Commonwealth of Kentucky
Cabinet for Health and Family Services

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

040.201 Internal Risk Assessment Policy

Version 1.7
April 9, 2024

Revision History

Date	Version	Description	Author
4/29/2016	1.0	Effective Date	CHFS IT Policies Team Charter
04/09/2024	1.7	Review Date	CHFS Policy Charter Team
04/09/2024	1.7	Revision Date	CHFS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
Executive Director (or delegate)	04/09/2024	Jeremy Rogers	DocuSigned by: Jeremy Rogers FBFD1DB52F7A404...
CHFS Chief Information Security Officer (or delegate)	04/09/2024	Kelvin Brooks	DocuSigned by: Kelvin Brooks A0F3F24DC182406...

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 (Kentucky Revised Statute 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 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 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.
- **Major System Change:** Defined by CHFS as the installation of a new or upgraded operating system, middleware component, or application, modifications to system ports, protocols, or services, installation of a new or upgraded hardware platform, modifications to cryptographic modules or services, and/or modifications to security controls. Examples of significant changes to the environment of operation may

include for example: moving to a new facility, adding new core missions or business functions, acquiring specific and credible threat information that the organization is being targeted by a threat source, and/or establishing new/modified laws, directives, policies, or regulations.

- **Personally Identifiable Information (PII):** Defined by Kentucky Revised Statute (KRS) Chapter 61.931-934and in accordance with National Institute of Standards and Technology (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.
- **Risk:** Defined by NIST SP 800-30 as a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Information System security related risk is one that arises through the loss of confidentiality, integrity, or availability of information or information systems considering impacts to organizational operations and assets, individuals, other organizations, and the Nation.
- **Risk Assessment:** Defined by NIST SP 800-30 as the process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.
- **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.
- **Threat:** Defined by NIST SP 800-30 as any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.
- **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.
- **Vulnerability:** Defined by NIST SP 800-30 as a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

2 Policy Overview

2.1 Purpose

The Cabinet for Health and Family Services (CHFS) must establish a comprehensive level of security controls through a risk assessment policy. This document establishes the agency's Internal Risk Assessment (RA) Policy, which helps manage risk and provides guidelines for security best practices regarding risk assessments, preparation, and strategy.

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.

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

CHFS coordinates with their 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 NIST. Additionally, applicable agencies follow security and privacy frameworks outlined within CMS, the 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 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 Information Security (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.

3.3 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.

3.4 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 PCI, PII, 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 adherence to this policy.

3.6 CHFS Contract, State, and Vendor Staff/Personnel

All CHFS contract, state, and vendor staff/personnel must adhere to this policy. 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).

3.7 System Data Owner and System Data Administrators

Management/lead, or appointed delegate, who works with the application's

development team, to document components that are not included in the base server build and ensures that functionality and backups are conducted in accordance with business needs. This individual(s) is also responsible for working with personnel within the enterprise, agency, application, technical and business areas for providing full recovery of all application functionality as well as meeting federal and state regulations for disaster recovery situations. The System Data Owner, or appointed delegate, is responsible for preparing the annual risk assessment as mandated by the HIPAA Security Rule 45CFR164.308(a)(1)(ii)(A). System Data Owners, or appointed delegate, are also responsible for performing the various steps related to identifying potential risks and threats and are required to ensure that identification of risks is properly categorized and documented in terms of their potential threat to their program area. All information regarding risks to the business systems will be the responsibility of the System Data Owner, or appointed delegate, to document, track and respond whenever appropriate.

3.8 CHFS Security Risk Manager

This position is responsible for the governance of the overall risk assessment program within the Cabinet. This role will provide guidance to program areas in the assessment and identification of potential risks. They will inform, coordinate and assist the System Data Owner with documenting the risks and successful completion of the assessment. The Risk Manager will maintain communication with the System Data Owner and ensure that the schedule of upcoming security control assessments is conveyed so that timely submissions of the assessments are met and completed. The Risk Manager works with the System Data Owner to ensure that all risks be addressed based on National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations for moderate baseline requirements.

4 Policy Requirements

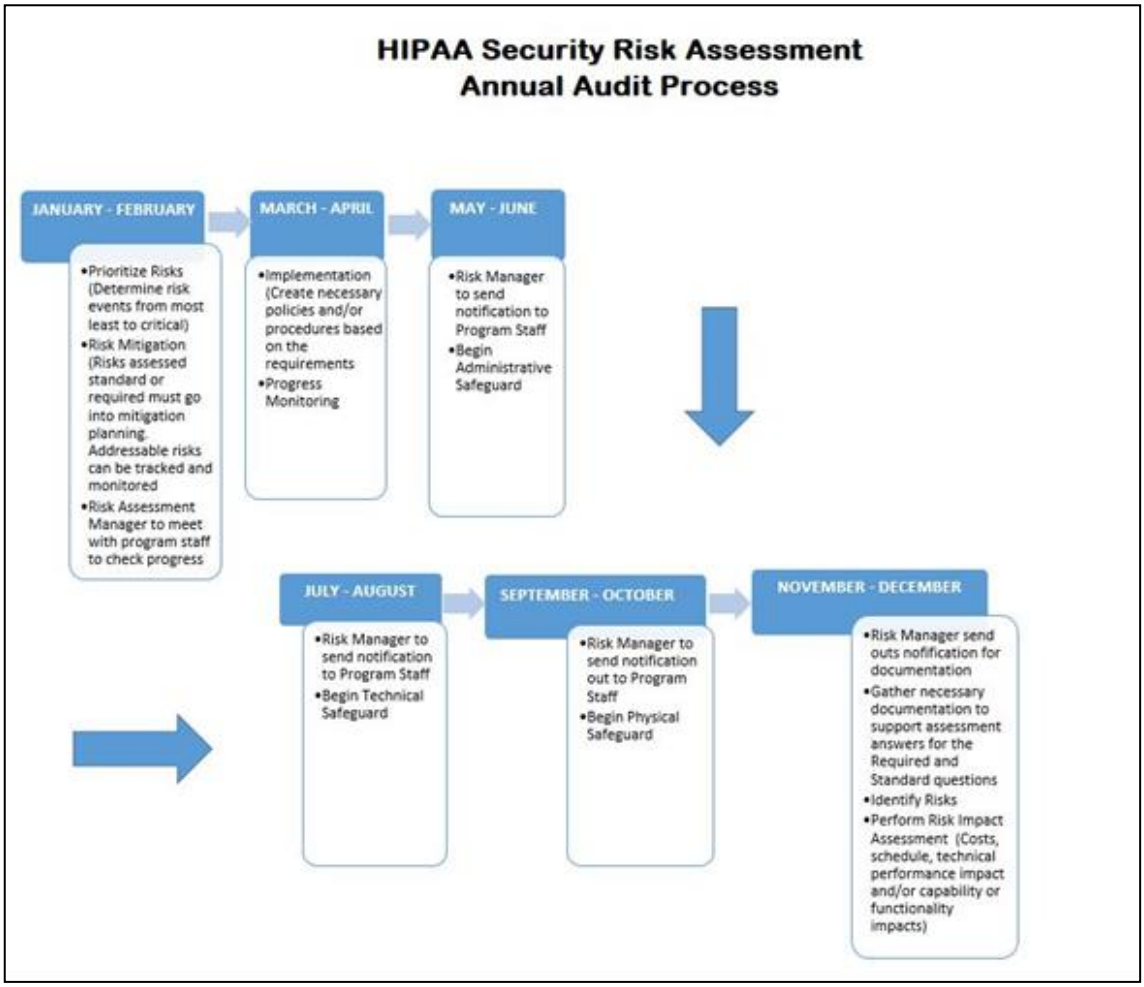
4.1 Risk Assessments

The agency will complete a risk assessment on all applicable privacy and security controls prior to new application inception, at the time of any major system change and at least once annually. Risk assessments provide a mechanism for reaching a consensus as to which risks are the greatest and what steps are appropriate for mitigating them. This approach makes it more likely that the System Data Owners will understand the need for agreed-upon controls, the controls are aligned with their systems and support the effective implementation. These assessments will be conducted in accordance with the National Institute of Standards and Technology (NIST) Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments and the HIPAA Security Rule, 45CFR164.308(a)(1)(ii)(A).

Additional guidelines for Risk Assessments can be found within the Enterprise CIO-093 Risk Assessment Policy and the CHFS Risk Assessment Program Procedure.

4.2 Risk Assessment/Annual Audit Process

An annual risk assessment is to be conducted by the System Data Owners for each system that contains ePHI. After the assessment is conducted, it is the sole responsibility of the System Data Owners to mitigate risks found. A mitigation plan strategy must be presented to the CHFS Security Risk Manager outlining what steps are being taken to eliminate the risk. All activity will be tracked using the Archer governance tool or other comparable method. An assessment completion record shall be entered into Information Technology Management Portal (ITMP). If using Archer, notifications are sent to the System Data Owners to start the process of mitigating the identified risk.



4.3 Cyber Security Framework (CSF) Components: CSF vs RMF

Organizations can use the Cybersecurity Framework (CSF) to complement the existing NIST Risk Management Framework (RMF). The CSF was developed under Presidential Executive Order 13636. The RMF is part of a suite of risk management standards and practices developed in response to the Federal Information Security Modernization Act (FISMA), as amended in 2014. The CSF Framework is to be used in conjunction with the CHFS risk management process and cybersecurity program. CHFS can use its current risk assessment processes and leverage the CSF to identify opportunities to strengthen and communicate its management of cybersecurity risk. Assessments using the RMF can use aspects of the CSF to strengthen the RMF activities, which are not impacted by the CSF.

Each agency will be subject to ongoing internal security control assessments. The NIST control families are initiated by utilizing pre-defined procedures and the NIST CSF. These assessments shall:

- Identify Risk.
- Leverage existing assessments.
- Obtain evidence (evidentiary artifacts) that items identified in policy/procedure directives are being carried out.
- Enable artifact validation.
- Help determine residual risk.
- Enable gap analyses.

Initiate risk treatment as necessary.

5 Policy Maintenance Responsibility

The 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 Policy: 070.203- Security Exceptions and Exemptions to CHFS Policies and Security Control Policy
- CHFS Procedure: Risk Assessment Program Procedure
- Enterprise IT Policy: CIO-093 Risk Assessment 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)
- National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity
- National Institute of Standards and Technology (NIST) Special Publication 800-18 Guide for Developing Security Plans for Federal Information Systems
- National Institute of Standards and Technology (NIST) Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments
- National Institute of Standards and Technology (NIST) Special Publication 800-37 Risk Management Framework for Information Systems and Organizations
- National Institute of Standards and Technology (NIST) Special Publication 800-39 Managing Information Security Risk
- National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- National Institute of Standards and Technology (NISTIR) 8170 The Cyber Security Framework Implementation Guidance for Federal Agencies
- Presidential Executive Order 13636: Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive (PPD) 21 Critical Infrastructure Security and Resilience
- Payment Card industry (PCI) data Security Standard (DSS) Requirements and Security Assessment Procedures Version 3.2.1
- Social Security Administration (SSA) Security Information
- U.S. Department of Education Family Educational Rights and Privacy Act (FERPA)