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 Accounting of Disclosures and Retention Policy

Version 1.0
10/28/2019

Revision History

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

Sign-Off

Sign-off Level	Date	Name	Signature
Executive Director (or delegate)	10/28/2019	Robert E Putt	Robert E Putt
CHFS Chief Privacy Officer (or delegate)	10/28/2019	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

4 POLICY REQUIREMENTS 7

4.1 ACCOUNTING OF DISCLOSURES 7
4.2 DISCLOSURE RETENTION 8
4.3 PROVISIONING OF DISCLOSURES 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 (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 13 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).

- **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 to implement through an Accounting of Disclosures and Retention Policy. These regulations will be available in the CHFS Privacy Framework (accessible in RSA Archer enterprise governance and compliance application or other comparable method). This document establishes the agency's Accounting of Disclosures and Retention, to manage privacy related risks and provide guidelines for practices regarding accounting of disclosures and retention of disclosures of PII.

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)

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 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).

4 Policy Requirements

4.1 Accounting of Disclosures

As per KRS 194A.060 Confidentiality of records and reports, CHFS shall protect the confidential nature of all records and reports of the cabinet that directly or indirectly identify a client or patient or former client or patient of the cabinet and ensure that records are not disclosed to or by any person except for:

- To person identified or the guardian, if any, with given consent; or
- Under state or federal law

HIPAA Privacy Rule dictates that organizations are required to maintain an accounting of disclosures for personally identifiable information. An individual has a right to receive an accounting of these disclosures of PII in the six years prior to the date on which the accounting is requested, except for disclosures:

- To carry out treatment, payment, and health care operations
- To individuals of protected health information about themselves
- Pursuant to an authorization
- Incident to a use or disclosure otherwise permitted or required
- For the facility's directory or to persons involved in the individual's care or other notification purposes
- For national security or intelligence purposes
- To correction institutions or law enforcement professionals
- As part of a limited data set in accordance with § 164.514(e)

At a minimum, CHFS agencies shall provide the individual requesting the disclosure a written accounting that includes, but is not limited to:

- The date of the disclosure
- The name of the entity or person who received the information and, if known, the address of the entity or person
- A brief description of the PII disclosed
- A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis of disclosure

If CHFS agencies makes multiple disclosures during the period of disclosures to the same person for a single purpose, the accounting of disclosures may also include the following, in addition to the above:

- The frequency, periodicity, and the number of disclosures made
- The date of the last disclosure during the accounting period

Additionally, if CHFS agencies disclose PII for a research purpose for 50 or more individuals, the accounting may also include the following, in addition to the above:

- The name of the protocol or research activity
- A description of the research activity, including the purpose of research and the criteria for selecting particular records

If CHFS agencies discloses PII of an individual for research purposes, at the request of the individual, they shall assist the individual with contacting the entity that sponsored the research and the researcher.

4.2 Disclosure Retention

CHFS agencies shall maintain within their own departments, at a minimum, an accounting of disclosures that occurred during the six years prior to the date of the request for an accounting, including disclosures made to any associates of CHFS. This excludes the criteria mentioned in section 4.1

Individuals may request an accounting of disclosures for period less than six years from the date of the request of a disclosure.

4.3 Provisioning of Disclosures

CHFS agencies shall act on an individual's request for an accounting no later than 60

days after the request has been received. Within this period, the agencies shall:

- Provide the accounting of disclosures to the individual as requested or;
- Extend the period to provide the accounting by no more than 30 days. In this case, the agency shall provide a written statement of the reasons of the delay and the date by which they will provide the accounting. Agencies may only have one extension for time on a request for accounting.

CHFS agencies shall provide the first accounting of disclosures to an individual in any 12-month period for free. After the first request, the agencies may charge a reasonable fee for each subsequent request for an accounting by the same individual within the 12-month period. If a CHFS agency charges a fee to an individual for an accounting of disclosures, in any case, they must inform the individual in advance of the fee and shall provide an opportunity for the individual to withdraw or modify their request to avoid or reduce the fee.

CHFS agencies shall retain:

- Information defined in Content of the Accounting of Disclosures as mentioned in section 4.1
- Written accounting that is provided to the individual
- The titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals

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 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
- 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