

**KENTUCKY PERSONNEL CABINET
DEPARTMENT OF EMPLOYEE INSURANCE
KENTUCKY EMPLOYEES’ HEALTH PLAN
HIPAA PRIVACY POLICIES AND PROCEDURES**

Table of Contents

1. Introduction	1
.....	
2. Privacy Official and Contact Person	1
.....	
3. Safeguards	1
.....	
4. Complaints	5
.....	
5. Sanctions for Violations of Privacy Policy	6
.....	
6. Mitigation of Disclosures of PHI	6
.....	
7. No Intimidating or Retaliatory Acts; No Waiver of Rights	8
.....	
8. Plan Document	9
.....	
9. Use and Disclosure Defined	10
.....	
10. Workforce, Human Resource Generalists and Insurance Coordinators Must Comply with Plan’s Policy and Procedure	12
.....	
11. Permitted Uses and Disclosures for Plan Administration Purposes	12
.....	
12. No Disclosure of PHI for Non-Health Plan Purposes	14
.....	
13. Mandatory Disclosures of PHI and as Required by Law	14
.....	
14. Business Associates	18
.....	
15. Disclosures of PHI Pursuant to an Authorization	19
.....	

16. Complying with the “Minimum Necessary Standard”	20
.....	
17. Disclosures of De-Identified Information	21
.....	
18. Breach Notification Requirements	23
.....	
19. Accounting: Disclosure of PHI	25
.....	
20. Accounting: Request Amendments to PHI	27
.....	
21. Requests for Alternative Communication Means or Locations	29
.....	
22. Requests for Restrictions on Use and Disclosure of PHI	29
.....	
23. Documentation	31
.....	
<u>Exhibit 1: DEI Breach Notification Policy</u>	32
.....	
<u>Exhibit 2: DEI Privacy Complaint Procedures</u>	37
.....	

1. Introduction

It shall be the policy of the Personnel Cabinet, Department of Employee Insurance (DEI) to protect and safeguard the protected health information created, acquired and maintained in accordance with the Privacy Regulations promulgated pursuant to the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and any applicable state laws.

The Policies contained herein are intended to provide guidance to DEI Staff in regard to the protection and enhancement of Kentucky Employees' Health Plan (KEHP) Members rights by:

- a. establishing rules related to the internal and external Use and Disclosure of Protected Health Information (PHI);
- b. affording access and information regarding the Use and Disclosure of their PHI; and
- c. implementing administrative procedures intended to assist Members and DEI Staff to implement these Policies.

These Policies will apply to all PHI collected by DEI after January 1, 2006. The Policies apply to all DEI Staff and others involved in the administration of KEHP. This Policy was updated in September 2010 and November 2011.

These Policies supersede and replace any existing policies and procedures.

2. Privacy Official and Contact Person

Joe R. Cowles, General Counsel, DEI, is the Privacy Official for KEHP. The Privacy Official and the DEI Commissioner's Office will be responsible for the development and implementation of policies and procedures relating to privacy, including but not limited to this Privacy Policy and KEHP's privacy Use and Disclosure procedures. The Privacy Official also serves as the contact person for Members who have questions, concerns, or complaints about the privacy of their PHI.

The Privacy Official and DEI Commissioner's Office will be responsible for ensuring that KEHP complies with the provisions of the HIPAA Privacy Rules regarding Business Associates, including the requirement that KEHP has a HIPAA-compliant Business Associate Agreement in place with all Business Associates. The Privacy Official and DEI Commissioner's Office will be responsible for monitoring compliance by all Business Associates with the HIPAA Privacy Rules and KEHP's Privacy Policy.

3. Safeguards

The purpose of this policy is to establish guidelines for the safeguarding of PHI and to limit unauthorized disclosures.

DEI will establish on behalf of KEHP appropriate administrative, technical and physical safeguards to prevent PHI from intentionally or unintentionally being used or disclosed in violation of HIPAA requirements.

DEI will implement appropriate administrative, technical, and physical safeguards that will reasonably safeguard PHI from any intentional or unintentional Use or Disclosure in violation of these Privacy and Security Policies and the HIPAA Privacy or Security Regulations.

DEI Staff must reasonably safeguard PHI to limit incidental Uses or Disclosures made pursuant to an otherwise permitted or required Use or Disclosure.

This policy establishes minimum administrative and physical standards regarding the protection of PHI that DEI must enforce, as applicable.

Technical Safeguards regarding the protection of PHI maintained in electronic form are available in the HIPAA Security Policies. Same are incorporated by reference into this Policy.

A. Administrative Safeguards.

- 1) Oral Communications. DEI Staff must exercise due care to avoid unnecessary Disclosures of PHI through oral communications. Voices should be modulated and attention should be paid to unauthorized listeners in order to avoid unnecessary Disclosures of PHI. Identifying information should only be disclosed during oral conversations when necessary to further operational purposes. Dictation and telephone conversations must be conducted away from public areas if possible. Speakerphones may be used only in private areas.
- 2) Telephone Messages. Telephone messages containing demographic PHI may be left on answering machines and voice mail systems, unless the KEHP Member has requested and received approval for an alternative means of communication pursuant to Communication by Alternative Means – see Section 21. Requests for Alternative Communication Means or Locations. KEHP Authorizations can be found at: <http://personnel.ky.gov/dei/hipaa.htm>
- 3) Faxes. The following procedures must be followed when faxing PHI:
 - a) Only the PHI necessary to meet the authorized requester’s needs for administration of the health plan may be faxed.
 - b) All faxes containing PHI must be accompanied by a cover sheet that includes a confidentiality notice. A sample fax cover sheet is available upon request.

- c) Reasonable efforts shall be made to verify that fax transmissions are sent to the correct destination. Frequently used numbers should be programmed into fax machines or computers to avoid dialing errors. Programmed numbers should be verified on a regular basis. The numbers of new recipients should be verified prior to transmission.
- d) Fax machines must be located in secure areas not readily accessible to visitors or KEHP Members. Incoming faxes containing PHI must not be left on or near the fax machine for extended periods of time.
 - e) Fax confirmation sheets shall be reviewed to ensure the intended destination matches the number on the confirmation. The confirmation sheet shall be attached to the document faxed.
 - f) All instances of misdirected faxes containing PHI must be investigated and mitigated pursuant to and consistent with all Privacy Policies.
- 4) Mail. PHI shall be mailed in sealed envelopes. PHI mailed from DEI should be sent via first class mail and should be concealed.
- 5) Copying. All copying machines within DEI offices require an access code to operate.
- 6) Destruction Standards. PHI must be discarded in a manner that protects the confidentiality of such information. Paper and other printed materials containing PHI shall be destroyed or cross-cut shredded so that they cannot be read or reconstructed. Magnetic media and diskettes containing PHI shall be overwritten or reformatted.

B. Physical Safeguards.

- 1) Secure Floor. DEI offices are located on a secure floor. Access is limited to only necessary and authorized DEI Staff and Personnel Cabinet officials. Access is monitored daily and reports are reviewed on a weekly basis to ensure only necessary and authorized Staff are on the secure floor.
- 2) Paper Records. Paper records must be stored or filed in such a way as to avoid access by unauthorized persons. Some type of physical barrier must be used to protect paper records from unauthorized access. Paper records on desks or counters must be placed face down or concealed to avoid access by unauthorized persons. Paper records shall be secured when the office area is unattended by persons authorized to have access to paper records. Original paper records should not be removed from DEI premises unless necessary to operate the health plan or required by law. DEI Staff shall not remove paper records for their own convenience. Should DEI Staff need to remove any paper records from DEI premises the removal must be approved by a supervisor. Paper records that are removed from DEI premises must not be left unattended in places in which unauthorized persons can gain access, legally or otherwise. Paper records should not be left in automobiles or in view of passers-by. The theft or loss of any paper record shall be reported immediately to the Privacy Official so that mitigation options can be considered and implemented.

- 3) Escorting Visitors. Visitors must be appropriately escorted and monitored when on DEI premises where PHI is located to ensure they do not have access to PHI. Persons who are not employed by DEI shall not be in areas where PHI is stored, without appropriate continued supervision.
- 4) Computer/Work Stations Computer screens on unattended computers must be returned to a password-protected screen saver or login screen.

C. Technical Safeguards.

- 1) Commonwealth Office of Technology (COT). The Commonwealth Office of Technology (COT) has been given statutory authority under KRS 42.726 to develop strategies and policies to support and promote the effective applications of Information Technology (IT) within state government, including DEI. In addition COT is responsible for developing, implementing, and managing strategic information technology directions, standards, and enterprise architecture, including implementing necessary management processes to assure full compliance with those directions, standards, and architecture. This specifically includes but is not limited to directions, standards, and architecture related to the privacy and confidentiality of data collected and stored by state agencies, including DEI. COT has established Enterprise Policies that articulate the rules and regulations of state government regarding information technology. Enterprise Policies may be found at: <http://technology.ky.gov/governance/Pages/policies.aspx>
- 2) E-mail within DEI and COT. E-mails sent within the COT e-mail system that contain PHI should be encrypted. PHI sent must be limited to the minimum necessary and should be sent as a limited data set when possible.
- 3) E-mail Outside DEI. Except in emergency situations, the use of e-mail to transmit PHI outside the COT e-mail system is prohibited unless the message is encrypted between sender and recipient in a manner that satisfies Health Information Technology for Economic and Clinical Health Act (HITECH) requirements.

Confidentiality Notice. All e-mails transmitted with PHI shall contain a confidentiality notice indicating that “This communication contains information which is confidential and which is for the exclusive use of the intended recipient(s). If you are not an intended recipient, please note that any form of distribution, copying, forwarding, or use of this communication or the information therein is strictly prohibited and may be unlawful. If you have received this communication in error, please return it to the sender, delete this communication, and destroy all copies.

- 4) Electronic Documents. Documents and attachments and/or images containing PHI must be stored on network servers with appropriate security restrictions.
- 5) Portable Computing Devices. (i.e., laptops and hand-held computers). DEI Staff must use extreme caution when using Portable Computing Devices to store PHI. PHI should not be stored on Portable Computing Devices unless absolutely necessary but

rather should be stored on servers in a secure enterprise data center. Portable Computing Devices must never be left unattended in unsecured places. Staff storing PHI on personal portable devices are responsible for the security of the PHI stored on such devices. PHI contained on such devices must be encrypted. All COT Standards for Portable Computing Device Security, such as password protection, must be followed. The failure to take appropriate security precautions will be considered a violation of these Policies subjecting the Staff to sanctions.

- 6) Other Uses of the Internet. Any other electronic transmission of PHI requires that appropriate safeguards and procedures be implemented and approved by COT.
- 7) Use of Social Media Sites. PHI shall not be posted on social media sites, such as Facebook or Twitter.
- 8) Use of Digital Copiers/Scanners. DEI uses digital copiers, scanners, and fax machines and DEI Staff must verify that appropriate data security features (i.e., encryption, overwriting) are enabled. In addition, before such equipment is returned to the vendor, surplused, or otherwise disposed of, the vendor must take steps to ensure the hard drive is destroyed or completely overwritten. These steps may include, but are not limited to, imposing these requirements on the vendor or working with IT Security.
- 9) Theft or Loss. The theft or loss of any electronic record or device containing PHI shall be reported immediately to the Privacy and Security Officials so that mitigation and reporting options can be considered and implemented.

4. Complaints

The purpose of this policy is to establish procedures for individuals to submit complaints alleging Privacy incidents regarding DEI's Privacy Policies and the alleged failure to comply with such Policies by DEI Staff and others.

All incidents regarding DEI's Privacy Policies and compliance with such Policies, regardless of the form in which they are received, will be documented, reviewed, and acted upon, if necessary, by DEI's Privacy Official or designee. Documentation regarding complaints received and the resolution of such complaints will be retained, in written or electronic format, for at least six (6) years.

- A. DEI has developed and implemented an internal process for receiving privacy complaints, reporting them immediately to DEI's Privacy Official, and investigating them in coordination with the Privacy Official. This process can be as simple as notifying employees that each individual reporting a Privacy-related incident should be instructed to contact the DEI Privacy Official or designee. DEI shall track privacy complaints received using a process that involves notification of the DEI's Privacy Official of each complaint received so that the Privacy Official can also record and track the investigation and response to each complaint and can participate in the resolution of such complaints.

- B. The Privacy Official, DEI's Commissioner's Office, and the Personnel Cabinet's internal auditor will document each complaint received and maintain such documentation for at least six (6) years.
- C. The Privacy Official and DEI's Commissioner's Office will be responsible for the investigation and management of each complaint.
- D. A record of each Privacy incident, to the extent necessary or required by the investigation, and the resolution will be maintained.
- E. A copy of the complaint procedures will be provided to any KEHP Member upon request. The complaint procedures are contained in Exhibit 2.

5. Sanctions for Violations of Privacy Policy

The purpose of this policy is to ensure there are appropriate sanctions that will be applied to Employees and Business Associates who violate the requirements of HIPAA Privacy Regulations and/or DEI HIPAA Privacy Policies and Procedures.

DEI will apply appropriate sanctions against DEI Staff, Insurance Coordinators (ICs), Human Resource Generalists (HRGs) and its Business Associates who fail to comply with DEI's Privacy Policies and/or the HIPAA Privacy Regulations. DEI will not impose sanctions against DEI Staff or Business Associates for: (a) engaging in whistleblower activities; (b) submitting a complaint to the Secretary of the Department of Health and Human Services (HHS); (c) participating in an investigation; or (d) registering opposition to a violation of the HIPAA Privacy Regulations.

- A. Employees. A violation of the DEI Privacy Policies by Staff will be subject to sanction. The sanction imposed for a violation of the Privacy Policies will depend on the severity of the violation and will be imposed in accordance with KRS Chapter 18A or Personnel Cabinet policy, whichever is applicable.
- B. Business Associates. If DEI knows of a pattern of activity or practice of a Business Associate that constitutes a material breach or violation of the Business Associate's obligations under his/her/its contract with DEI, DEI will take reasonable steps to cure the breach or end the violation, as applicable, and, if such steps are unsuccessful: (a) terminate the contract, if feasible; or (b) report the problem to the Secretary of the Department of HHS or other applicable government agency. The term "Business Associate" is defined in Section 14.
- C. Documentation. Documentation regarding any sanction imposed for a violation of the Privacy Policies should be retained in the sanctioned employee's personnel or Agency file or a separate designated Agency file for ICs and HRGs, in written or electronic format, for at least six (6) years. Copies of such documentation should be forwarded to

the Privacy Official who also should maintain such documentation for the minimum retention period. Documentation of any sanction imposed against a Business Associate should be retained by the Privacy Official for the minimum retention period.

- D. Violation Review. The Privacy Official shall review the circumstances surrounding any substantiated violation and take appropriate action to mitigate, to the extent possible, any harmful effects of the violation. If, at the conclusion of the investigation, it is found that a violation of the Privacy Policy or Procedure has occurred, the Employee involved shall be disciplined in accordance with the severity of the violation. When imposing sanctions for the inappropriate use and disclosure of PHI, consideration should be given to whether the use or disclosure was made as a result of (a) carelessness or negligence, (b) curiosity or concern, or (c) the desire for personal gain or malice. Sanctions for using or disclosing PHI in violation of HIPAA or these Privacy Policies and Procedures will be imposed in accordance with DEI's policy, up to and including termination. Sanctions for ICs and HRGs include losing security access to the Kentucky Human Resource Information System (KHRIS).
- E. Notification. Consistent with DEI Breach Notification Policy, the violation will be reported to the United States Department of Human and Health Services, Civil Rights Office. If the violation involves more than five hundred (500) Members of KEHP, the local media (TV, newspaper, or radio) will be contacted to make known the violation.

6. Mitigation of Disclosures of PHI

The purpose of this policy is to establish procedures regarding the mitigation of harmful effects of inappropriate Uses or Disclosures of PHI.

DEI will mitigate, to the extent practicable, any harmful effect that is known to DEI of a Use or Disclosure of PHI in violation of DEI's Privacy Policies and Procedures or the HIPAA Privacy Regulations by DEI, DEI Staff, ICs, HRGs or a Business Associate. This applies to both intentional and unintentional disclosures of PHI.

- A. DEI must take all practicable steps to mitigate the harmful effects of a confirmed inappropriate Use or Disclosure. The type of mitigation that occurs will be based on the facts and circumstances of each case, based on the following factors:
- 1) knowledge of where the information has been disclosed;
 - 2) how the information might be used to cause harm to KEHP Member or another individual; and
 - 3) what steps can actually have a mitigating effect under the facts and circumstances of any specific situation.
- B. DEI must investigate the cause of the inappropriate Use or Disclosure and take corrective actions to prevent such Uses or Disclosures from recurring.

- C. DEI shall notify the Privacy Official, in accordance with Privacy Complaint Reporting Procedure, of inappropriate Uses and Disclosures, the results of the investigation, and the proposed mitigation efforts. The Privacy Official and Internal Auditor will assist with the investigation and provide DEI Commissioner's Office advice regarding mitigation efforts. If legal action is threatened or is a distinct possibility, the Personnel Cabinet Office of Legal Services must be notified.

7. No Intimidating or Retaliatory Acts; No Waiver of Rights

The purpose of this policy is to prohibit retaliation against individuals and others who exercise their rights under the HIPAA Privacy Regulations.

Neither DEI nor DEI Staff shall intimidate, threaten, coerce, discriminate against, or take other retaliatory action against:

- A. Individuals. Any individual for the exercise by the individual of any right under, or for participation by the individual in, any process established by the HIPAA Privacy Regulations;
- B. Individuals and Others. Any individual or other person for:
 - 1) Filing a complaint with DEI, or the Secretary of the Department of HHS as permitted by the HIPAA Privacy Regulations;
 - 2) Testifying, assisting, or participating in an investigation, compliance audit or review, proceeding, or hearing conducted by DEI or a government enforcement agency under the HIPAA Privacy Regulations; or
 - 3) Opposing any act or practice made unlawful by the HIPAA Privacy Regulations, provided the individual or other has a good faith belief that the practice opposed is unlawful and the manner of the opposition is reasonable and does not involve a disclosure of PHI in violation of the HIPAA Privacy Regulations or DEI's Privacy Policies and Procedures.

For purposes of this Policy, the term "individual" is not limited to natural persons, but includes any type of organization, association, or group such as other Covered Entities, Health Oversight Agencies, and advocacy groups.

Any individual who believes that some form of retaliation against an individual or other for exercising rights under the HIPAA Privacy Regulations is occurring or has occurred should report the incident to the Privacy Official.

If the Privacy Official receives a report of retaliation, the Privacy Official will conduct an investigation to determine if retaliation has occurred. If the report is substantiated, sanctions will be imposed in accordance with the Privacy Policies.

- C. **Waiver of Rights.** DEI will not require KEHP Members to waive (a) their right to file a complaint with the Secretary of the Department of HHS or any other enforcement agency regarding DEI's compliance with the HIPAA Privacy Regulations or (b) any other rights under the HIPAA Privacy Regulations as a condition of Treatment or Payment Activities.

8. Plan Document

The purpose of the Plan Document is to include provisions to describe the permitted and required Uses and Disclosures of PHI by DEI for administrative or other permitted purposes of KEHP.

KEHP's Plan Document will require DEI to:

- 1) not Use or further Disclose PHI other than as permitted by KEHP documents or as required by law;
- 2) ensure that any agents or subcontractors to whom it provides PHI received from KEHP agree to the same restrictions and conditions that apply to DEI;
- 3) not Use or Disclose PHI for employment-related actions;
- 4) report to the Privacy Official any Use or Disclosure of the information that is inconsistent with the permitted Uses or Disclosures;
- 5) make PHI available to KEHP Participants, consider their amendments and, upon request, provide them with an accounting of PHI disclosures in accordance with the HIPAA privacy rules;
- 6) make DEI's internal practices and records relating to the Use and Disclosure of PHI received from the Plan available to the Department of HHS upon request; and
- 7) if feasible, return or destroy all PHI received from the KEHP that DEI maintains in any form and retain no copies of such information when no longer needed for the purpose for which Disclosure was made, except that, if such return or destruction is not feasible, limit further Uses and Disclosures to those purposes that make the return or destruction of the information feasible.

The Plan document will require DEI to (1) certify to the Privacy Official that the Plan Document has been amended to include the above restrictions and that DEI agrees to those restrictions; and (2) provide adequate firewalls in compliance with the HIPAA Privacy Rules.

9. Use and Disclosure Defined

DEI cannot Use or Disclose PHI, except as permitted by its Privacy Policies and Procedures and the HIPAA Privacy Regulations.

- A. Required Disclosures. DEI will Use or Disclose PHI:
- 1) to a KEHP Member, when requested under the following Privacy Policy entitled “KEHP Member Access to PHI, and Accounting of Disclosures;” and
 - 2) when required by the Secretary of the Department of HHS to investigate DEI compliance with the HIPAA Privacy Regulations or otherwise Required by Law.
- B. Permitted Uses and Disclosures. DEI Staff are permitted to Use or Disclose PHI as follows:
- 1) for Payment or Health Care Operations;
 - 2) incident to a Use or Disclosure otherwise permitted or required by the HIPAA Privacy Regulations as long as the Minimum Necessary policies have been followed;
 - 3) pursuant to an authorization as permitted;
 - 4) pursuant to an agreement under, or as otherwise permitted by, HIPAA Privacy Policies;
 - 5) as permitted by and in compliance, Required by Law; Business Associate, etc.
- C. “Health Care Operations”. These include but are not limited to any of the following activities of DEI to the extent that the activities are related to Covered Functions:
- 1) conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
 - 2) business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating DEI, including formulary development and administration, or improvement of methods of payment or coverage policies; and
 - 3) business management and general administrative activities of DEI, including, but not limited to: (1) management activities relating to implementation of and compliance with the DEI’s Privacy Policies and Procedures; (2) resolution of internal grievances; (3) due diligence related to the sale, transfer, merger, or consolidation of all or part of DEI with another covered entity; and (4) creating de-identified health information or a limited data set and fundraising for the benefit of DEI. *See* 45 C.F.R. § 164.501.
- D. “Payment”. Payment means any activities of DEI to obtain payment for providing Health Care. Such activities relate to the individual to whom Health Care is provided and include, but are not limited to:
- 1) billing, claims management, collection activities, and related Health Care data processing; and

- 2) Disclosure to consumer reporting agencies of any of the following PHI relating to collection of premiums or reimbursement:
 - a) name and address;
 - b) date of birth;
 - c) social security number;
 - d) payment history;
 - e) account number; and
 - f) name and address of the Health Care Provider. *See* 45 C.F.R. §164.501.

E. Limited Data Sets:

DEI may Use and Disclose a limited data set without KEHP Member authorization only for the purposes of Research, public health, or Health Care Operations if DEI enters into a data use agreement with the intended recipient of the limited data set. DEI may Use PHI to create a limited data set or Disclose PHI to a Business Associate to create a limited data set on behalf of DEI.

If DEI knows of a pattern of activity or practice of the limited data set recipient that constitutes a material breach or violation of the data use agreement, it must take reasonable steps to cure the breach or end the violation, as applicable. If such steps are unsuccessful, DEI must discontinue Disclosure of PHI to the recipient and report the problem to the Secretary of the Department of HHS.

In order to create a limited data set, the following direct identifiers of the KEHP Member or of relatives, employers, or household members of the KEHP Member must be removed:

- 1) Names;
- 2) Postal address information, other than town, city, state, and zip codes;
- 3) Telephone numbers;
- 4) Fax numbers;
- 5) Electronic mail addresses;
- 6) Social Security Numbers;
- 7) Health plan beneficiary numbers;
- 8) Account numbers;
- 9) Certificate/license numbers;
- 10) Web Universal Resource Locators (URLs);
- 11) Internet Protocol (IP) address numbers; and
- 12) Biometric identifiers, including fingerprints and voiceprints.

The KEHP Member's birth date should be Disclosed only if DEI and the recipient of the information agree that it is needed for their purpose.

F. Data Use Agreements.

All data use agreements must be approved by the Personnel Cabinet Office of Legal Services prior to execution. A data use agreement must:

- 1) Establish the permitted Uses and Disclosures of the limited data set.
- 2) Establish who is permitted to Use or receive the limited data set.
- 3) Provide that the recipient of the information will:
 - a) Not use or further Disclose the information other than as permitted by the agreement;
 - b) Use appropriate safeguards to prevent Use or Disclosure of the information other than as permitted by the agreement;
 - c) Report to DEI any Uses or Disclosures the recipient is aware of that are not provided for by the data use agreement;
 - d) Ensure that the recipient's agents who have access to the information agree to the same restrictions as imposed on the recipient;
 - e) Not to be used to identify the information or contact the KEHP Members.

For other Uses and Disclosures, DEI Staff should first consult with the Privacy Official or the Personnel Cabinet Office of Legal Services.

10. Workforce, Human Resource Generalist and Insurance Coordinator Must Comply with Plan's Policy and Procedures

All DEI Staff, ICs and HRGs who have access to KEHP PHI must comply with this Policy.

See Personnel Cabinet, Department of Employee Insurance, KEHP Administrative Manual for additional information. Click here for access: [KEHP Administrative Manual](#).

11. Permitted Uses and Disclosures for Plan Administration Purposes

DEI may Use or Disclose PHI for its own Payment or Health Care Operations.

DEI may disclose PHI:

- 1) to another Covered Entity for the Payment activities of the entity that receives the information; and
- 2) to another Covered Entity for Health Care Operations activities of the entity that receives the information, if each entity either has or had a relationship with the KEHP

Member who is the subject of the PHI being requested and the health information pertains to such relationship.

For Uses and Disclosures of a KEHP Member's PHI other than for Treatment, Payment Activities, and Health Care Operations, an authorization from the KEHP Member must be obtained unless Disclosure is permitted and/or required pursuant to another Policy.

"Health Care Operations" includes but is not limited to any of the following activities of DEI to the extent that the activities are related to Covered Functions:

- 1) conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
- 2) business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating DEI, including formulary development and administration, or improvement of methods of payment or coverage policies; and
- 3) business management and general administrative activities of DEI, including, but not limited to: (1) management activities relating to implementation of and compliance with the DEI's Privacy Policies and Procedures; (2) resolution of internal grievances; (3) due diligence related to the sale, transfer, merger, or consolidation of all or part of DEI with another covered entity; and (4) creating de-identified health information or a limited data set and fundraising for the benefit of DEI. *See* 45 C.F.R. § 164.501.

"Payment" means any activities of DEI to obtain payment for providing Health Care. Such activities relate to the individual to whom Health Care is provided and include, but are not limited to: (a) billing, claims management, collection activities, and related Health Care data processing; and (b) Disclosure to consumer reporting agencies of any of the following PHI relating to collection of premiums or reimbursement: (i) name and address; (ii) date of birth; (iii) social security number; (iv) payment history; (v) account number; and (vi) name and address of the Health Care Provider. *See* 45 C.F.R. § 164.501.

DEI primarily Uses and Discloses in pursuit of Payment or Health Care Operations as follows:

- 1) Any and all Staff Members of DEI. This specifically includes for purposes of this document: the Commissioner's Office, Division of Insurance Administration; Division of Financial and Data Services, Wellness Staff, Personnel Cabinet Office of Legal Services and properly designated Members of the executive Staff of the Personnel Cabinet. Employees with access may disclose PHI to other employees with access for plan administrative functions (but the PHI disclosed must be limited to the minimum amount necessary to perform the plan administrative function). Employees with access may not disclose PHI to employees (other than employees with access) unless an authorization is in place or the disclosure otherwise is in compliance with this Policy and KEHP's Privacy Use and Disclosure Procedures.
- 2) Designated ICs and HRGs. Designated ICs and HRGs with access may disclose PHI to other employees, ICs and HRGs with access for plan administrative functions (but

the PHI disclosed must be limited to the minimum amount necessary to perform the plan administrative functions). ICs and HRGs with access may not disclose PHI to employees, ICs, and HRGs (other than employees, ICs, and HRGs with proper security access) unless an authorization is in place or the disclosure otherwise is in compliance with this Policy and KEHP's Privacy Use and Disclosure Procedures.

12. No Disclosure of PHI for Non-Health Plan Purposes

DEI cannot Use or Disclose PHI, except as permitted by its Privacy Policies and Procedures and the Privacy Regulations.

DEI may disclose PHI:

- 1) to another Covered Entity for the Payment activities of the entity that receives the information; and
- 2) to another Covered Entity for Health Care Operations activities of the entity that receives the information, if each entity either has or had a relationship with the KEHP Member who is the subject of the PHI being requested and the health information pertains to such relationship.

For Uses and Disclosures of a KEHP Member's PHI other than for Payment activities and Health Care Operations, an authorization from the KEHP Member must be obtained unless Disclosure pursuant to another Policy is permitted and/or required.

See Section 11. *Permitted Uses and Disclosures for Plan Administration Purposes* for additional information.

13. Mandatory Disclosures of PHI and as Required by Law

A Member's PHI must be disclosed, in accordance with KEHP's Privacy Use and Disclosure Procedures, in the following situations:

- 1) The disclosure is to the individual who is the subject of the information;
- 2) The disclosure is required by law; or
- 3) The disclosure is made to the Department of HHS for purposes of enforcing the Health Insurance Portability and Accountability Act (HIPAA).

A. Disclosures of PHI Pursuant to an Authorization:

See Privacy Policies and Procedures concerning KEHP Member Authorizations. KEHP Authorizations can be found at: <http://personnel.ky.gov/dei/hipaa.htm>

B. Disclosures Required by Law:

DEI may use or disclose PHI to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law. “Required by law” means a mandate in law enforceable in court that compels an entity to disclose PHI. The exception provides that disclosures about victims of abuse, neglect, or domestic violence, for judicial and administrative proceedings, or for law-enforcement purposes, even if required by law, must also comply with the conditions specific to those disclosures under the Privacy rule.

DEI may Disclose PHI without the KEHP Member’s consent, authorization, or opportunity to agree or object as required by applicable state and federal laws, including those listed below.

1) Abuse or Neglect of Children.

Reporting Child Abuse, Neglect, or the Birth of a Chemically-Dependent Child is required. All DEI Staff who have reason to believe that a child under the age of 18 is a victim of abuse or neglect must promptly notify the Cabinet for Health and Family Services.

“Abuse” for purposes of this section means harm or threatened harm to a child’s health, safety, or welfare by a parent; legal guardian; custodian; foster parent; adult residing in the home of the child; the owner, operator, or employee of a child care facility, or an agent or employee of a private residential home, institution, facility, or day treatment program.

“Neglect” for purposes of this section means a failure to provide (a) adequate food, clothing, shelter, medical care, and supervision; (b) special care which is necessary because of the physical or mental condition of the child; or (c) abandonment.

Reports of abuse or neglect may be made by telephone, in writing, or in person.

2) Adult Victims of Abuse, Neglect, Domestic Violence, or Criminally-Injurious Conduct.

DEI Staff, who have reasonable cause to believe that a Vulnerable Adult is suffering from abuse, neglect, or exploitation shall promptly report the matter to the Cabinet for Health and Family Services; the office of the district attorney in the county in which the suspected abuse, neglect, or exploitation occurred; or the local police or sheriff’s department.

A “Vulnerable Adult” is a person who is incapacitated or who, because of physical or mental disability, incapacity, or other disability is substantially impaired in the ability to provide adequately for the care or custody of him/herself; is unable to manage his or her property and financial affairs effectively; is unable to meet essential

requirements for mental or physical health or safety; or is unable to protect him/herself from abuse, neglect, or exploitation without assistance from others.

“Abuse” for purposes of this section means causing or permitting: (i) the infliction of physical pain, injury, sexual abuse, sexual exploitation, unreasonable restraint or confinement, or mental anguish, or (ii) the deprivation of nutrition, clothing, shelter, health care, or other care or services without which serious physical or mental injury is likely to occur to a Vulnerable Adult by a caretaker or other person providing services to a Vulnerable Adult.

“Exploitation” or “Exploit” means an unjust or improper use of the resources of a Vulnerable Adult for the profit or advantage, economic or otherwise, of a person other than the Vulnerable Adult through the use of undue influence, coercion, harassment, duress, deception, false presentation, or false pretense.

“Neglect” for purposes of this section means: (a) the failure to provide protection for a Vulnerable Adult who is unable to protect his or her own interest; (b) the failure to provide a Vulnerable Adult with adequate shelter, nutrition, health care, or clothing; or (c) the causing or permitting of harm or the risk of harm to a Vulnerable Adult through the action, inaction, or lack of supervision by a caretaker providing direct services.

Reports of Abuse, Neglect, and Domestic Violence may be made by telephone, in writing, or in person.

3) Court Orders.

A court order is a direction of the court that orders a party to produce certain specified documents. Upon the receipt of a court order for the disclosure of medical records containing PHI, DEI or the recipient of the order must immediately forward the court order to the Personnel Cabinet Office of Legal Services. Upon determining that the court order is valid and meets all legal requirements, DEI should release the information pursuant to the court order. The KEHP Members whose records are being requested are not required to provide an authorization to Disclose the records pursuant to a court order.

4) Subpoenas.

A subpoena is a unilateral request of a party for the production of documents. A subpoena is not generally approved by a judge. Therefore, it is important for DEI to determine whether the KEHP’s Member’s authorization or a court order is required for the release. All subpoenas must be sent to the Personnel Cabinet Office of Legal Services.

5) Other Disclosures to Law Enforcement Officials.

- a) Certain limited PHI regarding a KEHP Member's PHI may be Disclosed to a Law Enforcement Official who requests such information to identify or locate a suspect, fugitive, material witness, or missing person. Absent a request, such information may not be disclosed. A request may be made orally or in writing and may include a general request seeking the public's assistance in identifying a suspect, fugitive, material witness, or missing person.

If a request is made by a Law Enforcement Official for a KEHP Member's PHI, the Personnel Cabinet Office of Legal Services shall be contacted immediately to authenticate the request for Disclosure and to determine whether the Official is authorized to make such a request. Upon determining if the request is valid, the Office of Legal Services shall direct the appropriate person(s) to provide the limited information set forth below.

The Disclosure of PHI pursuant to this section is limited to the following:

- i. Name and address;
- ii. Date and place of birth;
- iii. Social Security Number.

DEI may Disclose PHI to Law Enforcement Officials pursuant to an administrative request (including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized by Federal or State law), so long as (i) the information sought is relevant and material to a legitimate law enforcement inquiry; (ii) the request is specific and limited in scope to the extent reasonably practicable for the purpose; and (iii) the de-identified information cannot reasonably be used. DEI Personnel should consult with the Personnel Cabinet Office of Legal Services before making any Disclosures pursuant to this provision.

6) Uses or Disclosures to Avert Serious Threats to Health and Safety.

DEI may, consistent with applicable law and ethical standards, Use or Disclose PHI if DEI Personnel, in good faith, believe such Use and Disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and the Disclosure is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; or is necessary for Law Enforcement Officials to identify or apprehend an individual. The Personnel Cabinet Office of Legal Services should be consulted before any Disclosures of PHI are made pursuant to this Section.

7) Uses and Disclosures for Special Government Functions.

- a) DEI may Use and Disclose PHI of KEHP Members in the United States and foreign armed forces for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission. The

Personnel Cabinet Office of Legal Services should be consulted to confirm that the requirements of such Use or Disclosure are met.

- b) DEI may Disclose PHI to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act, and to protect the President of the United States and certain other public officials as authorized by law. The Personnel Cabinet Office of Legal Services should be consulted to confirm that the requirements of this Disclosure are met.
- c) DEI may Disclose to a Correctional Institution or Law Enforcement Official having lawful custody of an inmate or other individual, and the Correctional Institution or Law Enforcement Official may use PHI about such individual, if the Correctional Institution or such Law Enforcement Official represents that such PHI is necessary for: (i) the provision of Health Care to such individuals; (ii) the health and safety of such individual or other inmates; (iii) the health and safety of the officers or employees of or others at the Correctional Institution or other persons responsible for the transporting of inmates; (iv) the health and safety law enforcement on the premises of the Correctional Institution; and/or (v) the administration and maintenance of the safety, security, and good order of the Correctional Institution. The Personnel Cabinet Office of Legal Services should be consulted to confirm that the requirements of this disclosure are met.

8) Public Health.

DEI Staff may Disclose PHI without the written authorization of the KEHP Members to the appropriate state or federal health authority conducting public health surveillance, public health investigations, public health interventions, and the Food and Drug Administration regulatory oversight.

9) Miscellaneous.

DEI Staff may Disclose PHI for other miscellaneous required reasons pursuant to 45 CFR § 164.512(a) and 45 CFR § 164.103.

10) Disclosures to the Department of Health and Human Services:

The Department of HHS Office for Civil Rights (OCR) is given the authority to investigate HIPAA-related complaints and to ensure HIPAA compliance.

14. Business Associates

A “Business Associate” is a person or entity not employed by DEI that provides certain functions, activities, or services for or on behalf of DEI, that involve the Use and/or Disclosure of a KEHP Member’s PHI. Such activities may include, but are not limited to, billing; re-pricing; claims processing and administration; data analysis; legal, accounting, and actuarial services; consulting; utilization review; quality assurance; and similar services or functions. A Business Associate may be a Covered Entity. The definition of a Business Associate excludes a person who is part of the Covered Entity’s workforce. See 45 C.F.R. § 160.103.

DEI may disclose PHI to a Business Associate, and may allow a Business Associate to create or receive PHI on its behalf, if DEI has executed an agreement with the Business Associate which contains language requiring the Business Associate to appropriately safeguard the PHI.

If DEI knows of a pattern of activity or practice of a Business Associate that constitutes a material breach or violation of the Business Associate’s obligation under the Business Associate agreement, DEI must take reasonable steps to cure the breach or end the violation. If such steps are unsuccessful, the Business Associate agreement must be terminated or, if termination is not possible, the problem with the Business Associate must be reported to the Secretary of the Department of HHS.

DEI Counsel will be responsible for drafting and implementing the appropriate Business Associate language and/or agreements. All contracts must be reviewed in accordance with DEI policies. Questions regarding the status of a vendor or independent contractor should be forwarded to the Personnel Cabinet Office Legal Services.

15. Disclosures of PHI Pursuant to an Authorization

PHI may be disclosed for any purpose if an authorization that satisfies HIPAA requirements for a valid authorization is provided by the participant. All Uses and Disclosures made pursuant to a signed authorization must be consistent with the terms and conditions of the authorization.

DEI cannot Use or Disclose PHI for purposes **other** than Treatment, Payment, and Health Care Operations without a valid written authorization from the KEHP Member, except as otherwise permitted by these Policies and the HIPAA Privacy Regulations. When DEI obtains or receives a valid authorization for its Use or Disclosure of PHI, such Use or Disclosure must be consistent with the authorization.

An authorization is required to disclose information to third parties for purposes other than Payment or Health Care Operations except as otherwise permitted by the HIPAA Privacy Regulations.

DEI must obtain an authorization for any Use or Disclosure of PHI for marketing, except in certain circumstances.

Revocation of Authorizations

DEI must permit KEHP Members to revoke their authorizations, except to the extent that DEI has already taken action in reliance on the authorization.

- 1) A valid authorization must contain all of the elements required by the HIPAA Privacy Regulations and State law. See Authorization to Release forms. <http://personnel.ky.gov/dei/hipaa.htm>
- 2) Prior to Using or Disclosing PHI pursuant to an authorization, DEI Staff must review the authorization to determine if it is valid. An authorization is not valid if it contains any of the following defects:
 - a) the expiration date has passed or the expiration event is known to have occurred;
 - b) the authorization has not been filled out completely;
 - c) DEI Staff have knowledge that the authorization has been revoked;
 - d) DEI Staff have knowledge that some material information in the authorization is false; or
 - e) the authorization is missing one of the elements required by the HIPAA Privacy Regulations or State law.
- 3) DEI shall keep copies of authorizations in the KEHP Member file for at least six (6) years.

16. Complying with the “Minimum Necessary Standard”

DEI Staff must make reasonable efforts to limit the Use and Disclosure of and requests for PHI to the minimum necessary to accomplish the intended purpose of the Use, Disclosure, or request. The minimum necessary rule does not apply to:

- 1) Disclosures to or requests by a Health Care Provider for Treatment;
- 2) Uses or Disclosures made to the KEHP Member or his/her legal representative;
- 3) Uses or Disclosures made pursuant to an authorization;
- 4) Disclosures made to the Secretary of the Department of HHS for compliance and enforcement of the Privacy Regulations;
- 5) Uses and Disclosures Required by Law;
- 6) Uses and Disclosures required for compliance with HIPAA standardized transactions.

In DEI, all access to PHI is based off the employee’s role in organization and need for access to PHI in pursuit of administering the KEHP.

A. Disclosures.

- 1) Routine Disclosures: DEI, if necessary, will implement standard protocols, when appropriate, to limit the PHI Disclosed on a routine or recurring basis.

- 2) Non-Routine Disclosures: All non-routine Disclosures (those that do not occur on a day-to-day basis as part of Health Care Operation activities or which are required by law on a regular basis) must be reviewed by the Personnel Cabinet Office of Legal Services or the Privacy Official. When considering non-routine Disclosures, consideration should be given to the following criteria: (a) the purpose of the request; (b) any potential harm that would result to the KEHP Member, DEI, or any other third party as a result of the Disclosure; (c) the relevancy of the information requested; and (d) other applicable state and federal laws and regulations.

B. Requests.

- 1) Routine Requests: DEI has implemented standard protocols, when appropriate, to limit the PHI requested on a routine or recurring basis.
- 2) Non-Routine Requests: DEI has designated individuals who will be responsible for reviewing all non-routine requests (those that do not occur on a day-to-day basis as part of Health Care Operation activities). Any questions regarding the propriety of a particular request must be submitted to the Personnel Cabinet Office of Legal Services or the Privacy Official. When considering non-routine requests, the following criteria must be considered: (a) the reason for the request; (b) any potential harm that would result to the KEHP Member, DEI, or any other third party as a result of the request; (c) the relevancy of the information requested; and (d) other applicable state and federal laws and regulations.

17. Disclosures of De-Identified Information

DEI may freely Use and Disclose information that has been “De-identified” in accordance with the HIPAA Privacy Regulations. De-identified information is health information that does not identify an individual and from which there is no reasonable basis to believe that the information can be used to identify an individual.

A. De-Identified Information

DEI may Use and Disclose de-identified Health Information without regard to the Privacy Policies or HIPAA Privacy Regulations as long as the code or other means of identification designed to permit re-identification is not Disclosed.

DEI may Use Protected Health Information (PHI) to create information that is not Individually Identifiable Health Information or Disclose PHI to a Business Associate to de-identify Health Information. If de-identified information is re-identified, its Use and Disclosure becomes subject to regulation under the Privacy Policies and HIPAA Privacy Regulations.

Health Information can be de-identified by using one of the two methods listed below:

- 1) Safe Harbor. The following identifiers of the KEHP Member or of the relatives, employers, or household Members of the KEHP Member are removed:
 - a) Names;
 - b) Geographic subdivision, such as street address, city, county, and zip code;
 - c) The geographic unit formed by combining all zip codes with the same three initial digits if the unit 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);
 - d) All elements of dates (except year) for dates directly related to the KEHP Member, 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;
 - e) Telephone numbers;
 - f) Fax Numbers;
 - g) E-mail addresses;
 - h) Social Security Numbers;
 - i) Medical record numbers;
 - j) Health plan beneficiary numbers;
 - k) Account numbers;
 - l) Certificate/license numbers;
 - m) Vehicle identifiers, serial numbers, license plate numbers;
 - n) Device identifiers and serial numbers;
 - o) Web Universal Resource Locators (URLs);
 - p) Internet Protocol address numbers (IP);
 - q) Biometric identifiers, including fingerprints and voiceprints;
 - r) Full face photographic images and other comparable images;
 - s) All other unique identifying numbers, characteristics, or codes.

- 2) Alternative Method of De-Identification. A biostatistician or other person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable must apply such principles and methods and determine that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify the individual who is the subject of the information. The person making this determination must be an independent third party and must document the methods and results of the analysis that justify the determination.

B. Re-Identification

DEI may assign a code or other means of record identification to allow de-identified information to be re-identified, provided that:

- 1) Derivation. 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; and

- 2) Security. The code and/or mechanism for re-identification is not Used or Disclosed for any other purpose.

18. Breach Notification Requirements

The purpose of this policy is to provide for notification in the case of breaches of unsecured PHI. For purposes of these requirements, section 13402(h) of the Health Information Technology for Economic and Clinical Health (HITECH) Act defines “unsecured Protected Health Information” to mean PHI that is not secured through the use of approved technologies or methodologies.

To be approved, technologies and methodologies must render PHI unusable, unreadable, or indecipherable to unauthorized individuals. If PHI is rendered unusable, unreadable, or indecipherable to unauthorized individuals, then the PHI is not “unsecured” PHI.

This policy establishes the requirements as outlined by HITECH regarding the protection of PHI that DEI must comply with and the notification that must occur in the event of a breach. The breach notification provisions of section 13402 of HITECH apply to the HIPAA Covered Entities and their Business Associates that access, maintain, retain, modify, record, store, destroy, or otherwise hold, Use, or Disclose unsecured PHI.

A. Methods of Protection – Either of the following methods may be used to secure PHI and make it unusable, unreadable, or indecipherable to unauthorized individuals.

- 1) Encryption. DEI has implemented and maintains reasonable and appropriate encryption technologies and methodologies to enhance the protection of PHI.
- 2) Destruction. When required or necessary, DEI has implemented destruction techniques that render PHI unusable and/or unreadable in any format.

For additional information on the guidelines and standards of encryption and destruction methods, contact the Finance Cabinet, Commonwealth Office of Technology (COT).

B. Notification of Breach

- 1) If a breach of PHI is discovered, the HIPAA Privacy Official must be notified immediately. The Privacy Official will determine whether and when a notice to the individual, the media, and/or the Department for HHS is appropriate and, if so, the content of the notice.
- 2) In the event a breach of unsecured PHI, DEI is required to notify each individual whose unsecured PHI has been, or is reasonably believed to have been, inappropriately accessed, acquired, or disclosed, according to the requirements of HITECH:

- a) Written notice to the individual (or next of kin if the individual is deceased) at the last known address of the individual (or next of kin) by first-class mail (or by electronic mail if specified by the individual);
 - b) In the case in which there is insufficient or out-of-date contact information, substitute notice, including, in the case of ten (10) or more individuals for which there is insufficient contact information, conspicuous posting (for a period determined by the Secretary of HHS) on the home page of the web site of DEI or notice in major print or broadcast media;
 - c) In cases that DEI deems urgent based on the possibility of imminent misuse of the unsecured PHI, notice by telephone or other method is permitted in addition to the above methods.
- 3) Details of the notice shall include the following:
- a) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
 - b) A description of the types of unsecured PHI that were involved in the breach (such as full name, Social Security Number, date of birth, home address, account number, or disability code);
 - c) The steps individuals should take to protect themselves from potential harm resulting from the breach;
 - d) A brief description of what DEI is doing to investigate the breach, to mitigate losses, and to protect against any further breaches;
 - e) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, web site, or postal address.

C. Tracking

- 1) DEI must maintain a log of breaches of unsecure PHI and notify the HIPAA Privacy Official of each breach.
- 2) DEI, through the HIPAA Privacy Official, shall maintain a log of all reported breaches of unsecure PHI and shall submit required reports of such to the Secretary of HHS annually, as required by HITECH.

Please see Exhibit 1, Breach Notification Policy.

19. Accounting: Disclosure of PHI

An Individual has the right to obtain an accounting of certain Disclosures of his or her own PHI. This right to an accounting extends to Disclosures made in the last six (6) years, other than disclosures:

- 1) to carry out treatment, payment or health care operations;
- 2) to individuals about their own PHI;
- 3) incident to an otherwise permitted Use or Disclosure;

- 4) pursuant to an authorization;
- 5) to persons involved in the individual's care or payment for the individual's care or for certain other notification purposes;
- 6) to correctional institutions or law enforcement when the disclosure was permitted without authorization;
- 7) as part of a limited date set;
- 8) for specific national security or law enforcement purposes; or
- 9) Disclosures that occurred prior to the compliance date.

Examples of Disclosures subject to the accounting requirement include but are not limited to Disclosures for, or pursuant to: (1) Research, unless authorized by KEHP Member; (2) subpoenas, court orders, or discovery requests; (3) abuse and/or neglect reporting; (4) communicable disease reporting; or (5) other reports to the Department of Health such as tumor registry.

- 1) A KEHP Member must request an accounting of Disclosure in writing using the Request for Accounting Disclosure form. Verification of the requester's identity must be obtained prior to granting the request for an accounting. KEHP Members making their request for an accounting by telephone or e-mail should be forwarded a copy of the form.
- 2) When DEI receives a request for an accounting of Disclosures it should provide the KEHP Member with the appropriate form. DEI shall designate individuals who will be responsible for processing requests for accountings of Disclosures.
- 3) For each Disclosure that must be recorded, the accounting log must include the following information:
 - a) the date of the Disclosure;
 - b) the name of the entity or person who received the PHI and, if known, the address of such entity or person;
 - c) a brief description of the PHI disclosed; and
 - d) a brief statement of the purpose of the Disclosure that reasonably informs the KEHP Member of the basis for the Disclosure.
- 4) An Accounting of Disclosure log must be used to record Disclosures and must be maintained for a period of at least six (6) years from the date of the last accounting.
- 5) The Accounting Request Form and the log forwarded to the Privacy Official also should be maintained for six (6) years.
- 6) DEI will act on the KEHP Member's request for an accounting no later than sixty (60) calendar days after receipt of such a request. If DEI is unable to provide the accounting within 60 calendar days, it may extend the period by 30 days, provided that it gives the KEHP Member notice (including the reason for the delay and the date the information will be provided) within the original 60 calendar day period.

- 7) The first accounting to a KEHP Member in any 12-month period must be provided at no charge. DEI may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same KEHP Member within the 12-month period, provided that DEI informs the KEHP Member in advance of the fee and provides the KEHP Member with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.
- 8) A KEHP Member's right to receive an accounting of Disclosures may be suspended at the request of a Health Oversight Agency or Law Enforcement Official if certain conditions are satisfied. If DEI receives a request to suspend a KEHP Member's right to receive an accounting from a Health Oversight Agency or Law Enforcement Official, the Personnel Cabinet Office of Legal Services should be contacted to determine if the appropriate conditions have been satisfied.

20. Accounting: Request Amendments to PHI

DEI will permit KEHP Members to request amendments to their PHI contained in a Designated Record Set.

A Designated Record Set is a group of records maintained by or for DEI that includes the records about individuals or that is used, in whole or in part, by DEI Staff to make decisions about individuals, regardless of who originally created the information. A Designated Record Set does not include: (a) duplicate information maintained in other systems; (b) data collected and maintained for Research; (c) data collected and maintained for peer review purposes; (d) Psychotherapy Notes; (g) information compiled in reasonable anticipation of litigation or administrative action; (h) employment records; (i) education records covered by the Family Educational Rights and Privacy Act (FERPA); and (j) source data interpreted or summarized in the individual's medical record (example: pathology slide and diagnostic films). *See* 45 C.F.R. § 160.103.

DEI may deny a KEHP Member's request for amendment if it determines that the PHI or record that is the subject of the request:

- 1) Was not created by DEI Staff, unless the KEHP Member provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment;
- 2) Is not part of the Designated Record Set;
- 3) Is not available for inspection by the KEHP Member;
- 4) Is accurate and complete.

KEHP Members requesting an amendment to their PHI must provide a reason to support a requested amendment.

- 1) KEHP Members must request amendments to their PHI in writing by using DEI's Request for Amendment of Protected Health Information form. KEHP Members making their request for an amendment by telephone or e-mail should be sent a copy

of the form. Verification of the requester's identity must be obtained prior to considering the amendment. The request form must be maintained in the KEHP Member's record for a minimum of six (6) years.

- 2) When DEI receives a request for an amendment, it should provide the KEHP Member with the appropriate form.
- 3) DEI has designated individuals who will be responsible for processing a particular amendment request. The specific provider responsible for recording the PHI or originating the record must be consulted, if possible, and should sign the amendment form.
- 4) DEI must act on the KEHP Member's request no later than sixty (60) calendar days after receipt of a request, as set forth below:
 - a) Accepting the Amendment. If DEI accepts the requested amendment, in whole or in part, DEI must: (i) make the appropriate amendment by identifying the records in the Designated Record Set that are affected by the amendment and appending the amendment to such record; (ii) inform the KEHP Member, in writing, that the amendment is accepted by sending the KEHP Member a copy of the Request for Amendment of Protected Health Information with the acceptance noted; (iii) obtain the KEHP Member's identification of an agreement to have DEI notify the relevant persons with whom the amendment needs to be shared by using the form; and (iv) make reasonable efforts to inform and provide the amendment within a reasonable time to: persons identified by the KEHP Member as having received PHI about the KEHP Member and needing the amendment; and persons, as well as Business Associates, that have the PHI that is the subject of the amendment and who may have relied, or could foreseeably rely, on such information to the detriment of the KEHP Member.
 - b) Denying the Amendment. If DEI denies the requested amendment, in whole or in part, DEI must: (i) inform the KEHP Member, in writing, that the amendment is denied by sending the KEHP Member a copy of the Denial form; (ii) permit the KEHP Member to submit to the Covered Entity a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement; (iii) identify, as appropriate, the record or PHI in the Designated Record Set that is the subject of the disputed amendment and append or otherwise link the KEHP Member's request for an amendment; DEI's denial of the request; the KEHP Member's statement of disagreement, if any; and the DEI's rebuttal, if any, to the Designated Record Set.
- 5) If a statement of disagreement has been submitted by the KEHP Member, DEI must include the material set forth in subsection (iii) of the preceding paragraph.
- 6) If the KEHP Member has not submitted a written statement of disagreement, DEI must include the KEHP Member's request for amendment and its denial, or an accurate summary of such information, with any subsequent Disclosure of the PHI only if the KEHP Member has requested such action.

- 7) When DEI is informed by another Covered Entity of an amendment to a KEHP Member's PHI, DEI must amend the PHI in its Designated Record Sets.
- 8) Requests for amendments and documentation of the response to such requests must be maintained in a KEHP Member's record for a minimum of six (6) years.

21. Requests for Alternative Communication Means or Locations

DEI will permit KEHP Members to request, and will accommodate reasonable requests by KEHP Members, to receive communications of PHI by alternative means or at alternative locations.

DEI **cannot** require an explanation from the KEHP Member as to the basis for the request as a condition of considering or granting the request.

DEI can condition the provision of an alternative means of communication on: (a) information as to how payment will be handled, if applicable and (b) the specification of an alternative address or other method of contact.

- 1) A KEHP Member must request communication by alternative means or at alternative locations in writing by using the Request for Communication by Alternative Means form found at <http://personnel.ky.gov/dei/hipaa.htm>.
- 2) When DEI receives a request for communications by alternative means or at alternative locations, DEI will provide the KEHP Member with the appropriate form.
- 3) DEI has designated individuals who will be responsible for determining if a particular request for alternative means of communication is reasonable in light of the expense and administrative burden involved with complying with the request. Questions regarding the reasonableness of a particular request should be forwarded to the Privacy Official.
- 4) DEI must notify the KEHP Member in writing if the request is denied by providing the KEHP Member notice that includes the reason for the denial.
- 5) Requests for alternative means of communication and documentation of any denials of such requests should be maintained for a minimum of six (6) years.
- 6) DEI must ensure that agreed upon alternative means of communication are communicated to other departments and Business Associates who may be sending the KEHP Member communications on behalf of DEI.

- 7) If a request for communication by alternative means is granted, DEI must place or affix a clear indication of the communication by alternative means whether it be paper or electronic.

22. Requests for Restrictions on Use and Disclosure of PHI

DEI will permit KEHP Members to request restrictions on the Use and Disclosure of their PHI: (a) to carry out Treatment, Payment, or Health Care Operations and/or (b) to people involved as described in § 164.510(b) of the HIPAA Privacy Regulations. However, DEI is not required to agree to any request to restrict the Use and Disclosure of PHI, unless the Disclosure is to the KEHP's third-party administrator's Humana or Express Scripts or an authorized subcontractor for purposes of Payment or Health Care Operations.

If DEI agrees to a restriction, it may not Use or Disclose PHI in violation of the restriction, except in emergency situations. Any agreed-upon restriction will not be effective to prevent Uses and Disclosures to the KEHP Member or as Required by Law. DEI must adhere to any agreed-upon restriction until the restriction is terminated according to the procedures set forth below.

- 1) KEHP Member must request restrictions on the Use and Disclosure of their PHI in writing by using the Request for Restriction on Use and Disclosures of Protected Health Information form. KEHP Members making their restriction requests by telephone or e-mail should be sent a copy of the form. Verification of the requester's identity must be obtained prior to considering the request.
- 2) When DEI receives a restriction request, DEI should instruct the KEHP Member to complete the Request for Restriction form.
- 3) DEI has designated individuals who will be responsible for determining if a particular restriction will be permitted.
- 4) The Privacy Official should be contacted prior to agreeing to any restriction request.
- 5) DEI must notify the KEHP Member in writing if the request is denied by providing the KEHP Member with a copy of the completed Request for Restriction form that includes the reason for the denial.
- 6) Requests for restrictions and documentation of approvals or denials of such requests should be maintained for a minimum of six (6) years.
- 7) DEI must ensure that agreed-upon restrictions on the Use and Disclosure of PHI are communicated to other departments, and Business Associates who may be Using or Disclosing the KEHP Member's PHI on behalf of DEI.

- 8) A restriction on the Use and Disclosure of PHI that is not Required by Law can be terminated if (a) the KEHP Member requests the termination in writing; (b) the KEHP Member orally agrees to or requests the termination and the oral request or agreement is documented in the KEHP Member's medical record and communicated in writing to the Privacy Official; or (c) DEI informs the KEHP Member that it is terminating its agreement to the voluntary restriction, in which case the termination will apply only to PHI created or received after the KEHP Member has been notified of the termination.
- 9) If a restriction request is granted, DEI must place or affix a clear indication of the restriction, whether it be paper or electronic.

23. Documentation

The purpose of this policy is to establish proper documentation procedures for DEI.

DEI's Privacy Policies and Procedures shall be documented and maintained for at least six (6) years from the date last in effect. Policies and procedures must be changed as necessary or appropriate to comply with changes in the law, standards, requirements and implementation specifications (including changes and modifications in regulations). Any changes to policies or procedures must be promptly documented.

DEI shall document certain events and actions (including authorizations, requests for information, sanctions, and complaints) relating to an individual's privacy rights. The documentation of any policies and procedures, actions, activities and designations may be maintained in either written or electronic form. DEI will maintain such documentation for at least six (6) years.

Exhibit 1

Breach Notification Policy

This Reportable Breach Notification Policy is adopted by the Commonwealth of Kentucky, Personnel Cabinet, Department of Employee Insurance's Kentucky Employees' Health Plan ("the Plan") as part of the Plan's Privacy Policy and is intended to comply with the Interim Final Rule, Breach Notification for Unsecured Protected Health Information, issued by the Department of Health and Human Services (HHS) ("Breach Regulations"). It applies to breaches occurring on or after September 23, 2009.

I. Identifying a Reportable Breach

The first step is to determine whether a Reportable Breach has occurred. If a Reportable Breach has not occurred, the notice requirements do not apply.

The Privacy Official is responsible for reviewing the circumstances of possible breaches brought to his or her attention and determining whether a Reportable Breach has occurred in accordance with this Reportable Breach Notification Policy and the Breach Regulations.

- All Business Associates, and all workforce Members who have access to Protected Health Information (PHI), are required to report to the Privacy Official any incidents involving possible breaches.

There is a Reportable Breach only if all of the following have occurred, as determined by the Privacy Official and DEI, Commissioner's Office:

- There is a violation of the HIPAA Privacy Rules involving "unsecured" PHI.
- The violation involved unauthorized access, use, acquisition, or disclosure of unsecured PHI.
- The violation resulted in a significant risk of harm to the individual(s) whose unsecured PHI was involved.
- No exception applies.

The Privacy Official's determination of whether a Reportable Breach has occurred will include the following considerations:

- **Was there a violation of HIPAA Privacy Rules?** There must be an impermissible use or disclosure resulting from or in connection with a violation of the HIPAA Privacy Rules by the Plan or a Business Associate of the Plan. If not, then the notice requirements do not apply.
- **Was PHI involved?** If not, then the notice requirements do not apply.
- **Was the PHI secured?** (For electronic PHI to be "secured," it must have been encrypted to National Institute of Standards and Technology (NIST) standards or destroyed. For

paper PHI to be “secured,” it must have been destroyed.) If yes, then the notice requirements do not apply.

- **Unauthorized access, use, acquisition, or disclosure of PHI.** The violation of HIPAA Privacy Rules must have involved one of these. If it did not, then the notice requirements do not apply.
- **Significant Risk of Harm.** The violation must have resulted in significant risk of harm to the individual. If it did not, then the notice requirements do not apply. The harm may be financial, reputational, or other harm.

To determine whether a risk of harm is significant, the Privacy Official will perform a risk assessment that considers various factors, which may include some or all of the following:

- **Who impermissibly used or to whom was the PHI impermissibly disclosed?** For example, if the disclosure was to another HIPAA covered entity or to a federal agency or other entity subject to privacy rules similar to HIPAA Privacy Rules, then there is probably not a significant risk of harm to the individual.
- **Was the PHI returned or destroyed prior to being accessed?** For example, if the Plan obtains satisfactory assurance or a binding agreement from the recipient that the PHI will be destroyed or not further used or disclosed, there is probably not a significant risk of harm to the individual. Similarly, if the PHI in question was returned prior to it being accessed for improper purpose (e.g., return of a computer that was not hacked into), there is probably not a significant risk of harm to the individual.
- **What type and amount of PHI was involved in the impermissible use or disclosure?** Generally, the greater the amount of PHI and the greater the risk that the individual can be identified by disclosed PHI, the more likely its disclosure creates a significant risk of harm.

If the Privacy Official determines that there was not a significant risk of harm to the affected individual(s), the Plan will document the determination in writing and keep the documentation on file. If an exception applies, the notice requirements do not apply.

- **Exception 1:** The notice requirements do not apply if the breach involved an inadvertent unauthorized access, use, acquisition, or disclosure to an employee, volunteer, or other workforce Member or Business Associate and no further unauthorized access, use, acquisition, or disclosure occurred, if—(a) the unauthorized access, use, acquisition or disclosure was in good faith; and (b) the unauthorized access, use, acquisition, or disclosure was within the scope of authority of a workforce Member or Business Associate. (For example, the exception might apply to an inadvertent email to the wrong co-worker; but if an unauthorized employee looks up the PHI of his neighbor, the exception does not apply.)
- **Exception 2:** The notice requirements do not apply if the breach involved an inadvertent disclosure from one person authorized by the Plan to have access to PHI to another person authorized by the Plan to have access to PHI.
- **Exception 3:** The notice requirements do not apply if the breach involved a disclosure where there is a good faith belief that the unauthorized person to whom the disclosure

was made would not reasonably have been able to retain the PHI. (For example, an EOB mailed to wrong person and returned to the Plan unopened, or a report containing PHI is handed to the wrong person, but is immediately pulled back before the person can read it.)

II. If a Reportable Breach Has Occurred: Notice Timing and Responsibilities

If the Privacy Official determines that a Reportable Breach has occurred, the Privacy Official will determine (in accordance with the Breach Regulations) the date the breach was discovered in order to determine the time periods for giving notice of the Reportable Breach. The Plan has reasonable systems and procedures in place to discover the existence of possible breaches, and workforce Members are trained to notify the Privacy Official or other responsible person immediately so the Plan can act within the applicable time periods.

The Privacy Official is responsible for the content of notices and for the timely delivery of notices in accordance with the Breach Regulations. However, the Privacy Official may, on behalf of the Plan, engage a third party (including a Business Associate) to assist with preparation and delivery of individual notices. The Breach Regulations may require a breach to be treated as discovered on a date that is earlier than the date the Plan had actual knowledge of the breach. The Privacy Official will determine the date of discovery as the earlier of—(a) the date that a workforce Member (other than a workforce Member who committed the breach) knows of the events giving rise to the breach; and (b) the date that a workforce Member or agent of the Plan, such as a Business Associate (other than the person who committed the breach) would have known of the events giving rise to the breach by exercising reasonable diligence. Except as otherwise specified in the notice sections that follow, notices must be given “without unreasonable delay” and in no event later than 60 calendar days after the discovery date of the breach. Accordingly, the investigation of a possible breach, to determine whether it is a Reportable Breach and the individuals who are affected, must be undertaken in a timely manner that does not impede the notice deadline. There is an exception to the timing requirements if a law enforcement official asks the Plan to delay giving notices.

III. Business Associates

If a Business Associate commits or identifies a possible Reportable Breach relating to Plan participants, the Business Associate must give notice to the Plan. The Plan is responsible for giving notices of the Reportable Breach.

Unless otherwise required under the Breach Regulations, the discovery date for purposes of the Plan’s notice obligations is the date that the Plan receives notice from the Business Associate.

In its Business Associate contracts, the Plan will require Business Associates to:

- report incidents involving breaches or possible breaches to the Privacy Official in a timely manner;

- provide to the Plan any and all information requested by the Plan regarding the a breach or possible breach, including, but not limited to, the information required to be included in notices (as described below); and
- establish and maintain procedures and policies to comply with the Breach Regulations, including workforce training.

IV. Notice to Individuals

Notice to the affected individual(s) is always required in the event of a Reportable Breach. Notice will be given without unreasonable delay and in no event later than 60 calendar days after the date of discovery (as determined above).

1. Content of Notice to Individuals. Notices to individuals will be written in plain language and contain all of the following, in accordance with the Breach Regulations:

- A brief description of the incident.
- If known, the date of the Reportable Breach and the Discovery Date.
- A description of the PHI involved in the Reportable Breach (for example, full name, SSN, address, diagnosis, date of birth, account number, disability code, or other).
- The steps individuals should take to protect themselves (such as contacting credit card companies and credit monitoring services).
- A description of what the Plan is doing to investigate the Reportable Breach, such as filing a police report or reviewing security logs or tapes.
- A description of what the Plan is doing to mitigate harm to individuals.
- A description of what measures the Plan is taking to protect against further breaches (such as sanctions imposed on workforce Members involved in the Reportable Breach, encryption, and installation of new firewalls).
- Contact information for individuals to learn more about the Reportable Breach or ask other questions, which must include at least one of the following: toll-free phone number, email address, website, or postal address.

2. Types of Notice to Individuals. The Plan will deliver individual notices using the following methods, depending on the circumstances of the breach and the Plan's contact information for affected individuals.

- a. **Actual Notice.** Actual Notice will be given in all cases, unless the Plan has insufficient or out-of-date addresses for the affected individuals. Actual notice—
- will be sent via first-class mail to last known address of the individual(s);
 - may be sent via email instead, if the individual has agreed to receive electronic notices;
 - will be sent to the parent on behalf of a minor child; and
 - will be sent to the next-of-kin or personal representative of deceased person.

- b. **Substitute Notice.** Substitute Notice will be given if the Plan has insufficient or out-of-date addresses for the affected individuals.
- If addresses of fewer than ten living affected individuals are insufficient or out-of-date, substitute notice may be given by telephone, in person, or via email.
 - If addresses of ten or more living affected individuals are insufficient or out-of-date, substitute notice must be given via either website or media.
 - Substitute notice via website. Conspicuous posting on home page of the website of the Plan or Plan Sponsor for 90 days, including a toll-free number to obtain information about the Reportable Breach. Contents of the notice can be provided directly on website or via hyperlink.
 - Substitute notice via media. Conspicuous notice in major print or broadcast media in the geographic areas where the affected individuals likely reside, including a toll-free number to obtain information about the Reportable Breach. It may be necessary to give the substitute notice in both local media outlet(s) and statewide media outlet(s).
 - Substitute Notice is required only for living persons.
- c. **Urgent Notice.** Urgent Notice will be given, in addition to other required notice, in circumstances where imminent misuse of unsecured PHI may occur. Urgent notice must be given by telephone or other appropriate means.
- Example: Urgent notice is given to an individual by telephone. The Plan must also send an individual notice via first-class mail.

V. **Notice to HHS**

Notice of all Reportable Breaches will be given to HHS. The time and manner of the notice depends on the number of individuals affected. The Privacy Official is responsible for both types of notice to HHS.

- **Immediate Notice to HHS.** If the Reportable Breach involves 500 or more affected individuals, regardless of where the individuals reside, notice will be given to HHS without unreasonable delay, and in no event later than 60 calendar days after the Discovery Date (as determined above). Notice will be given in the manner directed on the HHS website.
- **Annual Report to HHS.** The Privacy Official will maintain a log of Reportable Breaches that involve fewer than 500 affected individuals, and will submit a report of to HHS every year by the last day in February (60 calendar days after January 1) of the Reportable Breaches that occurred in the preceding calendar year. The reports will be submitted as directed on the HHS website.

VI. Notice to Media (Press Release)

Notice to media (generally in the form of a press release) will be given if a Reportable Breach affects more than 500 individuals who are residents of any one state or jurisdiction. For example:

- If a Reportable Breach affects 600 individuals who are residents of Oregon, notice to media is required.
- If a Reportable Breach affects 450 individuals who are residents of Oregon and 60 individuals who are residents of Idaho, notice to media is not required. If notice to media is required, notice will be given to prominent media outlets serving the state or jurisdiction. For example:
- If a Reportable Breach involves residents of one city, the prominent media outlet would be the city's newspaper or TV station.
- If a Reportable Breach involves residents of various parts of the State, the prominent media outlet would be a statewide newspaper or TV station. If notice to media is required, it will be given without unreasonable delay, and in no event more than 60 calendar days after the Discovery Date (as determined above). The content requirements for a notice to media are the same as the requirements for a notice to individuals. The Privacy Official is responsible for giving notice to media.

Exhibit 2

Privacy Complaint Procedures

The purpose of this policy is to establish procedures for individuals to submit complaints alleging Privacy incidents regarding DEI's Privacy Policies and the alleged failure to comply with such Policies by DEI Staff and others.

1. Validate the complaint. If the complaint is received by mail, phone, fax or email attempt to determine and validate the facts and circumstances of the complaint and determine if complaint relates to Personnel Cabinet, Department of Employee Insurance or Kentucky Employees' Health Plan.
2. Make determination if complaint is an internal or external matter.
3. Alert HIPAA Privacy Officer of privacy complaint.
4. Once validated log the complaint by placing a copy of the file with the Privacy Officer. The HIPAA Privacy Officer informs the Commissioner's Office and the HIPAA Security Officer of initial facts and findings.
5. The HIPAA Privacy Officer or other staff shall investigate the complaint by reviewing the circumstances with the relevant staff and reviewing all material and resources that may have relevance to the complaint.
6. Finalize the complaint investigation.
7. Determine the nature of complaint and next action needed based on investigation.
8. Mitigate damages. Actions must be taken to mitigate all damages and develop a corrective action plan. The corrective action depends on the nature the issue and will be fact specific. The corrective action will typically involve, at a minimum, drafting a letter to affected member(s), determine that all damages have been mitigated, possibly sanctioning, and steps taken to prevent this types of issue in the future including a review of current policies and procedures. If a HIPAA breach is involved then Breach Procedures should be followed.
9. Document event by maintaining file with the HIPAA Privacy Officer