CHFS-219V	
External Auditor Access Request Procedure	Current Version: 2.7
Category: Form	Review Date: 9/19/2023

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

CONTRACTOR PRIVACY AND SECURITY OF PROTECTED HEALTH, CONFIDENTIAL AND SENSITIVE INFORMATION AGREEMENT FORM FOR EXTERNAL VENDORS (CHFS-219V)

PLEASE PRINT:

[User Information and Vendor Company Name Here]

Last Name, First Name & MI Company Name

This agreement is entered into by the individual employee of **[Vendor Company Name Here]**, as identified - above, in connection with and subject to the Contract for **[Contract Name/Master Agreement Number]** between the Commonwealth of Kentucky Cabinet for Health and Family Services **[add additional agency names here or none]** and **[Vendor Company Name Here].**

I understand that I may be allowed access to confidential information and/or for records in order that I may perform my specific contract duties. I further understand and agree that I am not to disclose confidential Information and/or records without the prior consent of the appropriate authority(ies) in the Cabinet for Health and Family Services.

I understand that all CHFS vendor positions are considered to be assigned a high-risk designation based on potential access to and viewing of various data types, including but not limited to, protected health, confidential, sensitive and personally identifiable information.

I understand that certain vendor positions work-related duties involve access to or use of federal tax information and that these positions are considered to be assigned a critical-risk designation.

I understand that background screening and rescreens of vendor employees are periodically performed by the vendor based on the considered risk-designation of their position duties and that a formal determination will be made whether an additional background screening is required when a vendor employee is transferred, reclassified or promoted, or their job duties are changed.

I understand that all user id/passwords to access computer data are issued on an individual basis. I further understand that I am solely responsible for all information obtained, through system access, using my user id/passwords. At no time will I allow use of my user id/passwords by any other person. I understand my compliance is required, and that intentional or inappropriate misuse may result in dismissal from the project. **I understand**

that I should never respond to any messages asking for my password, username or personal information and to never open or download an email attachment unless I know that the sender is legitimate.

I understand that accessing or releasing confidential information and/or records or causing confidential information and/or records to be accessed or released to myself, other individuals, clients, relatives, etc., outside the scope of my assigned job duties would constitute a violation of this agreement and may result in a prohibition from further work on the project. I further understand that as a vendor employee, I may subject myself to civil and criminal liability pursuant to federal and Kentucky law for the disclosure of confidential information to unauthorized persons. I understand all data, information, documents, etc. belong to the Cabinet and I agree not to take any information in any form from the agency during the course of my work or upon termination of the contract.

I understand that the following is not an exhaustive list of all confidential information but is an attempt to include most of the major examples of such information. In the event of doubts about whether certain information is covered by confidentiality requirements, I understand that I should consult the contract manager.

Under KRS 194A.060, all records and reports of the Cabinet which directly or indirectly Identify a patient or client, or former patient or client, of the Cabinet or the Cabinet by a former name (CHR, CHS, CFC) are confidential.

Under KRS 209.140, all information regarding an adult protective service investigation is confidential.

Under KRS 216.530 all inspections of long-term care facilities shall be unannounced.

Under HIPAA, an individual's health care information must be used by the Cabinet and its employees and agents only for legitimate health purposes like treatment and payment. 45 C.F.R. § 160.101 and 160.103 at seq. and specifically §§ 164.500, 164.501, 164.502(a), 164.514 established standards for privacy of health information under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Health Information that must be kept private and secure is called Protected Health Information (PHI). HIPAA establishes in Federal Law the basic principle that an individual's medical records belong to that individual and, with certain exceptions, cannot be used, released or disclosed without the explicit permission of that individual or their legal guardian. This includes disclosing PHI in even casual or informal conversation not related to a legitimate health purpose (like treatment or payment) at any time whether at work or not. HIPAA gives consumers of Cabinet programs and services the right to an explanation of their privacy rights, the right to see his/her medical records (with some exceptions), the right to request corrections to these records, the right to control the release of information from their records with some exceptions, and the right to documented explanations of disclosures by the Cabinet and by others who may have

access to this information. Those who violate the rules laid down by HIPAA are subject to federal penalties. For non-criminal violations of the privacy standards, including disclosures made in error, there are civil monetary penalties of $100 per violation up to $25,000 per year, per standard. Criminal penalties are imposed for violations of the statute that are done knowingly (on purpose) — up to $50,000 and one year in prison for obtaining or disclosing protected health information; up to $100,000 and up to five years in prison for obtaining or disclosing protected health information under "false pretenses;" and up to $250,000 and up to 10 years in prison for obtaining protected health information with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm.

Under KRS 214.420 and 214.625, all information in the possession of local health departments or the Cabinet concerning persons tested for, having, or suspected of having sexually transmitted diseases, or identified in an epidemiologic investigation for sexually transmitted diseases, is strictly confidential. A general authorization for the release of medical or other information is not sufficient to authorize release of this information. Breach of this confidentiality is considered a violation under KRS 214.990(6).

Under KRS 214.181, no test results relating to human immunodeficiency virus are to be disclosed to unauthorized persons.

Under KRS 222. 271 and 42 C.F.R. part 2, treatment records of alcohol and drug abuse patients are confidential and a general authorization for release of this information is ineffective.

Under KRS 216.2927, raw data used by the Kentucky Health Policy Board are confidential. This includes data, data summaries, correspondence, or notes that could be used to identify an individual patient, member of the public, or employee of a health care provider.

Under KRS 202A.091, court records relating to hospitalization of the mentally ill are confidential. Violation of the confidentiality of these records is a Class B misdemeanor under KRS 202A.991.

Under KRS 202B.180, court records related to mental retardation admissions are confidential. Violation of the confidentiality of these records is a Class A misdemeanor under KRS 202B.990.

Under KRS 210.235, all records which directly or indirectly identify any patient, former patient, or person whose hospitalization has been sought are confidential.

Under KRS 211.902, the names of individuals are not to be disclosed in connection with lead poisoning records, except as determined necessary by the Cabinet Secretary.

Under KRS 211.670, lists maintained by hospitals, and all information collected and

analyzed, relating to the Kentucky birth surveillance registry (concerning birth defects, stillbirths, and high risk conditions) are to be held confidential as to the identity of the patient. Violation of this confidentiality is a Class A misdemeanor under KRS 211.991.

Under KRS 213.131, unauthorized disclosure or inspection of vital records is unlawful. Violation of the confidentiality laws for vital statistics is a Class B misdemeanor under KRS 213.991.

Under KRS 199.570, all adoption files and records are confidential and are not open to any person or entity that does not meet the requirements of KRS 199.572, except upon order of the court which entered the judgment of adoption.

Under KRS 205.175, all public assistance communications, both written and oral, generated during the course of business are confidential and privileged. KRS 205.835 prohibits the unauthorized use of information by an employee.

Under KRS 205.730(6), all child support parental locator information is confidential.

Under KRS 205.735, all child support Information supplied by an employer is confidential.

Under KRS 205.796, no employee or agent of the Commonwealth shall divulge confidential child support records unless the disclosure is authorized in a manner prescribed by KRS 205.715.

Under KRS 205.8465(4), no employee of the state Medicaid Fraud Control Unit, the Office of the Attorney General, the Office of the Inspector General, or the Cabinet for Health and Family Services shall notify the alleged offender of the identity of the person who in good faith makes a report required or permitted by KRS 205.8451 to 205.8483, nor shall the employee notify the alleged offender that a report has been made alleging a violation of KRS 205.8451 to 205.8483 until such time as civil or criminal proceedings have been initiated or a formal investigation has been initiated. Any information or report concerning an alleged offender shall be considered confidential in accordance with the Kentucky Open Records Law, KRS 61.870 to 61.884.

Under KRS 434.853, accessing any computer or computerized information without authorization, or causing any such access without authorization, is a Class B misdemeanor. In addition, under the Computer Fraud and Abuse Act, 18 U.S.C. Section 1030: Intentionally accessing a computer without authorization or exceeding authorized access and obtaining information is a misdemeanor.

Under KRS 610.340, all juvenile court records are confidential and shall not be disclosed to unauthorized persons unless ordered by a court for good cause.

Under KRS 620.050, all child protective service investigative records are confidential and shall only be released in accordance with the provisions set forth in KRS 620.050.

Under KRS 625.045, any and all records in a voluntary termination action are confidential and shall only be open to inspection with a written order or as authorized by the provisions of KRS Chapter 199.

Under KRS 625.108, any and all records in an involuntary termination action are confidential and shall only be open to inspection with a written order or as authorized by the provisions of KRS Chapter 199.

Under 7 C.F.R. 272.1 (c), all Food Stamp records are confidential and may only be used or disclosed in accordance with the provision set forth in 7 C.F.R. 272.1 (c).

Confidentiality of family planning services is required by 42 C.F.R. § 59. Section 59.11 states: “All information as to personal facts and circumstances obtained by the project staff about individuals receiving services must be held confidential and may not be disclosed without the individual's consent, except as may be necessary to provide services to the patient or as required by law, with appropriate safeguards for confidentiality: Otherwise, information may be disclosed only in summary, statistical, or other form which does not identify particular individuals.” The confidentiality rules applicable to all programs or projects supported in whole or in part by federal financial assistance, whether by grant or by contract, are found at 42 C.F.R. § 50.310, which states: “Information in the records or in the possession of programs or projects which is acquired in connection with the requirements of this subpart may not be disclosed in a form which permits the identification of an individual without the individual's consent, except as may be necessary for the health of the individual or as may be necessary for the Secretary [of Health and Human Services] to monitor the activities of those programs or projects. In any event, any disclosure shall be subject to appropriate safeguards which minimize the likelihood of disclosures of personal information in an Identifiable form.”

Under 42 C.F.R. § 431.305, the following types of information relating to Medicaid applicants and recipients are confidential: “(1) Names and addresses; (2) Medical services provided; (3) Social and economic conditions or circumstances; (4) Agency evaluation of personal information; (5) Medical data, including diagnosis and past history of disease or disability; (6).Any information received for verifying income eligibility and amount of medical assistance payments (see Sec. 435.940ff), income information received from SSA or the Internal Revenue Service must be safeguarded according to the requirements of the agency that furnished the data, and; (7) Any information received in connection with the identification of legally liable third party resources under Sec. 433.138 of this chapter.” Under 42 C.F.R. 431.306, all Medicaid records of applicants and recipients may only be released in accordance with the provisions set forth in 42 C.F.R. 431.306.

Under 45 C.F.R. 205.50, all financial assistance-programs’ records are confidential and

may only be released In accordance with the provisions set forth in 45 C.F.R. 205.50.

Under Internal Revenue Code (6103, 7213, 7213A, 7431) all federal tax information is confidential. Unauthorized disclosure or inspection is punishable up to $1,000, or imprisonment of not more than one year, or both, together with the costs of prosecution. Unauthorized disclosure of Federal income tax returns or return information is a felony offense and may be punishable by a $5,000 fine, five years imprisonment, or both, plus the cost of prosecution. Regarding criminal penalties for unauthorized disclosure of Social Security Administration (SSA) data with applicable rules and regulations:

Act, 5 U.S.C. Â§ 552a (i)(1) Criminal Penalties.

- Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain **individually identifiable information** the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, **willfully discloses** the material in any manner to any person or agency not entitled to receive it, shall be guilty of a **misdemeanor** and as described below.

- Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more than $5,000.

- Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency **under false pretenses** shall be guilty of a **misdemeanor** and fined not more than $5,000.

I understand that other types of information may also be protected by confidentiality, and that if in doubt as to confidentiality, I should not volunteer information before making certain that the information may be disclosed.

By affixing my signature to this document, I acknowledge that I have been apprised of the relevant laws, regulations, and policies concerning access, use, maintenance, and disclosure of confidential information and/or records which shall be made available to me through my work for the Cabinet for Health and Family Services. I further agree that it is my responsibility to assure the confidentiality of all Information that has been issued to me both during the course of the contract and after the contract with the agency has ended.

I have read the above, received a copy of the COT F 011 (OR include the document within this CHFS-219V like the Internet and Email Acceptable Use language) Cabinet's Confidentiality Policy (219V), and understand my responsibilities. I have also read the affixed copy of the CHFS Office of Human Resources (OHRM) Personnel Handbook Section 2.4 Internet and Electronic Mail Acceptable Use Policy and understand my responsibilities with regard to this policy. I also agree to ensure that my computer equipment provided by my employer, **[Vendor Company Name Here]**, stays updated with virus protections and Operating System patches while working on this contract.

Contractor Signature Date

As project manager for **[Vendor Company Name Here]**. I confirm that the **[Vendor Company Name Here]** employee named above has been made aware of the CHFS Confidentiality Policy (219V) and understands his/her responsibilities. The **[Vendor Company Name Here]** employee has also been made aware of his/her responsibilities as they relate to the CHFS Office of Human Resources (OHRM) Personnel Handbook Section 2.4 Internet and Electronic Mail Acceptable Use Policy and understand my responsibilities with regard to this policy. The person named is a **[Vendor Company Name Here]** employee and **[Vendor Company Name Here]** is responsible for their actions.

Project Manager Signature Date

The contractor provided an up-to-date screenshot of their equipment being used showing the current virus software and definitions and it is deemed to be updated as of the work start date.

CHFS DIRECTOR or Security Official Date

Cabinet for Health and Family Services (CHFS)
Office of Human Resource Management (OHRM)
Personnel Procedures Handbook

2.4 Internet and Electronic Mail Acceptable Use Policy

I. **Purpose**
CHFS employees are encouraged to use the Internet (which includes the intranet) and e-mail appropriately and to their full potential to further the CHFS mission and provide high-quality service. Supervisors will help employees determine appropriateness of Internet and e-mail use for professional activities and career development during working hours. Employees may not use the Internet or e-mail for personal gain. **Internet and e-mail are state resources and employees have no right or expectation of privacy using these resources.** The Commonwealth Office of Technology (COT) *CIO-060 policy* is the base policy for the Commonwealth. This policy is in addition to CIO-060 to enforce more restrictive policies.

CHFS will work with COT to review CHFS Internet use within CHFS (refer to Internet Blocking and Reporting below).

Each department is responsible for ensuring its employees are aware of this policy. Employee compliance is required. Intentional inappropriate or excessive use may result in disciplinary action, up to and including dismissal.

II. **Scope**
This policy applies to all CHFS employees and contract employees, including all persons providing contract services (here-in-after referred to as "employees") who access the Internet and/or the state e-mail system.

III. **Policy/Procedure Maintenance Responsibility**
The CHFS OATS Security and Audit Section is responsible for the maintenance of this policy. The COT shares responsibility with CHFS for the maintenance of and compliance with this policy which applies to all executive branch agencies and employees.

IV. **Applicability**
All CHFS employees shall adhere to the following requirements.

V. **Exceptions**
Any exceptions to this policy must follow the procedure established in CHFS IT Policy #070.203.

VI. **Employee Responsibilities**
1. Read, acknowledge, and sign the CHFS 219V form before using these resources.
2. Employees will use their access to the Internet and e-mail responsibly and in compliance with applicable laws and regulations.
3. Employees must encrypt all e-mail and attachments containing sensitive or confidential information during transit outside of the state network

(including a non ky.gov address) with approved security services or encryption tools. See CHFS IT Policy #010.102-Data Media Security for a more detailed definition of confidential information.

4. As with other forms of publications, copyright restrictions/regulations are to be observed.
5. Employees should be mindful that information published online or via e-mail reflects on the reputation of the Commonwealth. Employees must accurately and honestly represent themselves, their departments, and other state departments through electronic information or service content.
6. Incidental personal use of Internet and e-mail resources are permissible, but not encouraged. Excessive personal use shall lead to loss of the resource privileges and may result in disciplinary action pursuant to KRS 18A. 095, up to and including dismissal. Employees are responsible for exercising good judgment regarding incidental personal use. Any incidental personal use of Internet or e-mail resources must adhere to the following limitations:
    a. It must not cause any additional expense to the Commonwealth or the employee's agency.
    b. It must be infrequent and brief.
    c. It must not have any negative impact on the employee's overall productivity.
    d. It must not interfere with the normal operation of the employee's agency or work unit.
    e. It must not compromise CHFS or the Commonwealth in any way; and
    f. It must be ethical and responsible.
7. All CHFS employees and onsite contract employees are prohibited from installing or utilizing unapproved browsers on CHFS workstations. Requests for exceptions must be submitted following the procedures outlined in CHFS IT Policy #070.203.

VII. Supervisor Responsibilities

1. Supervisors are required to identify Internet and e-mail training needs and resources, to encourage use of the Internet and e-mail to improve job performance, to support staff attendance at training sessions, and to permit use of official time for maintaining skills, as appropriate.
2. Supervisors are expected to work with employees to determine the appropriateness of using the Internet and e-mail for professional activities and career development, while staying within the general provisions of this policy, which prohibit using the Internet and e-mail for personal gain.
3. If inappropriate or excessive use of the Internet or e-mail is suspected, supervisors may request a report of the Internet usage and e-mail review.

VIII. Unacceptable Uses

Use of state Internet and e-mail resources is a privilege that may be revoked for inappropriate use. Any abuse of acceptable use policy may result in revocation of access, notification of department management, and disciplinary action, up to

and including dismissal.

Examples of inappropriate use include, **but are not limited to**:

1. Excessive non work-related activity.
2. Use of the Internet and e-mail for personal gain or personal business activities of a commercial nature such as buying or selling commodities or services with a profit motive. This would include eBay and other personal selling of merchandise.
3. Engaging in illegal activities or use for any illegal purposes, including initiating or receiving communications that violate any laws and regulations, including KRS 434.840-434.860 (Unlawful Access to a Computer) and KRS 512.020 (Criminal Damage to Property Law). This also includes malicious use, spreading of viruses, and hacking (gaining or attempting to gain unauthorized access to any computers, computer networks, databases, data, or electronically stored information).
4. Using resources to actively engage in procuring or transmitting material that is in violation of sexual harassment or anti-discrimination laws, whether through language, frequency, or size of messages. This includes printing or transmitting statements, language, images, e-mail signatures, or other materials reasonably likely to be perceived as offensive or disparaging of others based on race, color, national origin, gender, sexual orientation, individuals aged 40 and older, pregnancy, veterans, qualified special disabled veterans, gender identity, ancestry, qualified individuals with a disability, religion, genetic information, political affiliation, or status as a smoker.
5. Use of abusive or objectionable language in either public or private messages.
6. Knowingly visiting pornographic or illegal sites or disseminating, soliciting, or storing sexually oriented messages or images.
7. Misrepresentation of oneself, falsifying origin of identity or misrepresenting the Commonwealth, including the use of false or misleading addressing of subject headers in the distribution of e-mail or presentation of information.
8. Using the e-mail account of another employee without receiving written authorization or delegated permission to do so.
9. Forging e-mail headers to make it appear as though an e-mail came from someone else.
10. Sending or forwarding chain letters, pyramid schemes of any type, or other similar non-business related information.
11. Making fraudulent offers of products, items, or services originating from any Commonwealth account.
12. Distributing or forwarding unsolicited commercial e-mail.
13. Soliciting money for religious or political causes, advocating religious or political opinions, or endorsing political candidates.
14. Using official dissemination tools to distribute personal information including any information that constitutes an unwarranted invasion of personal privacy as defined in the Kentucky Open Records Act, KRS

61.870.

15. Violating the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, including but not limited to, the downloading, installation, or distribution of pirated software, digital music, and video files.
16. Online investing, stock trading, and auction services (such as eBay, eTrade, or Ameritrade) unless the activity is for Commonwealth business.
17. Developing or maintaining a personal Web page on or from a Commonwealth device.
18. Using of peer-to-peer (referred to as P2P) networks.
19. Non-business-related posting on blogs or any other interactive media is strictly prohibited.
20. Other activities and/or non-business-related activities that will cause congestion and disruption of networks and systems. This includes, but is not limited to:
    a. Internet games.
    b. Online gaming.
    c. Unnecessary Listsrv subscriptions and e-mail attachments; and
    d. Unnecessary chat rooms/social networking, instant messaging, or social media platforms.
    e. Unnecessary printing, such as printing non work-related material.
    f. Unnecessary downloading of electronic files, such as music, audio, video, or other similar streaming programs, storage of inappropriate data files on computer workstations, computing devices on CHFS servers.

IX. E-mail

No employee shall be given, or shall assume, any right to privacy with regard to the use of the state e-mail system.

Email operated by the Commonwealth is not to be considered a secure channel for sending/receiving sensitive, confidential data or Protected Health Information (PHI) to external agencies. Microsoft Outlook e-mail does not employ true encryption and is susceptible to being intercepted and read. Therefore, e-mailing of unencrypted PHI to agencies outside of the Commonwealth's network is forbidden. E-mailing PHI between state agencies when both are on the Commonwealth's Microsoft Exchange e-mail system is permitted (see CHFS IT Policy #010.102). **Federal tax information (FTI) and HIV information always must be encrypted when e-mailed internally or externally.**

X. Confidentiality Notice

All outgoing CHFS e-mail traffic must include a confidentiality notice at the end of the messages. No additional text or graphics (e.g. stationary, GIF's, etc.) may be used because of the additional amount of storage and network resources they consume, with the exception of work-related notices in text and/or links related to the employee's duties and programs.

The confidentiality notice is:
This email message, including any attachment, is for the sole use of the intended recipient(s) and may contain confidential information. Any unauthorized review, use, disclosure, or distribution is strictly prohibited. If you are not the intended recipient, please contact the sender by e-mail and destroy all copies of the original message.

XI. **Microsoft Outlook Public Folders**

The Public Folder resources within the Commonwealth's e-mail system should be used only to share public information that is not considered sensitive and/or confidential. No information that contains confidential or PHI information should ever be posted to a Public Folder. Each owner of a Public Folder will be responsible to ensure that information posted to that folder complies with this policy. The CHFS OATS IT Security and Audit Section and COT will audit Public Folders for compliance.

XII. **Internet and E-mail Monitoring, Reporting, and Blocking**

1. **Monitoring -** CHFS efforts to prevent Internet use include tools to monitor Internet activity. COT will monitor, report, and in some cases, block Internet use by CHFS employees. The CHFS OATS IT Security and Audit Section is responsible for monitoring individual users identified by supervisors and monitoring approved by OHRM.

   COT has the responsibility to monitor CHFS Internet and bandwidth use. COT will forward Cabinet-wide Internet usage summary reports to the CHFS Chief Information Officer (CIO) for review. Copies of the summary report will be forwarded to OHRM upon request.
2. **Reporting -** If employees are suspected of inappropriate or excessive Internet or e-mail use, supervisors may request reports of employees' usage. This request must come from the employees' supervisor (or higher) and be forwarded to OHRM. If approved, the request is forwarded to the CHFS CIO and OATS IT Security and Audit Section for processing. When the report is forwarded by COT, the CHFS OATS IT Security Section shall review and forward the report to OHRM.

3. **Blocking -** COT is responsible for the overall state blocking of Internet sites that are categorized as inappropriate web sites. These categories may include, but are not limited to: Instant Messaging and Chat Rooms, download sites, personal ads and dating sites, public proxy, pornography, gambling, and Internet e-mail. CHFS OATS CIO will help COT determine which categories are appropriate or inappropriate for CHFS.

   All inappropriate sites cannot be blocked through this automated

process. Employees should remain aware that intentionally visiting or downloading information from an inappropriate site that has not been blocked is against CHFS policy.

COT assigns an individual to a specific filtering group as established by the Cabinet CIO.

Based on specific agency functions and needs, work-related Internet sites may be unintentionally blocked based on standard criteria. To request access to a blocked site, e-mail your supervisor with the request and accompanying justification. The supervisor will, in turn, e-mail their directors with a recommendation and directors will approve or deny the request. Approved requests must be e-mailed to the CHFS OATS IT Security Section (CHFSOATSSecurity@ky.gov) for final disposition. If requests are approved by COT, the block will be removed and the user notified by e-mail.

Effective Date: 11/1/2004
Last Revised Date: 9/18/2023