Purpose:

As a KDADS employee, you may receive or create certain health or medical information (Protected Health Information or "PHI") in connection with the performance of your job related to individuals that receive services through the agency. The intent of this policy is to provide information and set forth the expectation for the collection, use, and disclosure of PHI in order to facility oversight and provide services, while maintaining reasonable safeguards to protect the privacy of the individual's information. It is the responsibility of all KDADS' employees to safeguard all PHI.

Table of Contents

General Policy:

1. KDADS may collect or maintain information about individuals to the extent needed to administer KDADS programs and services.
2. KDADS may not use or disclose PHI unless there is a valid authorization by the individual or unless an exception allows for such use or disclosure under state/federal laws or regulations. *See the Use and Disclosure section and Minimum Necessary of this policy for more information.*
3. KDADS shall safeguard all confidential information and PHI about individuals, inform individuals about privacy practices and respect individual privacy rights, to the full extent required under this policy and by state/federal laws and regulations. *See the Individual Privacy Rights section and Safeguards section of this policy for more information.*
4. The KDADS workforce shall utilize the ***KDADS Authorization for Release of Protected Health Information*** form. Forms not approved by KDADS may not be used when KDADS is seeking the authorization.

5. All of the KDADS workforce shall complete KDADS approved HIPAA training at least on an annual basis. Additional trainings may be required.
6. KDADS workforce shall report compliance concerns immediately to supervisors. If a supervisor is unable or fails to respond to reported compliance concerns, the reporting employee shall elevate the concern to the next level of management staff immediately. Unresolved concerns must be reported to the compliance officer in the KDADS Legal Division.

Glossary

- Agency: Kansas Department for Aging and Disability Services ("KDADS")
- Business Associate: A separate entity, working for or on behalf of the KDADS, that creates, receives, maintains, or transmits protected health information ("PHI") or provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services where the provision of service involves the disclosure of PHI.
- Covered Entity: Refers to, but is not limited to, health plans, healthcare clearinghouses, healthcare providers, and hybrid entities.
- Disclose/Disclosure: The release, transfer, relay, provision of access to, or conveying an individual's information to any person or entity outside of KDADS.
- Healthcare: Care, services or supplies related to the health of an individual. Healthcare includes, but is not limited to: preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care; and assessments.
- Health Information: any information, including genetic information, whether oral or recorded in any form or medium, that: is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearing house; and relates to past, present, or future payment for the provision of health care to an individual.
- Healthcare Operations: Any of the following activities of KDADS to the extent that the activities are related to covered functions:
    - Conducting quality assessment and improvement activities, including income evaluation and development of clinical guidelines, population-based activities related to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and customers with information about treatment alternatives; and related functions that do not include treatment.
    - Reviewing the competence of qualifications of healthcare professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students and trainees in areas of healthcare learn under supervision to practice or improve their skills, accreditation, certification, licensing, or credentialing activities.
    - Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs.
    - Business planning and development, such as conducting cost-management and planning analysis related to managing and operating KDADS.
    - Business management and general administrative activities of KDADS, including but not limited to:
        - Management of activities relating to compliance with the requirements of HIPAA.
        - An individual's services, including the provision of data analysis.
        - Resolution of internal grievances, including the resolution of dispute(s) from program participants regarding the care and services.
        - Creating de-identified data or a limited data set.

- Health Oversight Agency: An agency, such as KDADS, or a person or entity under a grant of authority or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

- HIPAA: Health Insurance Portability and Accountability Act of 1996 and HITECH, and the federal regulations adopted to implement the Act, and amendments thereto.

- Hybrid entity: A single legal entity that is a covered entity. The entity's business practices include both covered and non-covered functions.

- Individual: The person receiving services from KDADS and/or KDADS business associates and who is the subject of information collected, used or disclosed by KDADS and/or KDADS business associates.

- Individually Identifying Information: A subset of health information, which identifies the individual or there is a reasonable belief that the information can be used to identify the individual, that includes demographic information collected from an individual and is created or received by a health care provider, health plan, employer, or healthcare clearing house. The information relates to past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual or the past, present, or future payment for the provision of health care to an individual.

- KDADS Workforce: Includes employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of KDADS or a KDADS business associate, whether paid by KDADS or a KDADS business associate.

- Minimum necessary: The least amount of information, when using or disclosing confidential information that is needed to accomplish the intended purpose of the use, disclosure or request.

- Open Office Environment: A work location structured with few enclosed offices or rooms in which private conversations may be conducted. An open office environment is characterized by individual work stations not separated by walls or partitions that do not extend from floor-to-ceiling or have a closable door, and therefore do not allow for workstation conversations that cannot be overhead by other person.

- Payment: Any activities undertaken by KDADS related to an individual to whom healthcare or payment for healthcare is provided in order to:

    - Obtain or provide reimbursement for the provision of healthcare.

    - Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts) and adjudication of health benefits or healthcare claims;

    - Billing, claims management, collection activities, obtaining payment under a contract of reinsurance, and related healthcare data processing.

    - Review of healthcare services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges.

    - Utilization review activities, including concurrent and retrospective review of services.

- Protected Health Information ("PHI"): Any individually identifiable health information, transmitted or maintained electronically or in another form or medium that is created or received by KDADS and

relates to the past, present or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present or future payment for the provision of healthcare to an individual; and that identifies the individual or there is a reasonable basis to believe the information can be used to identify the individual.

- Provider: A person or entity that may seek reimbursement from KDADS as a provider of services to an individual pursuant to a contract. For purposes of this policy, reimbursement may be required on the basis or encounter or other means of requesting payment.

- Storage System: Any form of office equipment or furniture, including but not limited to file cabinets, lateral files, or shelving units, in which a KDADS office stores an individual's information or files.

- Treatment: The provision, coordination, or management of healthcare and related services by one or more healthcare providers, including the coordination or management of healthcare by a healthcare provider with the third party; consulting between health providers relating to a patient or the referral of a patient for healthcare from one healthcare provider to another.

- Use: The sharing, application, utilization, examination, or analysis of information of individually identifiable information within KDADS.

- 42 CFR Part 2 records: These are treatment records pertaining to individuals who have received treatment for or participated in drug and alcohol treatment programs. Such treatment records are governed not only by HIPAA, but also the 42nd Code of Federal Regulations (CFR) Part 2, *Confidentiality of Alcohol and Drug Abuse Patient Records*.

All Glossary References: See generally Health Insurance Portability and Accountability Act of 1996 (HIPAA) and HITECH, (generally see also *45 CFR 160.103; 164.103; 164.501; 164.502, 42 CFR Part 2)*

Individual Privacy Rights

I. General:

A. KDADS may not deny an individual their right to the following:

1. Access to their own information, consistent with certain limitations (for example individuals do not have automatic access to psychotherapy notes).

2. Receive an accounting of disclosures KDADS has made of their PHI for up to six (6) years prior to the date of the request. Certain limitations do apply.

3. Submit complaints if:

- The individual believes or suspects that information about them has been improperly used or disclosed or if they have concerns about the KDADS Privacy policies (see http://www.kdads.ks.gov/required/privacy-statement).

- The individual's request for an amendment to their health information is denied.

B. Individuals may ask KDADS to take specific actions regarding the use and disclosure of their information and KDADS may either approve or deny the request. Specifically, individuals have the right to request:

1. KDADS restrict uses and disclosures of their individual information.

- As a general rule, KDADS applies policies and procedures applicable to specific programs and activities to safeguard the privacy of an individual's information. Even if policies and procedures permit KDADS to make a use or disclosure of information, the individual has the right to request a restriction. All requests for restriction shall be submitted to the KDADS Legal division for review.

- Requests for restrictions must be documented on a "Restriction of Use and Disclosure Request form" completed by the individual or KDADS staff member and submitted to a KDADS staff member as designated by the applicable Commissioner. Staff shall provide the pending request to within 3 days of receipt to the Commissioner designated staff.

- KDADS is not obligated to agree to a restriction and may deny the request or may agree to a restriction more limited than what the individual requested.

2. To receive information from KDADS by alternative means such as mail, email, fax, or telephone, or at alternative locations.

3. That KDADS amend their information that is held by KDADS.

- All requests for amendments will be made in writing and submitted to the appropriate KDADS staff. All requests shall be submitted to the KDADS Legal division for review.

- KDADS is not obligated to agree to an amendment and may deny the request.

Current Page's References: 45 CFR 164.502, 164.508, 164.528, 164.530, 164.526, 164.510, 164.522

C. Decision-making authority within KDADS

1. Prior to any decision, based on an individual's request for KDADS to amend their health information, the KDADS Legal Division staff shall review the request and any related documentation.

    - KDADS has 60 days in which to respond to a request. If additional time is needed to respond, KDADS must provide notice to the individual within the 60 days that an additional 30 days may be needed to respond to the request.

2. Prior to any decision, to amend any other information that is not in the individual's health information, the KDADS staff as designated by the applicable Commissioner shall review the request and any related documentation.

3. KDADS may deny an individual's access to their health information on the ground that access may result in risk or harm to the individual or to another person. However, prior to any decision to deny such access, the KDADS Legal staff shall review the request and any related documentation.

4. Decisions related to any other request made to KDADS by individuals shall be handled in a manner consistent with federal and state rules and regulations and/or KDADS policies and procedures applicable to the program, service, or activity.

II. Rights of Individuals to Access Their Information

A. All requests for access will be made by having the individual complete an "Access to Records Request form" and submitting it to appropriate KDADS staff.

B. KDADS may deny an individual's access to their health information if federal or state law prohibits the disclosure. Prior to any decision, the KDADS Legal staff shall review the request and any related documentation. Under federal law, individuals have the right to access, inspect, and obtain a copy of health information contained in KDADS files or records except for the following which is not an exhaustive list:

    i. Psychotherapy notes

    ii. Information compiled for use in civil, criminal, or administrative proceedings

    iii. Documents protected by attorney work-product privilege.

C. Before KDADS denies an individual access to their information based on professional judgment that its disclosure could cause harm to the individual or to another person, the decision to deny must be made by a Program Director or a Commissioner designated staff and KDADS must make a review of the denial (completed by a KDADS Privacy Officer in the Legal Division to act as a reviewing official who did not participate in the original decision to deny) available to the requesting individual. Such a denial and review shall be documented in writing.

Current Page's References: 45 CFR 164.520, 164.526, 164.524

III. Rights of Individuals to an Accounting of Disclosures of PHI

A. Individuals have the right to receive an accounting of disclosures of their PHI KDADS has made for any period of time not to exceed six (6) years, preceding the date the request for an accounting.

B. The accounting will only include health information NOT previously authorized by the individual for use or disclosure, and will not include information collected, used, or disclosed for treatment, payment, or healthcare operations for that individual.

C. All requests for accounting will be made in writing.

IV. Rights of Individuals to Request to Receive Information from KDADS by Alternative Means or at Alternative Locations

A. KDADS may accommodate a written request by an individual to receive communications by reasonable alternative means, such as by mail, email, fax, or telephone.

i. Information disclosed over the phone from a request for PHI shall be limited to situations of an accommodation.

1. Prior to the disclosure of any PHI over the phone, the KDADS employee must verify that the person requesting the information provide at least three of the following five points of data: name, last four of the social security number, date of birth, Medicaid identification number, or home address. If the individual is unable to provide three points of data, then KDADS staff shall not release the information over the phone.

B. KDADS may accommodate written requests by an individual to receive communications at a reasonable alternative location.

C. Health information or health services must be handled with strict confidentiality under state and federal law.

Current Page's References: 45 CFR 164.528, 164.526, 164.522, 42 CFR Part 2

Use and Disclosure of an Individual's Information

I. General Rule: Authorization is required

- KDADS shall not use or disclose any information about an individual under one of KDADS programs or services without a valid, signed authorization for release of that information from the individual, the individual's legally authorized representative, or as otherwise required by state or federal law.

II. Healthcare Oversight

- For purpose of carrying out duties in its role as a Healthcare Oversight Agency, KDADS does not need to obtain an individual's authorization to lawfully receive, use, disclose or exchange protected information.

III. HealthCare Oversight Exception

- Applies only where limited uses or disclosures are allowed without authorization (to the extent not prohibited or otherwise limited by federal or state requirements applicable to the program or activity).

- Unless prohibited, or otherwise limited, by federal or state law applicable to the program or activity requirements, KDADS Legal counsel may authorize disclosure.

IV. Authorization not required when individual is informed in advance & given the opportunity to object:

- In limited circumstances, KDADS may use or disclose an individual's information without authorization if:

    i. KDADS informs the individual in advance and the person has been given an opportunity to object. For questions regarding these uses or disclosures KDADS workforce will consult with the KDADS Legal division.

    ii. Unless otherwise protected by law, KDADS may orally inform the individual and obtain and document the individual's oral agreement.

- Disclosures are limited to disclosure of health information to a family member, other relative, or close personal friend of the individual, or any other person names by the individual unless further restricted by State or Federal law.

    i. For individuals receiving mental health services, oral permission is not sufficient and written authorization is required.

- Oral permission to use or disclose information for the purposes described in subsection (a) of this section is not sufficient when the individual is referred to or is receiving mental health services, where written authorization for the treatment program to make such disclosures is required.

V. Re-disclosure of an individual's information:

- Unless prohibited by state and federal laws, information held by KDADS and authorized by the individual for disclosure may be subject to re-disclosure and no longer protected by KDADS policies. Whether or not the information remains protected depends on whether the recipient is subject to federal or state privacy laws, court protective orders or other lawful process.

VI. Revocation of Authorization for KDADS Authorization for release of Protected Health Information

- An individual may revoke an authorization at any time.

- Any revocation must be in writing and signed by the individual. A revocation may refer to one or more authorizations that have been received by KDADS.

- No such revocation shall apply to information already released while the authorization was valid and in effect.

VII. Verification of individuals requesting information

- Information about an individual may be disclosed only upon reasonable verification of the identity and authority of the person requesting the information.

- Prior to the disclosure of any PHI over the phone, the KDADS employee must verify that the person requesting the information provide at least three of the following five points of data: name, last four of the social security number, date of birth, Medicaid identification number, or home address. If the individual is unable to provide three points of data, then KDADS staff shall not release the information over the phone.

VIII. Denial of requests for information

- KDADS shall deny any request for individual information, unless KDADS has received a valid written authorization signed by the individual or the individual's authorized representative with documentation verifying authority, or the information about the individual can be disclosed pursuant to this policy or as authorized by federal or state law.

References for Use and Disclosure section: 45 CFR 164.501 et seq.

Minimum Necessary Information

I. General

A. KDADS will use or disclose only the minimum amount of information necessary to provide services and benefits to individuals, and only to the extent provided in KDADS' policies and procedures.

B. This policy does not apply to:

i. Disclosure to or requests by a healthcare provider for treatment;

ii. Disclosures made to the individual;

iii. Uses or disclosures authorized by the individual that are within the scope of the authorization;

iv. Disclosures made to the United States Department for Health and Human Services, Secretary.

v. Uses or disclosures that are required by law.

II. Minimum Necessary

A. When permissible to use or disclose an individual's information to another entity, or when KDADS requests an individual's information from another entity, KDADS workforce must make reasonable efforts to limit the amount of information to the minimum necessary needed to accomplish the intended purpose of the use, disclosure, or request.

III. Access & Use of information

A. KDADS has established role-based access that affords access to information necessary for employees to perform the duties of their position. KDADS programs management will identify the category of information needed for workforce members, and any conditions appropriate to such access. Access will include information accessible by computer, kept in paper files, or other forms of information consistent with KDADS policy.

B. KDADS workforce shall be informed of their role-based access during initial orientation of employment. If questions arise regarding role-based access during the course of employment, KDADS workforce members shall address questions with their supervisor.

IV. KDADS' Request for an Individual's Information from Another Entity

A. When requesting information about an individual from another entity, KDADS workforce must limit requests to those that are reasonably necessary to accomplish the purpose for which the request is made.

Current Page's References: 45 CFR 164.502, 164.308

Safeguards

I. General

- KDADS shall implement appropriate administrative, technical, and physical safeguards that will reasonably safeguard an individual's PHI/confidential information from any intentional or unintentional use or disclosure that would violate KDADS policy, Kansas law/regulations, or federal law/regulations.

II. Administrative Safeguards

A. KDADS shall provide HIPAA & Security Awareness training to all KDADS workforce.

B. KDADS shall create, maintain, and enforce its HIPAA policy.

C. KDADS shall conduct audits and monitor its workforce to ensure compliance.

III. Technical Safeguards

A. All KDADS workforce shall know and comply with the requirements contained in the most up to date **KDADS Information Privacy & Security Acknowledgement**, which can be found on the KDADS intranet page.

B. As it relates to Technical Safeguards, all KDADS workforce shall know and comply with the most up to date **KDADS Employee Policy Manual Section 16: Information Technology**, which can be found on the KDADS intranet page.

C. All KDADS workforce are required to participate in Security Awareness Training as necessary.

IV. Physical Safeguards

A. Workstation Security

i. All KDADS workforce shall check his/her workstations before leaving at the end of a work period to make sure that all confidential data and PHI in any form is secured.

ii. All KDADS workforce shall secure PHI at his/her workstation by: moving PHI so that it is not visible in an unattended work area or on an unattended device, locking up paperwork in lockable cabinets and/or desk drawers, locking office doors (this is in addition to locking the building doors at the end of the day where applicable), not posting or storing passwords and User IDs in non-secure areas around the work area, locking one's device when not in use, and locking/logging off one's device when he/she walks away from his/her workstation.

B. Proper PHI Destruction

i. KDADS workforce is responsible for properly and securely destroying PHI when appropriate, including but not limited to: paper documents, electronic media such as cds or disks, or thumb drives in compliance with vendor requirements. Each floor or office building shall have a physical secured shred bin that shall be used for the destruction of paper PHI or confidential documents. KDADS workforce shall not destroy any PHI by

recycling paper documents or by throwing the paper documents in a trash can.

C. Control over Devices

i. All KDADS workforce are responsible to maintain the physical security of any and all portable devices in his/her possession at all times. Portable devices include, but are not limited to: computers, laptops, notebooks, cellular phones, tablets, PDAs, flash drives, external data storage, any removable drives such as CDs/DVDs or diskettes, portable printers/scanners, and tape recorders/recording devices.

ii. Physical security includes the use of physical and technical precautions to protect the device from loss, theft, natural and environmental hazards and any other unauthorized intrusion.

iii. If a KDADS portable device or a device that contains KDADS-related information is lost or stolen, the KDADS workforce member who was last in possession of the item shall **immediately** contact the local police force of where he/she is, contact the KDADS Help Desk, and contact the KDADS Legal Division.

D. Visitors/Guests

i. KDADS workforce shall instruct all non-KDADS staff attending state business meetings at KDADS to first check in at the reception desk and obtain a visitor's badge. Visitors must be escorted to their meeting room by at least one KDADS staff member and remain accompanied by one or more KDADS staff at all times for the duration of the visit.

ii. Non-KDADS workforce is not allowed in areas of KDADS' facilities where confidential data or PHI in any form is observable. Infants authorized to participate in the Infants-At-Work program are the only exception.

iii. KDADS workforce shall not allow unauthorized persons to enter secure areas by leaving doors open or allowing people to "piggy back" after a KDADS workforce member has utilized his/her ID badge to enter a secure area.

References for Safeguard Section: 45 CFR 164.306, 164.308, 164.310, 164.312; see also KDADS Employee Policy Manual Section 16: Information Technology

De-identification of Individual's Information

I. General

A. KDADS workforce may use and disclose de-identified health information as long as the code or other means of identification designed to permit re-identification is not disclosed. KDADS Legal must be informed of the intent to release the "de-identified" version of the information prior to its release.

II. Process for De-Identification

A. All of the following identifiers of the individual or of the relatives, employers, or household members of the individual shall be removed (and the KDADS does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information):

1. Names;
2. Geographic subdivision smaller than a State including, but not limited to:
    a) a street address, city, county, and zip code, and
    b) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people, and, if it has fewer than 20,000 people, the zip code is changed to 000 (example, for the zip code 73069, all areas using the zip code beginning with 730 have more than 20,000 in the aggregate).
3. All elements of dates (except year) for dates directly related to the individual, including birth date, admission date, discharge date, date of death; all ages over 89; and all elements of dates (including year) indicative of such age;
4. Telephone numbers;
5. Fax Numbers;
6. E-mail addresses;
7. Social Security Numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers, serial numbers, license plate numbers
13. Device identifiers and serial numbers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including fingerprints and voiceprints ;
17. Full face photographic images and other comparable images; and
18. All other unique identifying numbers, characteristics, or codes.

II. Re-Identification

A. KDADS may assign a code or other means of record identification to allow information de-identified to be re-identified by KDADS provided that both of the following are true:

1. The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual.

2. KDADS does not use or disclose the code or other means of record identification for any other purpose (other than re-identification) and does not disclose the mechanism for re-identification.

B. Disclosure of a code or other means of record identification, designed to enable coded or otherwise de-identified information to be re-identified, constitutes disclosure of PHI.

C. If de-identified information is re-identified, such re-identified information is PHI and KDADS may use or disclose such re-identified information only as permitted.

References for De-Identification Section: 45 CFR 164.514

Enforcement, Sanctions, and Discipline for Violations

I. General

a. All members of the KDADS workforce must guard against improper uses or disclosures of an individual's PHI or confidential.

i. KDADS workforce who are uncertain if a use or disclosure is permitted are advised to consult with the KDADS chain of supervision, beginning with the supervisor through the Commissioner level supervisor. If a concern remains unresolved, all concerns must be reported to the KDADS Legal Division within 48 hours, if the concern has not been resolved.

b. All KDADS workforce are required to know the content of this policy and all HIPAA training received and shall comply with all policies/training requirements.

c. Any of KDADS workforce who violate KDADS policies/procedures regarding HIPAA are subject to progressive discipline by KDADS. KDADS shall utilize the Offense Tiers stated below to aid in the assessment of progressive discipline.

d. KDADS workforce who violates applicable law for improper use or disclosure of an individual's information may be subject to civil or criminal penalties.

II. Violation Tiers

a. Tier I violation examples include, but are not limited to the following:
(1) Accessing information that you do not need to know to do your job;
(2) Sharing employee computer access codes (user name & password);
(3) Leaving your computer unattended while logged in;
(4) Sharing PHI with another employee unnecessarily or without authorization;
(5) Discussing PHI in public area where the conversation could be overheard;
(6) Failure to complete mandated training;
(7) Discussing confidential information with an unauthorized person; or
(8) Failure to cooperate with KDADS privacy officer or designee.

b. Tier II violation examples include, but are not limited to the following:
(1) Second offense of any Tier I offense (does not have to be the same offense);
(2) Unauthorized use or disclosure of PHI; or
(3) Using another person's computer access codes (user name & password).

c. Tier III violation examples include, but are not limited to the following:
(1) Third offense of any Tier I offense (does not have to be the same offense);
(2) Second offense of any Tier II offense (does not have to be the same offense);
(3) Obtaining PHI under false pretenses; or
(4) Using and/or disclosing PHI for commercial advantage, personal gain or malicious harm.

III. Additional Considerations

a. Factors that may be considered in making a discipline decision include the following:
(1) Severity of the offense;

(2) Potential or actual impact of the behavior or performance on individual's or an the agency;
(3) Nature and duration of the problem;
(4) Efforts made to help you adjust and efforts by you to adjust;
(5) Your length of service;
(6) History of your behavior/performance and prior formal disciplinary actions against you while you have been employed, considering the severity of such problems, and the time elapsed since the last problem situation; and
(7) Type of disciplinary action taken against other employees under similar circumstances.

IV. Retaliation prohibited

a. Neither KDADS as an entity or any of KDADS workforce will intimidate, threaten, coerce, discriminate against, or take any other form of retaliatory action against any individual for:

i. Reporting a compliance concern or filing a complaint.

ii. Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing relating to enforcement of KDADS policy.

Reference: 45 CFR 160 and 164, 45 CFR Part 2, KDADS Employee Policy Manual: Disciplinary Action Policy 3.6.