

Commonwealth of Kentucky
Cabinet for Health and Family Services



**Cabinet for Health and Family Services (CHFS)
Privacy Policy**



**CHFS Personally Identifiable Information (PII)
Inventory, Minimum Necessary, and Limited Use**

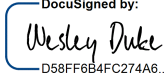
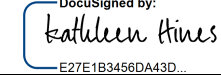
**Version 2.1
05/13/2024**

CHFS Personally Identifiable Information (PII) Inventory, Minimum Necessary and Limited Use Policy	Current Version: 2.1
Category: Policy	Review Date: 05/13/2024

Revision History

Date	Version	Description	Author
09/13/2021	1.0	Original Document	CHFS Privacy Program
05/13/2024	2.1	Revision	CHFS Privacy Office- OLS
05/13/2024	2.1	Revision	CHFS Privacy Office- OLS

Sign-Off

Sign-off Level	Date	Name	Signature
General Counsel (or delegate)	5/24/2024	Wesley Duke	DocuSigned by:  D58FF684FC274A6...
CHFS Chief Privacy Officer (or delegate)	5/28/2024	Kathleen Hines	DocuSigned by:  E27E1B3456DA43D...

CHFS Personally Identifiable Information (PII) Inventory, Minimum Necessary and Limited Use Policy	Current Version: 2.1
Category: Policy	Review Date: 05/13/2024

Table of Contents

2 POLICY OVERVIEW.....6

2.1 PURPOSE6

2.2 SCOPE6

2.3 MANAGEMENT COMMITMENT.....6

2.4 COORDINATION AMONG ORGANIZATIONAL ENTITIES6

2.5 COMPLIANCE6

3 ROLES AND RESPONSIBILITIES7

3.1 AGENCY LIAISONS7

3.2 CHIEF INFORMATION SECURITY OFFICER (CISO)7

3.3 CHIEF LEGAL COUNSEL/GENERAL COUNSEL.....7

3.4 CHIEF PRIVACY OFFICER7

3.5 CHFS OATS INFORMATION SECURITY (IS) TEAM7

3.6 CHFS CONTRACT, STATE, AND VENDOR STAFF/PERSONNEL8

ALL CHFS CONTRACT, STATE, AND VENDOR STAFF/PERSONNEL MUST ADHERE TO THIS PROGRAM. ALL NAMED IN THIS SUBSECTION MUST COMPLY WITH REFERENCED DOCUMENTS THAT PERTAIN TO THE AGENCY’S APPLICATIONS, APPLICATION SERVERS, APPLIANCES, OPERATING SYSTEMS, WEB SERVERS, NETWORK COMPONENTS, AND DATABASE (SERVER AND COMPONENTS) THAT RESIDE ON CHFS/OATS INFORMATION SYSTEM(S).....8

4 POLICY REQUIREMENTS8

4.1 PII INVENTORY8

4.2 PII MINIMIZATION8

4.3 ACCESS AND USE9

4.4 EXCEPTIONS.....10

4.5 DISCLOSURES.....10

4.6 RELIANCE ON MINIMUM NECESSARY ASSURANCES10

4.7 DATA RETENTION AND DISPOSAL.....11

5 THIRD PARTY AGREEMENTS AND BUSINESS ASSOCIATE AGREEMENTS.....11

6 POLICY MAINTENANCE RESPONSIBILITY11

7 POLICY REVIEW CYCLE.....11

8 POLICY REFERENCES11



CHFS Personally Identifiable Information (PII) Inventory, Minimum Necessary and Limited Use Policy	Current Version: 2.1
Category: Policy	Review Date: 05/13/2024

1 Policy Definitions

- **Business Associate:** is 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

CHFS Personally Identifiable Information (PII) Inventory, Minimum Necessary and Limited Use Policy	Current Version: 2.1
Category: Policy	Review Date: 05/13/2024

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.
- 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 chip), 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

CHFS Personally Identifiable Information (PII) Inventory, Minimum Necessary and Limited Use Policy	Current Version: 2.1
Category: Policy	Review Date: 05/13/2024

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 to implement a Minimum Necessary Standard within the organization for PII minimization and inventory. This document establishes the agency's Minimum Necessary Standard, to manage risks and provide guidelines for best practices regarding the restriction of access and use of Protected Health Information (PHI) and Personally Identifiable Information (PII) minimally necessary to accomplish the intended purpose of a disclosure.

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 Office of Legal Services, General Counsel 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

Office of Legal Services (OLS) and Office of Application Technology Services (OATS) coordinate 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).

CHFS Personally Identifiable Information (PII) Inventory, Minimum Necessary and Limited Use Policy	Current Version: 2.1
Category: Policy	Review Date: 05/13/2024

3 Roles and Responsibilities

3.1 Agency Liaisons

Individuals that serve as representatives of their agencies as members of the ODA Data Governance Steering Committee and the CHFS Privacy Advisory Council. These individuals are responsible for the decision-making process alongside General Counsel, CPO, and Executive Advisor for matters related to privacy and data governance. They serve as liaisons between the members of the ODA Data Governance Steering Committee, Privacy Advisory Committee, 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 the program.

3.3 Chief Legal Counsel/General Counsel

Individual(s) from the Office of General Counsel (OGC) 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

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 ODA 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.

CHFS Personally Identifiable Information (PII) Inventory, Minimum Necessary and Limited Use Policy	Current Version: 2.1
Category: Policy	Review Date: 05/13/2024

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 that pertain to the agency's applications, application servers, appliances, operating systems, web servers, network components, and database (server and components) that reside on CHFS/OATS information system(s).

4 Policy Requirements

CHFS employees and contractors must use PII (which, may also include PHI as a subset) properly. They must reduce to the minimum necessary for authorized program performance purposes their use of PII, as well as the volume and types of PII they collect. Members of the workforce must also minimize PII collection and retain PII no longer than necessary to accomplish their program purposes.

Information collected that is subject to the Health Insurance Portability and Accountability Act (HIPAA) must be assessed for potential risks that may compromise the PII/PHI. Completing an inventory of PII is a critical requirement to ensure HIPAA and National Institute of Standards and Technology (NIST) compliance. The HIPAA Privacy Rule also requires covered entities to determine what additional measures need to be in place to mitigate identified risks.

4.1 PII Inventory

A PII Inventory is a catalogue of existing programs and information systems that collect, use, maintain, share, or disclose PII. The PII inventory should also contain potential PII that may be collected, used, and disclosed in the future. CHFS is required to establish, maintain, and update their PII inventory once every three hundred sixty-five (365) days. Each inventory update is completed by a designated responsible party and reported to the Chief Information Security Officer (CISO) and the Chief Privacy Officer (CPO) to support the Cabinet's information security and privacy requirements for all new or modified information systems and programs which contain PII.

CHFS must identify the system locations of PII, from usage to storage, including all employees who have access to and may use data.

4.2 PII Minimization

CHFS must only collect PII elements that are directly relevant and necessary to

CHFS Personally Identifiable Information (PII) Inventory, Minimum Necessary and Limited Use Policy	Current Version: 2.1
Category: Policy	Review Date: 05/13/2024

accomplish the specified purpose(s) and intent of the data collection. CHFS limits collection and retention of PII to the minimum elements identified and when individuals consent to such collection and use. CHFS designated parties are to conduct routine evaluations of PII holdings and schedules regular reviews in collaboration with CHFS Privacy and OATS Security every three hundred sixty-five (365) days to determine the minimum PII necessary is collected.

CHFS must implement appropriate safeguards at all stages of the PII lifecycle and in proportion to the sensitivity of PII. Through the use of security and privacy safeguards, CHFS protects data against theft, loss, copying, modification, or unauthorized access. Privacy Impact Assessments (PIA) are a tool used by CHFS to reduce privacy risks and ensure PII minimization. PIAs should be conducted when CHFS is involved in procuring or initially developing any new technologies or systems that handle or collect personal information as well as revising or updating systems. PIAs may also be conducted when a new rule is implemented that affects personal information. System Security Controls categorized as “High-Major” or “Moderate-Major” require a Privacy Analysis Worksheet (PAW) for all systems, even if the system does not handle or collect personal information. A PIA can assist in determining what information is being collected, why it is being collected, how the data will be used, accessed, shared, safeguarded, and stored. Through the PIA process performed by designated personnel, CHFS can determine PII minimization standards are maintained. CHFS must also minimize duplication and dissemination of electronic files and documents containing PII, making data containing PII only available to employees and partners of CHFS who have a reasonable and appropriate purpose to receive the information.

4.3 Access and Use

To improve the privacy of confidential information that CHFS uses or discloses, CHFS shall ensure the collection and use of PII and PHI is limited to the minimum necessary to accomplish a legitimate purpose authorized by law in accordance with [CHFS Collection, Use, and Retention of Personal Information Policy](#). CHFS will take reasonable efforts to use, disclose, or request only the minimum necessary PII/PHI to accomplish the intended purpose and as authorized by regulation and statute.

Minimum Necessary Use under HIPAA [45CFR 164.502 & 164.514]

- A. Workforce Access: CHFS will identify people or classes of people in its work force who need access to PII/PHI to carry out their duties, the categories of PII/PHI to which access is needed, and any conditions appropriate to such access.
- B. PHI and PII shall only be accessed, used, requested and/or disclosed for job related purposes. CHFS will limit access and use of PHI and PII based on the specific needs and roles of a workforce members’ position, thereby limiting access to that which is required to carry out their duties.
- C. When using, requesting or disclosing PHI/ PII, employees shall make reasonable

CHFS Personally Identifiable Information (PII) Inventory, Minimum Necessary and Limited Use Policy	Current Version: 2.1
Category: Policy	Review Date: 05/13/2024

efforts to limit the use or disclosure to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.

- D. CHFS should not use, disclose, or request an entire medical record unless it is justified as the amount absolutely necessary.

4.4 Exceptions

The following are exceptions to the minimum necessary standard under 45 CFR 164.502(b):

- Disclosures to or requests by a health care provider for treatment;
- Disclosures to the individual or his/her personal representative;
- Uses or disclosures made pursuant to a valid authorization;
- Disclosures made to the Secretary of the United States Department of Health and Human Services for compliance reviews or investigations pursuant to the HIPAA Privacy Rule;
- Other uses or disclosures that required by law; and
- Uses or disclosures that are required for compliance with the HIPAA Privacy Rule.

4.5 Disclosures

Routine and Non-Routine requests or Disclosures:

- A. For routine or recurring requests for disclosures of PII/PHI, CHFS will implement standard protocols where appropriate in order to limit the requests or disclosure to the minimum reasonably necessary.
- B. For any non-routine requests for or disclosure of PII/PHI, the responsible agency should review such requests or disclosures on an individual basis to ensure that it requests or discloses only the minimum necessary PII/PHI. When necessary, request guidance from the Privacy Office.

4.6 Reliance on Minimum Necessary Assurances

CHFS may rely, if reasonable given the circumstances, on a request for disclosure as being for the minimum necessary, if the requester is either a covered entity or a professional (including an attorney or accountant) who provides professional services, either as an authorized member of the CHFS workforce or as a CHFS business associate, who states that the requested information is the minimum necessary in the following circumstances:

- A. The disclosure is made to a public official, permitted to receive information under the HIPAA Privacy Rule under 45 CFR 164.512 (such as a public health authority or law enforcement agency), and the public official represents that the request is for the minimum necessary information;
- B. The request is from another covered entity;
- C. The request is from a professional who is a CHFS workforce member or a CHFS business associate who provides professional services to CHFS.

CHFS Personally Identifiable Information (PII) Inventory, Minimum Necessary and Limited Use Policy	Current Version: 2.1
Category: Policy	Review Date: 05/13/2024

4.7 Data Retention and Disposal

CHFS must retain, dispose of, destroy, erase, and/or anonymize PII, regardless of the method of storage, in accordance with an approved record retention schedule provided by the Kentucky Department of Library and Archives (KDLA) and in a manner that prevents loss, theft, misuse, or unauthorized access in accordance with [CHFS Collection, Use, and Retention of Personal Information Policy](#).

CHFS must use methods to ensure secure deletion or destruction of PII (including originals, copies, and archived records) in accordance with [CHFS OATS Policy: 010.102 Data Media/Security Policy](#)

Section 4.8 Disposal/Destruction for Electronic & Non-Electronic Media. No sensitive or confidential information shall be disposed of by any publicly accessible means. All sensitive or confidential media must be properly disposed of in accordance with [CIO-092 Media Protection Policy](#). The agency/division with the external drive will be responsible for delivering the drive to COT for completion of the disposal process.

5 Third Party Agreements and Business Associate Agreements

HIPAA Privacy Rule allows CHFS to disclose PHI to a "Business Associate" under certain conditions. CHFS will ensure that before any third party receives or accesses PHI that the third party has signed a HIPAA-compliant Business Associate Agreement (BAA), according to the [CHFS Business Associates and Third Party Agreements Policy](#).

6 Policy Maintenance Responsibility

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

7 Policy Review Cycle

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

8 Policy References

- [Centers for Medicare and Medicaid Services \(CMS\) MARS-E 2.2](#)
- [CHFS Business Associates and Third Party Agreements Policy](#)
- [CHFS Collection, Use, and Retention of Personal Information Policy](#)
- [CHFS OATS 010.102 Data Media/Security Policy](#)
- [CIO-092 Media Protection Policy](#)
- [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](#)

CHFS Personally Identifiable Information (PII) Inventory, Minimum Necessary and Limited Use Policy	Current Version: 2.1
Category: Policy	Review Date: 05/13/2024

- Kentucky Information Technology Standards (KITS): 4080 Data Classification Standard
- Kentucky Revised Statute (KRS) Chapter 61.931 *et seq.*
- 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