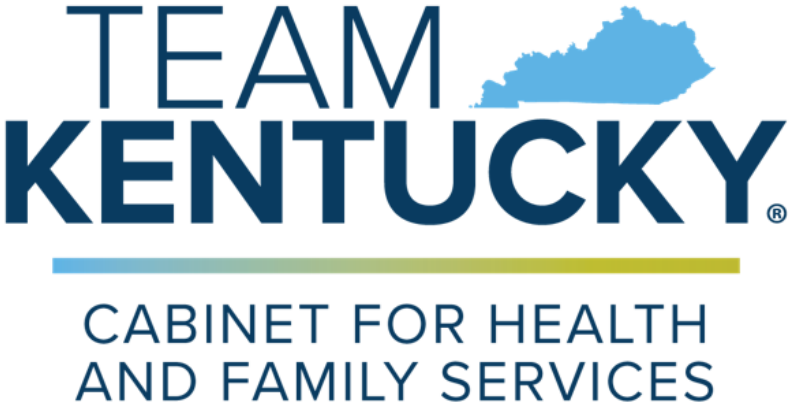
Commonwealth of Kentucky
Cabinet for Health and Family Services

Cabinet for Health and Family Services (CHFS) Information Technology (IT) Policy



010.102 Data/Media Security Policy

Version 3.6
March 4, 2024

Revision History

Date	Version	Description	Author
11/16/2006	1.0	Effective Date	CHFS Policy Charter Team
03/04/2024	3.6	Review Date	CHFS Policy Charter Team
03/04/2024	3.6	Revision Date	CHFS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
Executive Director (or delegate)	03/04/2024	Jeremy Rogers	DocuSigned by: Jeremy Rogers FBFD1DB52F7A404...
CHFS Chief Information Security Officer (or delegate)	03/04/2024	Kelvin Brooks	DocuSigned by: Kelvin Brooks A0F3F24DC182406...

Table of Contents

1 Policy Definitions

- **Business Associate Agreement (BAA):** Contract between a HIPAA-covered entity and a HIPAA business associate (BA).
- **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 (Kentucky Revised Statue 61.878); 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 Media:** Defined by CHFS as physical, electronic media used to store information (ex. diskettes, magnetic tapes, desktops, laptops, hard drives, read only memory, compact disks, thumb drives, mobile devices, tablets, etc.). Laptops and mobile devices will be configured by COT Desktop Support to ensure the maximum level of security necessary to protect any sensitive data downloaded to that drive.
- **Electronic Protected Health Information (ePHI):** Defined by the Health Insurance Portability and Accountability Act of 1996 (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. Identifiable protected 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 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.

- **Media:** Defined by National Institute of Standards and Technology (NIST) 800-53 Revision 4 as Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.
- **Memorandum of Agreement (MOA):** Memorandum of Agreement, program administration contract, inter local agreement to which the Commonwealth is a party, privatization contract, or similar device relating to services between a state agency and any other governmental body or political subdivision of the Commonwealth or entity qualified as nonprofit under 26 U.S.C. sec. 501(c)(3) not authorized under KRS Chapter 65 that involves an exchange of resources or responsibilities to carry out a governmental function. It includes agreements by regional cooperative organizations formed by local boards of education or other public educational institutions for the purpose of providing professional educational services to the participating organizations and agreements with Kentucky Distinguished Educators pursuant to KRS 158.782.
- **Memorandum of Understanding (MOU):** Formal agreement between two or more parties. Companies and organizations can use MOUs to establish official partnerships.
- **Non-Electronic Media**: Defined by CHFS as a hard copy or physical representation of information (ex. paper copies, printouts, drums, microfilm, handwritten notes, etc.).
- **Personally Identifiable Information (PII):** Defined by Kentucky Revised Statute (KRS) Chapter 61.931-934 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, not requiring a combined additional field of information.
- **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.). Production data is prohibited to be accessed by any contract, state, or vendor personnel located

offshore. All users requesting production data must be located within the United States. This applies to all CHFS employees, consultants, temporary personnel, contractors, and other entities that interact with CHFS information related resources. By definition, production data is classified as “production data” when located in any environment. If production data is obfuscated, it is not considered live production data, such as, it may be accessed via offshore personnel.

- **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’s proprietary information including but not limited to intellectual property, financial data and more.
- **Sensitive Financial Data (including PCI):** Defined by Payment Card Industry (PCI) Data Security Standards (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, Card Security Codes such as CAV2/CVC2/CVV2/CID, and PIN(s). CHFS also defines sensitive financial data as 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 with final approval and appointment by the Kentucky Personnel Cabinet.
- **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 security controls through a data/media and security policy. This document establishes the agency's Data/Media Security Policy, to manage risks and provide guidelines for security best practices regarding protecting the agency's data/media.

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 the applicable computer hardware, software, application, configuration, business data, and data communication systems. External vendors or other defined groups/organizations providing information security or technology services may work with the CHFS agency(s) to request exceptions to this policy.

2.3 Management Commitment

Division Directors, the CHFS Chief Technical Officer (CTO), Chief Information Security Officer (CISO), and IT Executive Management 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

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 the official guidance domain for this policy, CHFS agencies abide by the security and privacy requirements established in applicable state laws and regulations as well as federal guidelines outlined in the NIST. Additionally, applicable agencies follow security and privacy frameworks outlined within CMS, IRS, and SSA.

3 Roles and Responsibilities

3.1 Chief Information Security Officer (CISO)

An 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 Information Security (IS) Team

The CHFS 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 Health Insurance Portability and Accountability Act (HIPAA) risk assessments through coordination with the Information Security Agency Representative, the CISO, or CHFS 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 for adherence to this policy.

3.4 Chief/ Deputy Chief Technology Officer (CTO)

This individual makes decisions related to a company's technology. This includes the integration and deployment of new technology, systems management and the overseeing of technical operations personnel. The CTO also works with outside vendors to ensure they meet customer service expectations. This individual is responsible for adherence to this document.

3.5 Security/Privacy Lead

Individuals are designated by the division leadership to coordinate privacy and/or security issues and incidents with all appropriate personnel. This individual(s) is responsible for providing privacy and security guidance for the protection of PII, PCI, ePHI, FTI and other financially sensitive information to all CHFS staff and contractor personnel. This role, along with the CHFS IS team, is responsible for the adherence of this policy.

3.6 CHFS Contract, State, and Vendor Staff/Personnel

All CHFS contract, state, and vendor staff/personnel must adhere to this procedure. All staff/personnel must comply with referenced documents, found in Section 8 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 information system(s).

4 Policy Requirements

4.1 General

All data and media must be sufficiently protected and monitored, consistent with CHFS IT policies and procedures, to prevent unauthorized use, modification, disclosure, destruction, and denial of service. CHFS and Enterprise documentation must apply security controls in a manner that is consistent with the value and classification of the data, as defined. Access to data/media is assigned on the "Principle of Least Privilege", which only allows access/permission necessary to perform their job through an authorized process. Access to data/media shall be subject to approval by appropriate management personnel. All production data must remain within the production environment and must not be manually or electronically copied, reproduced, shared with any party or used in a lower environment without an approved security exception. This policy shall align with all COT enterprise IT policies that pertain to data/media security.

4.2 Data Classification

The Information Technology Management Portal (ITMP) contains a mission critical flag, Business Impact Assessment (BIA) level and sensitive data flags. All CHFS applications will be reviewed by the owner of the data as well as the CHFS IS team to determine its classification and criticality. If the environment has a mixed set of classified data, the classification that requires the most stringent controls must be applied. Any exception to this policy requires approval by the CHFS IS team, see Section 6 Policy Exceptions below.

4.3 External Markings

All sensitive or confidential data/media shall contain external restrictive markings for easy identification as CHFS property. The restrictive markings, including destruction and retention instructions are affixed to all media output to warn users of the degree of protection needed. Media belonging to external vendors, in the possession of CHFS employee/contractors, is subject to the same restrictive markings.

4.4 External Storage Device Acquisition and Process

External storage is not to be used except for that obtained through CHFS procurement process. All storage devices approved for issue shall be encrypted using an acceptable encryption process.

To request an external storage drive, a submission must be made that includes a description of the business need and justification. The request shall be submitted in the Procurement, Payables, and Asset Tracking System (PPATS) for review and approval before the request is made to COT for further processing or approval.

Before receiving a requested storage device, the employee must be informed of

the following:

- The care and stewardship of keeping data secure and the standards for maintaining the access/chain of custody for any external storage device utilized by an employee.
- The employee must annually sign a CHFS Employee Privacy and Security of Protected Health, Confidential and Sensitive Information Agreement (CHFS-219) outlining their responsibilities for the care, stewardship and understanding of the duties and potential penalties for neglecting these responsibilities.

4.5 Reproduction

FTI is never to be printed or otherwise reproduced. When sensitive or confidential cabinet and/or agency data/media is reproduced in total or in part, the reproductions shall bear the same restrictive markings as the original. Reproductions of sensitive or confidential data/media shall be kept to the minimum number of copies required. All CHFS employees and contractors are responsible for ensuring any sensitive or confidential information that is printed to a shared printer, is picked up immediately and stored securely.

If FTI is mistakenly printed or otherwise reproduced:

- Immediately notify the CHFS IS team at CHFSOATSSecurity@ky.gov and the appropriate supervisor to initiate appropriate incident response activity.
- Logging for audit purposes must be performed to properly track all printed or other reproductions of FTI.
- Secure the printed or other reproduced FTI in a locked location protected by a minimum of two secured physical barriers.
- Refer to Section 4.12 Penalties for Failure to Safeguard IRS information

4.6 Storage and Security for Non-Electronic Media

All sensitive or confidential data/media entering or leaving offices, processing areas, or storage facilities must be appropriately secured, such that only authorized access is permitted. Storage solutions such as filing cabinets and/or drawers used for sensitive or confidential data/media shall be secured by a lock. Sensitive or confidential data must be placed behind two barriers of security while being stored.

The IRS in Publication 1075, Section 2.B.1 states, security may be provided for a document, an item, or an area in several ways. These include but are not limited to locked containers of various types, vaults, locked rooms, locked rooms that have reinforced perimeters, locked buildings, guards, electronic security systems, fences, identification systems and control measures. How the required security is provided depends on the facility, the function of the activity, how the activity is organized and what equipment is available. Please refer to the Internal Revenue Services (IRS) Publication 1075 for additional appropriate safeguards for Federal Tax Information

(FTI) data. Refer to Section 4.12 Penalties for Failure to Safeguard IRS information

4.7 Storage and Security for Electronic Media

All sensitive or confidential data/media entering or leaving offices, processing areas, or storage facilities must be appropriately secured, such that only authorized access is permitted. As defined by Enterprise CIO-072: IT Access Control and User Management Policy and Enterprise CIO-092 Media Protection Policy all data/media must be securely stored and protected.

Any personal removable storage devices not issued by the Commonwealth of Kentucky (Commonwealth) are not to be attached to state owned workstations with the purpose of storing and/or retrieving electronic data/media.
As a best practice, computers should be protected within a secured building.

Write to CD/DVD privileges shall be removed as determined necessary from the ability of employees unless a business need can be proven beyond a doubt.

Designated CHFS management, or delegated personnel can perform unannounced inspections to confirm that all external storage devices are being stored and secured properly per guidelines. Inspections may assess the correct labeling and serial number for that device is provided, a proper log of access/chain of custody to the drive has been or is being kept, and that the employee does indeed still have the device. The employee shall produce, on demand the hard drive requested for inspection by CHFS at the exact date and time it is requested, without warning or scheduling.

The IRS in Publication 1075, Section 2.B.1 states, security may be provided for a document, an item, or an area in several ways. These include but are not limited to locked containers of various types, vaults, locked rooms, locked rooms that have reinforced perimeters, locked buildings, guards, electronic security systems, fences, identification systems and control measures. How the required security is provided depends on the facility, the function of the activity, how the activity is organized and what equipment is available. Please refer to the Internal Revenue Services (IRS) Publication 1075 for additional appropriate safeguards for Federal Tax Information (FTI) data. Refer to Section 4.12 Penalties for Failure to Safeguard IRS information

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 Enterprise 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.
Logging for audit purposes must be performed to properly track all FTI.

4.9 Shipping and Manual Handling

CHFS data/media shall not be supplied to vendors, contractors or other external organizations without properly executed contracts, agreements, (i.e., MOU, BAA, MOA, etc.), and confidentiality agreements. Contracts and agreements shall specify conditions of use, security requirements, and return dates. CHFS personnel involved with the movement of media shall document the movement of and the person(s) responsible for such. When shipping sensitive or confidential information, receipt of delivery must be verified with identification and signature proof, unless otherwise action/receipt is required by law or statutory regulation.

4.10 Facsimile Transmission

FTI is never to be transmitted via fax. The CHFS IS team highly recommends that, if possible, no sensitive or confidential data be transmitted via fax. If non-FTI sensitive or confidential data must be transmitted via fax the following safeguards must be followed:

- The recipient must be notified of the time it will be transmitted and agree that an authorized person will be present at the destination machine. Should an authorized person not be present, the fax machine must be in a secured area, such that unauthorized personnel may not access sent/received transmissions (i.e., fax machine is in a locked room with restricted access).
- Always use a coversheet that includes the senders contact information and a confidentiality statement as defined and approved by each agency's management.
- Do not include any sensitive or confidential information on the coversheet.
- Confirm validity of the recipient number before sending.
- Sensitive or confidential CHFS data must not be faxed via non-trusted intermediaries like hotel staff, rented mailbox store staff, etc.
- If fax is sent or received from an incorrect recipient, immediately notify the CHFS IS team at CHFSOATSSecurity@ky.gov.

Following these precautions does not eliminate the risk of faxing. Please note that faxing over a non-secure/non-encrypted line can easily be intercepted.

If FTI is mistakenly received or sent by fax:

- Immediately notify the CHFS IS team at CHFSOATSSecurity@ky.gov and the appropriate supervisor to initiate appropriate incident response activities.
- Logging for audit purposes must be performed to properly track all facsimiles that contain FTI.

- Secure the facsimiles containing FTI in a locked location protected by a minimum of two secured physical barriers.
- Refer to Section 4.12 Penalties for Failure to Safeguard IRS information

4.11 Electronic Transmission (E-mail, File Transfer Protocol, etc.)

FTI is never to be emailed or distributed. Sensitive or confidential data that is to be sent via the internet or other media transmission facility, shall be sent securely via one of the Commonwealth's approved methods (i.e., Encryption, SSL, etc.) in accordance with best practices as defined by Enterprise CIO-091 Enterprise Information Security Program and Enterprise COT-078 COT Cloud Stage Gate Process.

If FTI is mistakenly received or sent via email or other electronic transmission:

- Immediately notify the CHFS IS team at CHFSOATSSecurity@ky.gov and the appropriate supervisor to initiate appropriate incident response activities.
- Logging for audit purposes must be performed to properly track all email or other electronic transmissions that contain FTI.
- Secure email or other electronic transmissions FTI in a locked location protected by a minimum of two secured physical barriers.
- Refer to Section 4.12 Penalties for Failure to Safeguard IRS information.

4.12 Penalties for Failure to Safeguard IRS Information

A. Unauthorized inspection is punishable up to $1,000, or imprisonment of not more than one year, or both, together with the costs of prosecution, per Internal Revenue Code Section 7213A(b). Unauthorized disclosure of Federal income tax returns or return information is a felony offence and may be punishable by a $5,000 fine, five years imprisonment, or both, plus the cost of prosecution, per Internal Revenue Code Section 7213(a);

B. A taxpayer may bring suit for civil damages in a US District Court for unauthorized disclosure or unauthorized inspection of returns and return information, per Internal Revenue Code Section 7431. This Section allows for punitive damages in case of willful inspection or disclosure or gross negligence, as well as the cost of the action. The taxpayer has two years from the date of discovery to bring suit; and

C. These civil and criminal penalties apply to the individual worker even if the unauthorized disclosures or unauthorized inspection were made after employment with the Agency terminated and if the individual is no longer an employee of the Commonwealth of Kentucky.

5 Policy Maintenance Responsibility

The CHFS IS team is responsible for the maintenance of this policy.

6 Policy Exceptions

Any exceptions to this policy must follow the guidance established in CHFS Policy: 070.203 Security Exceptions and Exemptions to CHFS Policies and Security Control 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 Employee Privacy and Security of Protected Health, Confidential and Sensitive Information Agreement (CHFS-219)
- CHFS Policy: 070.203 Security Exceptions and Exemptions to CHFS Policies and Security Control Policy
- Enterprise IT Policy: CIO-072- IT Access Control and User Access Management Policy
- Enterprise IT Policy: CIO- 091- Enterprise Information Security Program Policy
- Enterprise IT Policy: CIO-092- Media Protection Policy
- Enterprise IT Process: COT-078 COT Cloud Stage Gate Process
- Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule
- Internal Revenue Services (IRS) Publication 1075
- Information Technology Management Portal (ITMP)
- Kentucky Information Technology Standards (KITS): 4080 Data Classification Standard
- Kentucky Revised Statue (KRS) Chapter 61: House Bill 5 (HB5)
- 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
- Procurement, Payables, and Asset Tracking System (PPATS)
- Social Security Administration (SSA) Security Information
- U.S. Department of Education Family Educational Rights and Privacy Act (FERPA)