: 070.203 Security Exceptions and Exemptions to CHFS OATS Policies and Security Controls Policy. Further, the production data is required to be protected at the same level as data in an existing in-use system.

4.2 Training

CHFS shall not use production data in employee training, and any exception would need to be approved by the following CHFS OATS Policy: 070.203 Security Exceptions and Exemptions to CHFS OATS Policies and Security Controls Policy. CHFS may use dummy data that is de-identified and compiled from multiple sources in training situations.

4.3 Research

The HIPAA Privacy Rule states PHI may be used or disclosed by covered entities for research purposes. Research is defined in the Privacy Rule as, “a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge” per 45 CFR 164.501. A covered entity may use or disclose for research purposes health information which has been de-identified under 45 CFR 164.502(d), and 164.514(a)-(c) of the Rule.

The Privacy Rule also describes the means by which individuals will be informed of uses and disclosures of their medical information for research purposes and their rights to access such information. The Privacy Rule protects the privacy of individually identifiable health information, while ensuring researchers have and maintain access to medical information necessary to conduct research.

CHFS has developed a process to receive, review, approve or deny, and process research related data requests. The requestor must meet all of CHFS’ criteria prior to submitting a proposal for any individual-level de-identified data or PII, including the requirements of 45 CFR part 46 for protecting human research subjects. Those requirements also correspond to those of the CHFS Institutional Review Board (IRB) approval. Upon approval of the request, CHFS and the requesting entity may enter into a data sharing agreement (DSA). The DSA will be reviewed by the CHFS Chief Privacy Officer to determine PII protection under the HIPAA Privacy Rule. Additional review of a DSA will potentially include the data owner, OHDA Data Governance, Office of Legal Services, and OATS Security.

CHFS may or may not disclose PII of an individual without the authorization from the individual, according to applicable laws including 45 CFR § 164.508 and 45 CFR Part 2.

5 Security

CHFS regularly reviews and analyzes information system audit records for indications of inappropriate or unusual activity affecting PII and PHI. CHFS Security and the CHFS Chief Privacy Officer investigate suspicious activity and potential policy violations, report findings to appropriate officials, and take other necessary actions, if necessary.

6 Policy Maintenance Responsibility

The CHFS CPO is responsible for maintenance of this policy.

7 Policy Exceptions

Any exceptions to this policy must follow the guidance established in CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy.

8 Policy Review Cycle

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

9 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
- CHFS OATS Policy 010.102 Data/Media Security 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