

*KANSAS DEPARTMENT ON AGING*

**HEALTH INSURANCE  
PORTABILITY AND  
ACCOUNTABILITY ACT  
(HIPAA) GUIDE**

*APRIL 1, 2003*

## TABLE OF CONTENTS

Glossary .....	2
General Privacy Policy .....	9
Business Associates .....	13
Customer Privacy Rights .....	14
De-identification of Customer Information and Use of Limited Data Sets .....	19
Minimum Necessary Information .....	24
Uses and Disclosures for Research Purposes & Waivers .....	27
Uses and Disclosures of Customer Information .....	33
Enforcement, Sanctions, and Penalties for Violations of Individual Privacy .....	38

## GLOSSARY

### **Administrative Order:**

An order that has the same meaning as the definition in KSA 77-502 (d) where an “order” means an state agency action of particular applicability that determines the legal rights, duties, privileges, immunities or other legal interest of one or more specific persons.

### **Administrative Hearings:**

The entity authorized by state law to preside over an administrative proceeding, whether conducted by the director or administrator, or designated employee, of a Kansas State agency or before an administrative hearing officer in a contested case. The hearing will be governed by KSA 77-513 through 77-523 and amendments thereto, except as otherwise provided by (a) statute other than this act or (b) KSA 77-533 through 77-541.

### **Agency:**

Kansas Department on Aging also referred to as “KDOA”.

### **Person:**

As used in KSA 77-502, “person” means an individual, partnership, corporation, association, political subdivision or unit thereof or public or private organization or entity of any character, and includes another state agency.

### **Business Associate:**

An individual or corporate “person” who: performs on behalf of the Agency any function or activity involving the use or disclosure of protected health information (PHI); and is not a member of the Agency’s workforce.

- The definition of “function or activity” includes: claims processing or administration, data analysis, utilization review, quality assurance, billing, legal, actuarial, accounting, consulting, data processing, management, administrative, accreditation, financial services and similar services for which the Department might contract are included, if access to PHI is involved.

- Business associates do not include Licensees or Providers unless the licensee or provider performs some “function or activity” on behalf of KDOA.

**Collect / Collection:**

The assembling of personal information through interviews, forms, reports or other information sources.

**Corrective Action:**

For purposes of KDOA programs, an action that a KDOA business associate must take to remedy a breach of violation of the business associate’s obligations under the business associate agreement or other contractual requirement, including but not limited to reasonable steps that must be taken to cure the breach or end the violation, as applicable.

**Covered Entity:**

Health plans, health care clearinghouses, and health care providers who transmit any health information in electronic form in as connection with a transaction that is subject to federal HIPAA requirements, as those terms are defined and used in the HIPAA regulations, 45 CFR Parts 160 and 164.

**Corrective Letter:**

A letter sent by one party to another, proposing or agreeing to actions that a party will take to correct legal errors or defects that have occurred under a contract between the parties or other legal requirement.

**Customer:**

An individual who requests or receives services from KDOA.

**Customer Records:**

All personal information that KDOA has collected, compiled, or created about KDOA customers, which KDOA may maintain in one or more locations and in various forms, reports, or documents, including information that is stored or transmitted by electronic media.

**Disclosure / Disclose:**

The release, transfer, relay, provision of access to, or conveying customer information to any individual or entity outside KDOA

**Employee:**

A public employee or officer for whom KDOA is the appointing official.

**Health Care:**

Care, services or supplies related to the health of an individual. Health care includes but is not limited to: preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care and counseling services, assessment, or procedure with respect to the physical or mental condition, or functional status of an individual, or that affects the structure or function of the body; and the sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

**Health Care Operations:**

Any of the following activities of KDOA or a covered entity 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 or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students and trainees in areas of health care learn under supervision to practice or improve their skills, accreditation, certification, licensing, or credentialing activities.
- Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits
- 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-related analysis related to managing and operating KDOA, including formulary development and administration, development of methods of payments or coverage policies.
- Business management and general administrative activities of KDOA, including but not limited to the following:
  - Management activities relating to implementation of a compliance with the requirements of HIPAA.
  - Customer/Customer services, including the provision of data analysis;
  - Resolution of internal grievances, including the resolution of dispute from customers or enrollees regarding the quality of care and eligibility for services.
  - Creating de-identified data or a limited data set.

**Health Oversight Agency:**

An agency, including KDOA, or a person or entity acting under a grant of authority from 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:**

Title II, subtitle F of the Health Insurance Portability and accountability Act of 1996, 42 USC 1320d et seq., and the federal regulations adopted to implement the Act.

**Individual:**

The person who is subject of information collected, used or disclosed by KDOA

**Individually Identifying Information:**

Any single item or compilation of information or data that indicates or reveals the identity of an Individual, either specifically (such as the individual's name or social security number), or that does not specifically identify the Individual but from which the Individual's supervised release, or otherwise is no longer in custody.

**Institutional Review Board (IRB):**

A specially constituted review body established or designated by an entity in accordance with 45 CFR Part 46 to protect the welfare of human subjects recruited to participate in biomedical or behavioral research.

**KDOA Workforce:**

Employees, volunteers, trainees, and other persons who conduct, in the performance of work for a covered entity (KDOA), is under the direct control of KDOA, whether or not they are paid by KDOA.

**Law Enforcement Official:**

An officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:  
Investigate or conduct an official inquiry into a potential violation of law; or  
Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

**Licensee:**

A person or entity that applies for or receives a license, certificate, registration or similar authority from KDOA to perform or conduct a services or activity or function.

**Minimum Necessary:**

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

**Non-routine Use:**

The disclosure of records that is not for a purpose for which it was collected.

**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, or by 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 overheard by other persons.

**Participant:**

Individuals participating in KDOA population-based services, programs, and activities that serve the general population, but who do not receive program benefits or direct services that are received by a

“customer”. Examples of “Participants” include but are not limited to: individuals who contact KDOA for Information & Referral services or Alzheimer’s Help Line.

**Payment:**

Any activities undertaken by KDOA related to an individual to whom health care or payment for health care is provided in order to:

- Obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan
- Obtain or provide reimbursement for the provision of health care.  
Payment includes:
- Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication of health benefits or health care claims;
- Billing, claims management, collection activities, obtaining payment under a contract for reinsurance, and related health care data processing;
- Review of health care 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; and

**Personal Representative:**

A person who has authority, under applicable state law, to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to the program, service or activity that KDOA provides to the Individual. If under applicable state law a parent, guardian, or other person acting in loco parent is has authority to act on behalf of an Individual who is an un-emancipated minor in making decisions relate to the program, service or activity, KDOA will treat that person as the personal representative of the Individual. KDOA guide, procedure or rule may include requirements related to documentation of the authority of the Personal Representative.

**Privacy Rights:**

The specific actions that an Individual can take or request to be taken with regard to the uses and disclosures of their information.

**Protected Health Information (PHI):**

Any individually identifiable health 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 clearinghouse; and 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. Any data transmitted or maintained in any other form or medium by covered entities, including paper records, fax documents and all oral communications, or any other form, i.e. screen prints of eligibility information, printed e-mails that have identified individual’s health information, claim or billing information, hard copy birth or death certificate. Protected health information excludes: school records that are subject to the Family Educational Rights and Privacy Act; and employment records held by KDOA in its role as an employer.

**Provider:**

A person or entity that may seek reimbursement from KDOA as a provider of services to KDOA Customers pursuant to a contract. For purposes of this guide, reimbursement may be requested on the basis of claims or encounter or other means of requesting payment.

**Public Official:**

Any employee of a government agency, including but not limited to KDOA, who is authorized to act on behalf of that agency in performing the lawful duties and responsibilities of that agency.

**Psychotherapy Notes:**

Notes recorded in any medium by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session, or a group, joint, or family counseling session, when such notes are separated from the rest of the individual's record. Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical test, and any summary of the following items; diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

**Public Health Agency:**

An agency, including KDOA, or a person or entity acting under a grant of authority form or contract with KDOA or such public agency, that performs or conducts one or more of the following essential functions that characterize public health programs, services or activities:

1. Monitor health status to identify community health problems;
2. Diagnose and investigate health problems and health hazards in the community;
  - Inform, educate, and empower people about health issues;
  - Mobilize community partnerships to identify and solve health problems;
  - Develop policies and plans that support individual and community health efforts;
  - Enforce laws and regulations that protect health and ensure safety;
  - Link people to needed personal health services and assure the provision of health care when otherwise unavailable;
  - Assure a competent public health and personal health care workforce;
  - Evaluate effectiveness, accessibility, and quality of personal and population-based health services; and
  - Research for new insights and innovative solutions to health problems.

KDOA provided and conducts a wide range of public health programs, services and activities.

**Public Health Authority:**

For purposes of this guide, Public Health authority is intended to have the same meaning as the HIPAA Privacy rules, as follows: "An agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority form or contract with such public agency, including the employees or agents of such public agency or its contractors of persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate."

**Research:**

A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

**Required by Law:**

A duty or responsibility that federal or state law specifies that a person or entity must perform or exercise. *Required by law includes* but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; and statutes or rules that require the production of information, including statutes or rules that require such information if payment is sought under a government program providing public benefits.

**Routine & Recurring Use:**

The disclosure of records for a purpose that is compatible with the purpose for which the information was collected.

**Storage System:**

Any form of office equipment or furniture, including but not limited to file cabinets, lateral files, or shelving units, in which a KDOA office stores customer information or files.

Treatment, Payment, and Operations (TPO):

Please refer to the separate definitions for Treatment, Payment, and Health Care operations.

**Treatment:**

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

**Use:**

The sharing, employment, application, utilization, examination, or analysis of information with KDOA.

## GENERAL PRIVACY

### **Purpose:**

The intent of this guide is to outline KDOA general guidelines and expectations for the necessary collection, use, and disclosure of confidential information about individuals in order to provide services and benefits to individuals, while maintaining reasonable safeguards to protect the privacy of their information.

*References: See KDOA Privacy Guide Glossary (a separate document)*

### **Guide:**

#### **1. General – KDOA will Safeguard Confidential Information about Individuals**

- a. KDOA may collect, maintain, use, transmit, share and/or disclose information about individuals to the extent needed to administer KDOA programs, services and activities.
- b. KDOA will safeguard all confidential information about individuals, inform individuals about KDOA privacy practices and respect individual privacy rights, to the full extent required under this guide.
- c. This guide identifies two types of individuals on whom KDOA is most likely to obtain, collect or maintain individual information:
  - i. KDOA Customers; and
  - ii. Licensees or Providers.
- d. KDOA shall provide training to its entire workforce on KDOA privacy policies, and shall require every staff to sign and acknowledge the “Privacy Program Statement of Understanding” outlining their role and responsibilities relating to protecting the privacy of KDOA customers.
- e. In the event that more than one guide applies but compliance with all such policies cannot reasonably be achieved, the KDOA workforce member will seek guidance from supervisors according to established KDOA guide and procedures. KDOA workforce should consult with their Privacy Coordinator or the KDOA Legal Counsel in appropriate circumstances.

#### **2. Safeguarding Information about Customers**

***A “Customer” is an individual who requests or receives services from KDOA.***

- a. KDOA, its workforce, and business associates will respect and protect the privacy of records and information about Customers who request or receive services from KDOA.
- b. All information on KDOA customers is confidential and must be safeguarded in accordance with KDOA privacy policies and procedures.
- c. KDOA shall not use or disclose information unless either permitted in accordance to, or the customer has authorized the use or disclosure in accordance with, KDOA’s “Use and Disclosures of Customer Information” guide.
- d. All KDOA offices shall adopt procedures to reasonably safeguard customer information.

### 3. **Safeguarding Customer Information**

- a. When KDOA or its business associates obtain individually identifiable information about customers; KDOA may use and disclose such information consistent with Federal and State law and regulation. Information regarding the qualifications of Licensees and Providers are public records.
- b. KDOA will safeguard all confidential information about customers consistent with Federal or State rules and regulations and KDOA policies and procedures.

### 4. **Safeguarding Information about Licensees and Providers**

*A “Licensee” is a person or entity that applies for or receives a license, certificate, registration or similar authority from KDOA to perform or conduct a service, activity or function.*

*A “Provider” is a person or entity who may seek reimbursement from KDOA as a provider of services to KDOA customers.*

KDOA shall not use or disclose any information about a customer of KDOA programs or services without a signed authorization for release of that information from the individual, or the individual’s personal representative, unless authorized by this guide, or as otherwise allowed or required by state or federal law, as outlined in the “Uses and Disclosures of Customer Information.”

### 5. **Conflict with Other Requirements Regarding Privacy & Safeguarding**

KDOA workforce shall act in accordance with established KDOA guide and procedures regarding the safeguarding and confidentiality of all individuals’ information, whether health-related or not, in all KDOA programs, services and activities.

### 6. **KDOA Notice of Privacy Practices**

- a. KDOA will make publicly available a copy of the, “KDOA Notice of Privacy Practices”.
- b. The KDOA Notice of Privacy Practices shall contain all information required under federal regulations regarding the notice of privacy practices for protected health information under HIPAA.

### 7. **Customer Privacy Rights**

KDOA privacy policies and procedures, as well as other federal and state laws and regulations, outline the customer’s right to access their own information, with some exception. These policies also describe specific actions that a customer can take to request restrictions or amendments to their information, and the method for filing a complaint. The specific actions are outlined in the “Customer Privacy Rights Guide.”

## 8. **Minimum Necessary Information**

- a. KDOA will use or disclose only the minimum amount of information necessary to provide services and benefits to customers, and only to the extent provided in KDOA policies and procedures.
- b. This guide does not apply to:
  - i. Disclosures to, or requests by, a health care provider for treatment;
  - ii. Uses or disclosures made to the individual;
  - iii. Uses or disclosures authorized by the individual;
  - iv. Disclosures made to the Secretary of the United States Department of Health & Human Services in accordance with federal HIPAA regulations at 45 CFR 160, Subpart C.
  - v. Uses or disclosures that are required by law; and
  - vi. Uses or disclosures that are required for compliance with federal HIPAA regulations at 45 CFR, Parts 160 and 164 (<http://www.hhs.gov/ocr/hipaa>)
- c. When using or disclosing an individual's information, or when requesting an individual's information from a provider or health plan, KDOA's 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, as outlined in the "Minimum Necessary Information." This section does not preclude more limiting restrictions that may be imposed by state or federal laws.

## 9. **Administrative, Technical and Physical Safeguards**

KDOA workforce must take reasonable steps to safeguard confidential information from any intentional use or disclosure, as outlined in the "Administrative, Technical, and Physical Safeguards."

## 10. **Use and Disclosures for Research Purposes and Waivers**

KDOA may use or disclose an individual's information for research purposes as outlined in "Uses and Disclosures for Research Purposes and Waivers."

## 11. **De-Identification of Customer Information and Use of Limited Data Sets**

KDOA workforce will follow standards under which customer information can be used and disclosed if information that can identify a person has been removed or restricted to a limited data set. Unless otherwise restricted or prohibited by other federal or state law, KDOA can use and share information as appropriate for the work of KDOA, without further restriction, if KDOA or another entity has taken steps to de-identify the information as outlined in "De-identification of customer information and Use of Limited Data Sets."

## 12. **Business Associate Relationships**

KDOA may disclose protected health information to business associates with whom there is a written contract or memorandum of understanding as outlined in "KDOA Business Associate Relationships."

### **13. Enforcement, Sanctions and Penalties for Violations of Individual Privacy**

All KDOA workforce must comply with and guard against improper uses or disclosures of KDOA customer's information as outlined in "Enforcement, Sanctions, and Penalties for Violations of Individual Privacy."

#### **Form(s):**

- KDOA Notice of Privacy Practices
- KDOA Employee Privacy & Security Statement of Understanding (Handbook)

#### **Reference(s):**

- 45 CFR Parts 160 and 164

#### **Contact(s):**

- Privacy Coordinator

## BUSINESS ASSOCIATES

### **Purpose:**

The intent of this guide is to establish the expectation KDOA has of external parties, referenced as business associates, who are contracted specifically to provide KDOA services involving the use and disclosure of protected health information and who are not a member of KDOA's workforce.

The term "services" is all encompassing: legal, actuarial, accounting, consulting, data processing, management, administrative, accreditation, financial and anything else for which KDOA might contract are included, if access to PHI is involved.

It is the guide of KDOA that identifiable health information may only be shared with business associates pursuant to an approved business associate agreement.

KDOA is required to obtain assurances that any business associate with whom it shares health information handles that information in compliance with privacy regulations.

*References: See Privacy Guide Glossary (a separate document)*

### **Guide:**

#### **1. General**

- a. Health information may only be shared with business associates pursuant to an approved business associate agreement.
  - i. Business associate agreements must be in writing and must contain KDOA approved HIPAA complaint language and authorized signatures.
  - ii. At any time KDOA determines that a business associate has violated a material term or obligation under the agreement relating to HIPAA compliance, the department that is party to the agreement and/or the agency's privacy official shall be notified and shall seek to immediately remedy the breach or, if that is not possible, to alter or terminate the agreement.
- b. KDOA business associates shall not use or further disclose protected health information other than as permitted by the contract or as required by law;
  - i. Business associates shall use appropriate safeguards to prevent unauthorized use or disclosure of protected health information;
  - ii. Business associates shall report to KDOA any unauthorized use or disclosure of which it becomes aware;
  - iii. Business associates shall ensure that any agents, including subcontractors, to whom it provides protected health information, agree to the same restrictions and conditions that apply to the business associate;
  - iv. Business associates shall on termination of the contract, return or destroy all protected health information in its possession, or, where that is not possible, extend the protections of the contract for as long as the information is retained.

- c. Business associates must cooperate with KDOA to provide access to protected health information for the subjects of that information (per 45 CFR 164.524), allow for amendment of correction (164.528), and in accounting of protected health information disclosures (164.528).
- d. KDOA is not liable for the privacy violations of business associates. However, if KDOA becomes aware of a pattern of activity or practice by a business associate that constitutes a material breach, it will:
  - i. Take reasonable steps to remedy the situation;
  - ii. If such steps are not successful, terminate the contract or arrangement; or
  - iii. If termination is not feasible, report the problem to DHHS

**Form(s):**

- Business Associate Agreement
- Compliance Report Investigation Form

**Reference(s):**

- 45 CFR Parts 164.502 , 164.504 (e) (2) (3) (4)
- 45 CFR Parts 164.504 (e) (1) (2) (3) (4)

## CUSTOMER PRIVACY RIGHTS

### **Purpose:**

The intent of this guide is to establish the privacy rights that KDOA customers have regarding the use and disclosure of their protected information that is held by KDOA and to describe the process for filing a complaint should customers believe those rights have been violated.

*Reference: KDOA Privacy Guide Glossary (a separate document)*

### **Guide:**

#### **1. General**

- a. KDOA may not deny a customer their right to the following:
  - i. Access to their own information, consistent with certain limitations;
  - ii. Receive an accounting of disclosures KDOA has made of their protected health information (PHI) for up to six years prior to the date of request. Information may not be available prior to the effective date of this guide (April 14, 2003) and certain limitations do apply as outlined in this guide, section 6; and
  - iii. Submit complaints if they believe or suspect that information about them has been improperly used or disclosed, or if they have concerns about the privacy policies of KDOA.
- b. Customers may ask KDOA to take specific actions regarding the use and disclosure of their information and KDOA may either approve or deny the request. Specifically, customers have the right to request:
  - i. That KDOA restrict uses and disclosures of their individual information while carrying out treatment, payment activities, or health care operations;
  - ii. To receive information from KDOA by alternative means, such as mail, e-mail, fax or telephone, or at alternative locations; and
  - iii. That KDOA amend their information that is held by KDOA.
- c. Relationship to Notice of Privacy Practices.
  - i. KDOA will use the “KDOA Notice of Privacy Practices,” to inform customers about how KDOA may use and/or disclose their information. The Notice of Privacy Practices also describes the actions a customer may take, or request KDOA to take, with regard to the use and/or disclosure their information; and
    - A. The policies related to the “Notice of Privacy Practices” and the distribution of the Notice are addressed in “General Privacy.”
  - ii. Nothing in this guide, or the guide related to the “Notice of Privacy Practices,” shall prevent KDOA from changing its policies or the Notice at any time, provided that the changes in the policies or Notice comply with state or federal law.
- d. Decision-making authority within KDOA.
  - i. Prior to any decision, based on a customer’s request for KDOA to amend their health record, the appropriate KDOA staff shall review the request and any related documentation;

- ii. Prior to any decision, to amend any other information that is not in the customer record, appropriate KDOA staff shall review the request and any related documentation;
- iii. KDOA may deny a customer access to their health information on the grounds that access may result in risk or harm to the customer or to another person. However, prior to any decision to deny such access, the appropriate KDOA staff shall review the request and any related documentation; and
- iv. Decisions related to any other requests made to KDOA under this guide shall be handled in a manner consistent with federal and state rules and regulations and/or KDOA policies and procedures applicable to the program, service or activity.

**2. Rights of Customers to Request Privacy Protection of Their Information**

- a. Customers have the right to request restrictions on the use and/or disclosure of their information.
- b. KDOA applies confidentiality policies and procedures applicable to specific programs and activities to protect the privacy of customer information. Even if those laws permit KDOA to make a use or disclosure of information, a KDOA customer has the right to request a restriction on a use or disclosure of that information.
- c. Requests for restrictions will be made by having the customer complete a “Restriction of Use and Disclosure Request form” and submitting it to appropriate KDOA staff.
- d. KDOA is not obligated to agree to a restriction and may deny the request or may agree to a restriction more limited than what the customer requested.

**3. Rights of Customers to Request to Receive Information from KDOA by Alternative Means or at Alternative Locations**

- a. KDOA will accommodate written requests by customers to receive communications by reasonable alternative means, such as by mail, e-mail, fax or telephone;
- b. KDOA will accommodate written requests by customers to receive communications at a reasonable alternative location; and
- c. In some cases, sensitive health information or health services must be handled with strict confidentiality under state law. For example, information about substance abuse treatment, mental health treatment, and certain sexually transmitted diseases, may be subject to specific handling. KDOA will comply with the more restrictive requirements.

**4. Rights of Customers to Access Their Information**

- a. All requests for access will be made by having the customer complete an “Access to Records Request form” and submitting it to appropriate KDOA staff.
- b. Customers may request access to their own information that is kept by KDOA by using a personal identifier (such as the customer’s name or case number).
  - i. If KDOA maintains information about the customer in a record that includes information about other people, the customer is only authorized to see information about him or herself, except as provided below:
    - A. If the person requesting information is recognized under Kansas law as a guardian or legal designee of the customer and is authorized by Kansas law to have access to the customer’s information or to act on behalf of the customer for making decisions about the customer’s services or care, KDOA will release information to the requestor.

- B. Under these special circumstances: the system in Kansas \_\_\_\_\_, to protect and advocate the rights of individuals with developmental disabilities under part C of the Developmental Disabilities Assistance and Bill of Rights Act (42 U.S.C. 6041 et seq.) and the rights of individuals with mental illness under the Protection and Advocacy for Individuals with Mental Illness Act \_\_\_\_\_, shall have access to all records, as defined in \_\_\_\_\_, as provided in \_\_\_\_\_.
- c. KDOA may deny customers access to their health information if federal or state law prohibits the disclosure. Under federal law customers have the right to access, inspect, and obtain a copy of health information contained in KDOA files or records except for:
  - i. Psychotherapy notes;
  - ii. Information compiled for use in civil, criminal, or administrative proceedings;
  - iii. Information that is subject to the federal Clinical Labs Improvement Amendments of 1988, or exempt pursuant to 42 CFR 493.3(a)(2);
  - iv. Information that, in good faith, KDOA believes can cause harm to the customer, participant or to any other person; and
  - v. Documents protected by attorney work-product privilege.
- d. Before KDOA denies a customer access to their information because there is a good faith belief that its disclosure could cause harm to the customer or to another person, the decision to deny must be made by a program director or other designated staff and KDOA must make a review of the denial (completed by a KDOA designee to act as a reviewing official who did not participate in the original decision to deny) available to the customer. Such a denial and review will be documented on the *Denial of Request to Access* form.

5. **Rights of Customers to Request Amendments to Their Information.**

- a. KDOA customers have the right to request that KDOA amend information contained in their customer file.
- b. All requests for amendments will be made by having the customer complete an “*Amendment of Health Record Request form*” and submit it to appropriate KDOA staff.
- c. KDOA is not obligated to agree to an amendment and may deny the requests or limit its agreement to amend.
- d. A customer’s request to delete or remove information from their health record will not be allowed.

6. **Rights of Customers to an Accounting of Disclosures of Protected Health Information.**
  - a. Customers have the right to receive an accounting of disclosures of protected health information (PHI) that KDOA has made for any period of time not to exceed six years, preceding the date of requesting the accounting.
  - b. The accounting will only include health information NOT previously authorized by the customer for use or disclosure, and will not include information collected, used or disclosed for treatment, payment or health care operations for that customer.
  - c. All requests for accounting will be made by having the customer complete an *Accounting of Disclosures Request* form and submit it to appropriate KDOA staff.
  - d. This right does not apply to disclosures made prior to the effective date of this guide, which is April 14, 2003.
  
7. **Rights of Customers to File Complaints Regarding Disclosure of Information**
  - a. Customers have a right to submit a complaint if they believe that KDOA has improperly used or disclosed their protected information, or if they have concerns about the privacy policies of KDOA or concerns about KDOA compliance with such policies.
  - b. Complaints may be filed with any of the following:
    - i. The Kansas Department on Aging; or
    - ii. The U.S. Department of Health and Human Services, Office of Civil Rights.

**Form(s):**

- “KDOA Notice of Privacy Practices”
- “Access to Records Request”
- “Amendment of Health Record Request”
- “Restriction of Use and Disclosures Request”
- “Accounting of Disclosures Request”

**Reference(s):**

- 45 CFR Parts 164.522 – 164.528

**Contact:**

- Privacy Coordinator

## DE-IDENTIFICATION OF CUSTOMER INFORMATION AND USE OF LIMITED DATA SETS

### Purpose:

The intent of this guide is to prescribe standards under which customer information can be used and disclosed if information that can identify a person has been removed or restricted to a limited data set.

*Reference: See KDOA Privacy Glossary*

### Guide:

#### 1. General

- a. De-identified information is customer information from which KDOA or another entity has deleted, redacted, or blocked identifiers, so that the remaining information cannot reasonably be used to identify a person.
- b. Unless otherwise restricted or prohibited by other federal or state law, KDOA can use and share information as appropriate for the work of KDOA, without further restriction, if KDOA or another entity has taken steps to de-identify the information consistent with the requirements and restrictions of this guide in Section (2).
- c. KDOA may use or disclose a limited data set that meets the requirements of Section (4) of this Guide, if KDOA enters into a data use agreement with the limited data set recipient (or with the data source, if KDOA will be the recipient of the limited data set) in accordance with the requirements of Section (5) of this Guide.
- d. KDOA may disclose a limited data set only for the purposes of research, or non-governmental public health purposes. However, unless KDOA has obtained a limited data set that is subject to a data use agreement, KDOA is not restricted to using a limited data set for its own activities or operations.
- e. If KDOA knows of a pattern or activity or practice of the limited data set recipient that constitutes a material breach or violation of a data set agreement, KDOA will take reasonable steps to cure the breach or end the violation and, if such steps are unsuccessful, KDOA will discontinue disclosure of information to the recipient and report the problem to the United States Department of Health and Human Services (DHHS), Office of Civil Rights.

#### 2. Requirements for Safe Harbor Method of De-identification

- a. Customer information is sufficiently de-identified, and cannot be used to identify an individual, only if **either** (i) or (ii) below has occurred:

- i. A statistician or other person with appropriate knowledge of, and experience with, generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:
  - A. Has applied such principles and methods, and determined that the risk is minimal that the information could be used, alone or in combination with other reasonably available information, by a recipient of the information to identify the person whose information is being used; and
  - B. Has documented the methods and results of the analysis that justify such a determination; **or**
- ii. KDOA has ensured that:
  - A. The following identifiers of the individual or of relatives, employers, and household members of the individual are removed:
    - I. Names;
    - II. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geo codes. However, the initial three digits of a zip code may remain on the information if, according to current publicly-available data from the Bureau of the Census, the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and the initial three digits for all such geographic unit containing 20,000 or fewer people is changed to 000;
    - III. All elements of dates (except year) for dates directly relating to an individual, including birth date, dates of admission and discharge from a health care facility, and date of death. For persons age 90 and older, all elements of dates (including year) that would indicate such age must be removed, except that such ages and elements may be aggregated into a single category of “age 90 or older;”
    - IV. Telephone numbers;
    - V. Fax numbers;
    - VI. Electronic mail addresses;
    - VII. Social security numbers;
    - VIII. Medical record numbers;
    - IX. Health plan beneficiary numbers;
    - X. Account numbers;
    - XI. Certificate or license numbers;
    - XII. Vehicle identifiers and serial numbers, including license plate numbers;
    - XIII. Device identifiers and serial numbers;
    - XIV. Web Universal Resource Locators (URLs);
    - XV. Internet Protocol (IP) address numbers;
    - XVI. Biometric identifiers, including fingerprints and voiceprints;
    - XVII. Full face photographic images and any comparable images; and
    - XVIII. Any other unique identifying number, characteristic, or codes, except as permitted under Section (3), below, of this guide; and
  - B. KDOA has no actual knowledge that the information could be used alone or in combination with other information to identify an individual who is the subject of the information.

- b. The KDOA Privacy Officer will designate the statistician or other person referred to in (2)(a)(i), above, who may be either:
  - i. A KDOA employee;
  - ii. An employee or another governmental agency; or
  - iii. An outside contractor or consultant, subject to KDOA contracting and personnel guide.

### 3. **Re-identification of de-identified information**

- a. KDOA may assign a code or other means of record identification to allow information de-identified under this guide to be re-identified by KDOA, except that:
  - i. The code or other record identification is not derived from or relating to information about the individual and cannot otherwise be translated to identify the individual; and
  - ii. KDOA does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

### 4. **Requirements for a limited data set**

- a. A limited data set is information that excludes the following direct identifiers of the individual, or of relatives, employers or household members of the individual:
  - i. Names;
  - ii. Postal address information, other than town or city, state and zip code;
  - iii. Telephone numbers;
  - iv. Fax numbers;
  - v. Electronic mail addresses;
  - vi. Social Security numbers;
  - vii. Medical record numbers;
  - viii. Health plan beneficiary numbers (such as Medicaid Prime Numbers);
  - ix. Account numbers;
  - x. Certificate/license numbers;
  - xi. Vehicle identifiers and serial numbers, including license plate numbers;
  - xii. Web Universal Resource Locators (URLs);
  - xiii. Internet Protocol (IP) address numbers;
  - xiv. Biometric identifiers, including finger and voice prints; and
  - xv. Full face photographic images and any comparable images.

### 5. **Contents of a Limited Data Set Use Agreement**

- a. KDOA may disclose a limited data set only if the entity receiving the limited data set enters into a written agreement with KDOA, in accordance with subsection (5)(b) immediately below, that such entity will use or disclose the protected health information only as specified in the written agreement.
- b. A data use agreement between KDOA and the recipient of the limited data set must:
  - i. Specify the permitted uses and disclosures of such information by the limited data set recipient. KDOA may not use the agreement to authorize the limited data set recipient to use or further disclose the information in a manner that would violate the requirements of this Guide if done by KDOA.
  - ii. Specify who is permitted to use or receive the limited data set; and
  - iii. Specify that the limited data set recipient will:

- A. Not use or further disclose the information other than as specified in the data use agreement or as otherwise required by law;
- B. Use appropriate safeguards to prevent use or disclosure of the information other than as specified in the data use agreement;
- C. Report to KDOA, if KDOA is the source of the limited data set, if the recipient becomes aware of any use or disclosure of the information not specified in its data use agreement with KDOA;
- D. Ensure that any agents, including a subcontractor, to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and
- E. Not identify the information or contact the individuals whose data is being disclosed.

**Reference(s):**

- 45 CFR Parts 164.514

**Contact(s):**

- Privacy Coordinator

<b>MINIMUM NECESSARY INFORMATION</b>
--------------------------------------

**Purpose:**

The intention of the KDOA Minimum Necessary Information Guide is to:

- Improve the privacy of confidential information that is used or disclosed by KDOA employees in the course of their work; and to
- Ensure that KDOA employees have access to the information they require to accomplish KDOA’s mission, goals and objectives.

*Reference: See KDOA Privacy Glossary*

**Guide:**

**1. General**

- a. KDOA will use or disclose only the minimum amount of information necessary to provide services and benefits to customers, and only to the extent provided in KDOA policies and procedures.
- b. This guide does not apply to:
  - i. Disclosures to or requests by a health care provider for treatment;
  - ii. Disclosures made to the individual about his or her own protected information;
  - iii. Uses or disclosures authorized by the individual that are within the scope of the authorization;
  - iv. Disclosures made to the United States Department of Health and Human Services (DHHS), Office of Civil Rights, in accordance with subpart C of part 160 of the HIPAA Privacy Rule; and
  - v. Uses or disclosures that are required by law.

## 2. **Minimum Necessary Information**

- a. When KDOA guide permits use or disclosure of an individual's information to another entity, or when KDOA requests an individual's information from another entity, KDOA 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.
- b. If KDOA guide permits making a particular disclosure to another entity, KDOA workforce may rely on a requested disclosure as being the minimum necessary for the stated purpose when:
  - i. Making disclosures to public officials that are permitted under 45 CFR 164.512, and as stated in KDOA guide, "Uses and Disclosures of Customer Information," if the public official represents the information requested is the minimum necessary for the stated purpose(s). in performing the lawful duties and responsibilities of that agency;
  - ii. The information is requested by another entity that is a "covered entity" under the HIPAA Privacy rules;
  - iii. The information is requested by a professional who is a member of the workforce of a covered entity or is a business associate of the covered entity for the purpose of providing professional services to the covered entity, if the professional represents that the information requested is the minimum necessary for the stated purpose(s);  
or
  - iv. Documentation or representations that comply with the applicable requirements of KDOA Guide, "Uses and Disclosures for Research Purposes & Waivers" have been provided by a person requesting the information for research purposes.

## 3. **Access & Uses of Information:**

- a. KDOA will establish role-based categories that identify types of information necessary for employees to do their jobs. KDOA program areas will identify the category of information needed for persons, or classes of persons, in the respective workforce to carry out their duties, and will further identify any conditions appropriate to such access. Categories will include all information, such as information accessible by computer, kept in files, or other forms of information consistent with KDOA Guide "Administrative, Technical and Physical Safeguards"; and
- b. KDOA workforce will be informed of their role-based authority and constraints during initial orientation of employment.

## 4. **Routine and Recurring Disclosure of an Individual's Information:**

The following identifies several examples of routine and recurring uses and disclosures of information that KDOA has determined to be compatible with the purposes for which information is collected and does not require an authorization from the individual.

- a. KDOA will not disclose an individual's entire case record unless the request specifically justifies why the entire medical record is needed;
- b. Routine and recurring uses include disclosures required by law. For example, a mandatory adult abuse report by KDOA workforce member would be a routine use;
- c. If KDOA deems it desirable or necessary, KDOA may disclose information as a routine and recurring use to the Kansas Department of Administration for the purpose of obtaining its advice and legal services;

- d. When federal or state agencies – such as the Office of Civil Rights, the Office of the Inspector General, or the State of Kansas Department of Social and Rehabilitation Services – have the legal authority to require KDOA to produce records necessary to carry out audit or oversight of KDOA programs or activities, KDOA will make such records available as a routine and recurring use; or
- e. When the appropriate KDOA official determines that records are subject to disclosure under the Kansas Open Records Act, KDOA shall make the disclosure as a routine and recurring use.

**5. Non-routine Disclosure of an Individual’s Information**

For Non-Routine Disclosures, KDOA program areas will:

- a. Implement procedures to limit the information disclosed to only the minimum amount of information necessary to accomplish the purpose for which the disclosure is sought; and
- b. Review requests for non-routine disclosures on an individual basis in accordance with such procedures.

**6. KDOA Request for an Individual’s Information from Another Entity:**

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

KDOA will not request an individual’s entire case record unless KDOA can specifically justify why the entire case record is needed.

**Reference(s):**

- 45 CFR Parts 160 and 164

**Contact(s):**

- Privacy Coordinator

**USES AND DISCLOSURES FOR RESEARCH PURPOSES & WAIVERS**

**Purpose:**

The intent of this guide is to specify when KDOA may use or disclose information about individuals for research purposes.

*References: See KDOA Privacy Guide Glossary*

**Guide:**

**1. General**

When KDOA uses or discloses an individual’s information for research purposes, they must consider the following:

- a. KDOA may use or disclose an individual’s information for research purposes as specified in this guide. “Research” means “a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.”
- b. All such research disclosures are subject to applicable requirements of state and federal laws and regulations and to the specific requirements of this guide.
- c. This guide is intended to supplement existing research requirements of the Common Rule, 45 CFR Part 46. The Common Rule is the rule for the protection of human subjects in research promulgated by the U.S. Department of Health and Human Services, and adopted by other federal governmental agencies, including the National Institutes for Health, for research funded by those agencies. In addition, KDOA may have requirements that supplement the Common Rule that are applicable to a particular research contract or grant.
- d. De-identified information may be used or disclosed for purposes of research, consistent with “De-identification of Customer Information and Use of Limited Data Sets.”
- e. A limited data set may be used or disclosed for purposes of research, consistent with the policies related to Limited Data Sets in “De-identification of Customer Information and Use of Limited Data Sets.”
- f. KDOA may also conduct public health studies, studies that are required by law, and studies or analysis related to its health care operations. Such studies will be discussed in Sections (4) and (5) of this Guide.

**2. Institutional Review Board (IRB) or Privacy Board Established by KDOA**

KDOA may use an IRB established in accordance with 45 CFR Part 46 or a Privacy Board that has been established by KDOA pursuant to this guide, to perform the duties and functions specified in this guide regarding a research project being conducted, in whole or in part, by KDOA or by a KDOA office or program.

**3. Uses and disclosures for Research Purposes – Specific Requirements**

- a. KDOA may use or disclose customer information for research purposes with the customer’s specific written authorization.
  - i. Such authorization must meet all the requirements described in “Uses and Disclosures of Customer Information,” and may indicate as an expiration date such terms as “end of research study,” or similar language.
  - ii. An authorization for use and disclosure for a research study may be combined with any other type of written permission for the same research study.
  - iii. If research includes treatment, the researcher may condition the provision of research related treatment on the provision of an authorization for use and disclosure for such research.

- b. KDOA may use or disclose customer information for research purposes without the customer's written authorization provided that:
  - i. An Institutional Review Board (IRB); or
  - ii. A Privacy Board that:
    - A. Has members with varying backgrounds and appropriate professional competency as needed to review the effect of the research protocol on the Individual's privacy rights and related concerns;
    - B. Includes at least one member who is not affiliated with KDOA, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any such entity; and
    - C. Does not have any member participating in a review of any project in which the member has a conflict of interest.
- c. Documentation required of IRB or privacy board that approved the waiver of an individual's authorization for release of information must include:
  - i. A statement identifying the IRB or privacy board that approved the waiver of an individual's authorization, and the date of such approval;
  - ii. A statement that the IRB or privacy board has determined that the waiver of authorization, in whole or in part, satisfies the following criteria:
    - A. The use or disclosure of an individual's protected information involves no more than minimal risk to the privacy of individuals, based on at least the following elements:
      - 1. An adequate plan to protect an individual's identifying information from improper use or disclosure;
      - 2. An adequate plan to destroy an individual's identifying information at the earliest opportunity consistent with the conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and
      - 3. Adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of the protected information would be permitted under this guide;
    - iii. The research could not practicably be conducted without the waiver; and
    - iv. The research could not practicably be conducted without access to and use of the individual's protected information;
- d. A brief description of the protected health information for which use or disclosure has been determined to be necessary by the IRB or privacy board;
  - i. A statement that the waiver of an individual's authorization has been reviewed and approved under either normal or expedited review procedures, by either an IRB or a privacy board, pursuant to federal regulations at 45 CFR 164.512(2); and
  - ii. The Privacy Board Chair must sign documentation of the waiver of an individual's authorization, or other member as designated by the Chair of the IRB or the Privacy Board, as applicable.
    - A. In some cases, a researcher may request access to individual information maintained by KDOA in preparation for research or to facilitate that development of a research protocol in anticipation of research. Before agreeing to provide such access to individual information, KDOA should determine whether federal or state law otherwise permits such use or disclosure

without individual authorization or use of an IRB. If there is any doubt whether the use and disclosure of the information by the researcher falls within this HIPAA exception, review by an IRB or privacy board and formal waiver of authorization is required. If such access falls within this HIPAA exception to authorization and is otherwise permitted by other federal or state law, KDOA will only provide such access if KDOA obtains, from the researcher, written representations that:

- B. Use or disclosure is sought solely to review an individual's protected information needed to prepare a research protocol or for similar purposes to prepare for the research project;
  - C. No customer information will be removed from KDOA by the researcher in the course of the review; the customer information for which use or access is sought is necessary for the research purposes;
    - 1. Researcher and his or her agents agree not to use or further disclose the information or contact the individual whose data is being disclosed; and
    - 2. Applicable federal or state law may require such other terms or conditions.
- iii. In some cases, a researcher may request access to individual information maintained by KDOA about individuals who are deceased. KDOA should determine whether federal or state law otherwise permits such use or disclosure of information about decedents without individual authorization or use of an IRB. There may be instances where it would be inappropriate to disclose information, even where the individual subject of the information is dead – for example, individuals who died of AIDS may not have wanted such information to be disclosed after their deaths. If there is any doubt whether the use and disclosure of the information by the researcher falls within this HIPAA exception, review by an IRB or privacy board and formal waiver of authorization is required. If such access falls within this HIPAA exception to authorization and is otherwise permitted by other federal or state law, KDOA will only provide such access if KDOA obtains the following written representations from the researcher:
- A. Representation that the use or disclosure is sought solely for research on the protected information of deceased persons;
  - B. Documentation, if KDOA so requests, of the death of such persons; and
  - C. Representation that the Individual's protected information for which use or disclosure is sought is necessary for the research purposes.
  - D. Researcher and his or her agents agree not to use or further disclose the information other than as provided in the written agreement, and to use appropriate safeguards to prevent the use or disclosure of the information other than is provided for by the written agreement;
  - E. Researcher and his or her agents agree not to publicly identify the information or contact the personal representative or family members of the decedent; and
  - F. Applicable federal or state law may require such other terms or conditions.

#### 4. **KDOA Public Health Studies and Studies Required by Law**

When KDOA is operating as a Public Health Authority, KDOA is authorized to obtain and use individual information without authorization for the purpose of preventing injury or controlling disease and for the conduct of public health surveillance, investigations and interventions. In addition to these responsibilities, KDOA may collect, use or disclose information, without

individual authorization, to the extent that such collection, use or disclosure is required by law. When KDOA uses information to conduct studies pursuant to such authority, no additional individual authorization is required nor does this guide require IRB or privacy board waiver of authorization based on the HIPAA Privacy rules. Other applicable laws and protocols continue to apply to such studies.

## 5. **KDOA Studies Related to Health Care Operations**

Studies and data analyses conducted for KDOA's own quality assurance purposes and to comply with reporting requirements applicable to federal or state funding requirements fall within the uses and disclosures that may be made without individual authorization as KDOA health care operations. Neither individual authorization nor IRB or privacy board waiver of authorization is required for studies or data analyses conducted by or on behalf of KDOA for purposes of health care operations, including any studies or analyses conducted to comply with reporting requirements applicable to federal or state funding requirements. "Health care operations" as defined in 45 CFR 164.512 includes:

- a. Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities;
- b. Conducting population-based activities relating to improving health care or reducing health care costs, protocol development, case management and care coordination, contacting health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;
- c. Reviewing the competence or qualifications of health care professionals, evaluating practitioners and provider performance, health plan performance, and conducting training programs, and accreditation, certification, licensing or credentialing activities;
- d. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
- e. Business planning and development, such as conducting cost-management and planning related analyses related to managing and operating KDOA, including improvement of administration or development or improvement of methods of payment or coverage policies; and
- f. Business management and general administrative activities of KDOA, including management activities related to HIPAA implementation and compliance.
- g. Creating de-identified information or a limited data set consistent with "De-identification of Customer Information and Use of Limited Data Sets."
  - **Exception:** HIV-AIDS information may not be disclosed to anyone without the specific written authorization of the individual. Re-disclosure of HIV test information is prohibited, except in compliance with law or with written permission from the individual.

**Reference(s):**

- 45 CFR Part 64
- 45 CFR 164.512

**Contract(s):**

- Privacy Coordinator

**USES AND DISCLOSURES OF CUSTOMER INFORMATION**

**Purpose:**

The intent of this guide is to specify that customer information cannot be used or disclosed without the individual's prior authorization, and to identify those exceptions that could be applicable.

*Reference: See KDOA Privacy Guide Glossary*

**Guide:**

**1. General – Individual Authorization**

KDOA shall not use or disclose any information about a customer or participant of KDOA programs or services without a signed authorization for release of that information from the individual, or the individual's personal representative, unless authorized by this guide, or as otherwise required by state or federal law.

**2. Health Oversight Agency**

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

**3. Exceptions 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]*

- a. KDOA may use or disclose information without an individual's authorization if the law requires or allows such use or disclosure.
- b. Internal communication within KDOA is permitted without individual authorization, in compliance with the KDOA Minimum Necessary Information Guide.
  - i. Mental health records disclosure may be limited to particular program areas named on the authorization form. If such a limitation is noted on the authorization form, disclosure is limited to the parties named.
- c. KDOA customers may access their own information; with certain limitations (see "Customer Privacy Rights").
- d. KDOA may use or disclose psychotherapy notes:
  - i. When a health oversight agency uses or discloses in connection with oversight of the originator of the psychotherapy notes; or
  - ii. To the extent authorized under state law to defend KDOA in a legal action or other proceeding brought by the individual.

- e. KDOA may disclose information for the purposes of payment, treatment, and health care operations.
- f. If KDOA has reasonable cause to believe that an adult is a victim of abuse or neglect, KDOA may disclose protected information to appropriate governmental authorities authorized by law to receive reports of adult abuse or neglect. If KDOA receives information requesting adult protective services, KDOA is authorized to use and disclose the information consistent with its legal authority.
- g. KDOA may disclose individual information without authorization for health oversight activities authorized by law, including audits; civil, criminal, or administrative investigations, prosecutions, or actions; licensing or disciplinary actions; Medicaid fraud; or other activities necessary for health oversight.
- h. Unless prohibited, or otherwise limited, by federal or state law applicable to the program or activity requirements, KDOA may disclose individual information without authorization for judicial or administrative proceedings, in response to an order of a court, a subpoena, a discovery request or other lawful purpose.
- i. For limited law enforcement purposes, to the extent authorized by applicable federal or state law, KDOA may report certain injuries or wounds; provide information to identify or locate a suspect, victim, or witness; alert law enforcement of a death as a result of criminal conduct; and provide information which constitutes evidence of criminal conduct on KDOA premises.
- j. KDOA may disclose to a coroner or medical examiner, for the purpose of identifying a deceased person, determining a cause of death, or other duties authorized by law.
- k. KDOA may disclose individual information without authorization to funeral directors, consistent with applicable law, as needed to carry out their duties regarding the decedent.
- l. KDOA may disclose individual information without authorization to organ procurement organizations or other entities engaged in procuring, banking, or transplantation of cadaver organs, eyes, or tissue, for the purpose of facilitating transplantation.
- m. KDOA may disclose individual information without authorization for research purposes, as specified in KDOA Guide “Uses and Disclosures for Research Purposes & Waivers.”
- n. To avert a serious threat to health or safety, KDOA may disclose individual information without authorization if:
  - i. KDOA believes in good faith that the information is necessary to prevent or lessen as serious and imminent threat to the health or safety of a person or the public; **and**
  - ii. The report is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat.
- o. KDOA may disclose individual information without authorization for other specialized government functions, including authorized federal officials for the conduct of lawful intelligence, counterintelligence, and other national security activities that federal law authorizes.
- p. KDOA may disclose limited information without authorization to a correctional institution or a law enforcement official having lawful custody of an inmate, for the purpose of providing health care or ensuring the health and safety of individuals or other inmates.
- q. In case of an emergency, KDOA may disclose individual information without authorization to the extent needed to provide emergency treatment.
- r. The Family Educational Rights and Privacy Act (FERPA) and state law applicable to student records governs KDOA access to, use, and disclosure of student records.

4. **Authorization Not Required When Customer is Informed in Advance & Given Opportunity to Object:**
  - a. In limited circumstances, KDOA may use or disclose an individual's information without authorization if:
    - i. KDOA informs the individual in advance and the person has been given an opportunity to object.
    - ii. Unless otherwise protected by law, KDOA may orally inform the individual and obtain and document the individual's oral agreement.
  - b. 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 named 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.
  - c. Oral permission to use or disclose information for the purposes described in subsections (a) of this section is not sufficient when the individual is referred to or is receiving mental health treatment services, where written authorization for the treatment program to make such disclosures is required.
5. **Re-disclosure of an Individual's Information:**
  - a. Unless prohibited by state and federal laws, information held by KDOA and authorized by the individual for disclosure may be subject to re-disclosure and no longer protected by KDOA guide. 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.
  - b. K.S.A. 65-119 prohibits further disclosure of HIV information.
  - c. K.S.A. - \_\_\_\_\_ prohibits further disclosure of genetics information without the specific written consent of the person to whom it pertains, or as otherwise permitted by such regulations. A general authorization for the release of medical information is not sufficient for this purpose.
  - d. K.S.A. - \_\_\_\_\_ places restrictions on re-disclosure of information regarding customers of publicly funded mental health or developmental disability providers.
6. **Revocation of Authorization**
  - a. An individual may revoke an authorization at any time.
  - b. 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 KDOA.
  - c. No such revocation shall apply to information already released while the authorization was valid and in effect.
7. **Verification of Individuals Requesting Information**

Information about an individual may be disclosed only upon reasonable verification of the identity of the person requesting the information.
8. **Denial of Requests for Information**

KDOA shall deny any request for individual information, unless an individual has signed an authorization, or the information about the individual can be disclosed pursuant to this guide or as authorized by federal or state law.

**Form(s):**

- KDOA 2097, “Disclosures of Protected Information”
- KDOA 2098, “Authorization for Uses and Disclosures of Non-Health Information”
- KDOA 2099, “Authorization for Uses and Disclosures of Health Information”

**Reference(s):**

- 45 CFR 164.502(a)
- 45 CFR 164.508-164.512
- 42 CFR Part 2
- ORS 179.505

**Contact(s):**

- Privacy Coordinator

**ENFORCEMENT, SANCTIONS, AND PENALTIES FOR VIOLATIONS OF INDIVIDUAL PRIVACY**

**Purpose:**

The intent of this guide is to specify enforcement, sanction, penalty, and disciplinary actions that may result from violation of KDOA policies regarding the privacy and protection of an individual’s information and to offer guidelines on how to conform to the required standards.

*Reference: See KDOA Privacy Guide Glossary*

**Guide:**

**1. General**

- a. All members of the KDOA workforce (employees, volunteers, trainees, & other persons who conduct work under the direct control of KDOA) must guard against improper uses or disclosures of a KDOA customer’s information.
  - i. Members of the KDOA workforce who are uncertain if a disclosure is permitted are advised to consult with a supervisor in the KDOA workplace. The KDOA Privacy Officer is a resource for any member of the KDOA workforce that cannot resolve a disclosure question, and may be consulted in accordance with the operational procedures of that KDOA workplace.
- b. All KDOA workforce members are required to be aware of their responsibilities under KDOA private policies.
  - i. KDOA employees will be expected to sign a “Privacy & Security Statement of Understanding,” indicating that they have been informed of the business practices in KDOA as it relates to Privacy, and they understand their responsibilities to ensure the Privacy of KDOA customers.
- c. KDOA employees who violate KDOA policies and procedures regarding the safeguarding of an individual’s information are subject to disciplinary action by KDOA.

- d. KDOA employees who violate applicable law for improper use or disclosure of an individual's information may be subject to civil or criminal penalties imposed by law.

## 2. Disclosures by Whistleblowers and Workforce Crime Victims

- a. A KDOA employee may disclose an individual's protected customer information if:
  - i. The KDOA employee believes, in good faith, that KDOA has engaged in conduct that is unlawful or that otherwise violates professional standards or KDOA guide, or that the care, services, or conditions provided by KDOA could endanger KDOA staff, persons in KDOA care or the public; and
  - ii. The disclosure is to:
    - A. An oversight agency or public authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of KDOA;
    - B. An appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or of misconduct by KDOA; or
    - C. An attorney retained by or on behalf of the KDOA employee for the purpose of determining the legal options of the KDOA employee with regard to this KDOA guide.
- b. A KDOA employee may disclose limited protected information about an individual to a law enforcement official if the employee is the victim of a criminal act and the disclosure is:
  - i. About only the suspected perpetrator of the criminal act; and
  - ii. Limited to the following information about the suspected perpetrator:
    - A. Name and address;
    - B. Date and place of birth;
    - C. Social security number;
    - D. ABO blood type and rh factor;
    - E. Type of any injury;
    - F. Date and time of any treatment; and
    - G. Date and time of death, if applicable.

## 3. Retaliation prohibited

- a. Neither KDOA as an entity nor any KDOA employee will intimidate, threaten, coerce, discriminate against, or take any other form of retaliatory action against any individual for:
  - i. Filing of a complaint with KDOA or with DHHS as provided in KDOA privacy policies; or
  - ii. Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing relating to KDOA privacy policy and procedures.
    - A. Opposing any unlawful act or practice, provided that:
      - 1. The individual or other person (including a KDOA employee) has a good faith belief that the act or practice being opposed is unlawful; and
      - 2. The manner of such opposition is reasonable and does not involve a use or disclosure of an individual's protected information in violation of KDOA guide.

**Form(s):**

- “Privacy Program Statement of Understanding”

**Reference(s):**

- 45 CFR 164.530

**Contact(s):**

- Privacy Coordinator