**2021 KALHD HIPAA PRIVACY RULE HANDBOOK**

**Kansas Association of Local Health Departments**



**ACKNOWLEDGEMENT**

The 2021 KALHD HIPAA Privacy Rule Handbook was produced under an arrangement between the Kansas Association of Local Health Departments and PYA, PC.

DISCLAIMER

**IMPORTANT DISCLAIMER REGARDING THE LAWS OF YOUR STATE**

Many state laws and regulations will continue to apply outside of the HIPAA Privacy Rule. This Manual does not include a review of state laws or regulations that may continue to apply outside of the HIPAA Privacy Rule. The form documents and agreements provided in this Manual for your review do **NOT** necessarily meet the requirements of your state’s laws that apply outside of the HIPAA Privacy Rule. This Manual is based upon regulations as of March 1, 2021 and does not consider currently proposed legislation.

**IMPORTANT DISCLAIMER REGARDING THE USE OF THIS HIPAA PRIVACY RULE MANUAL**

We acknowledge that PYA, P.C. did not, in any way, perform a management role, but instead, assisted KALHD by providing draft policies and procedures that comply with HIPAA Privacy Rule requirements.

The organization’s management is solely responsible for these policies and procedures and for establishing and ensuring implementation of each policy and procedure throughout the company. We acknowledge that management will be responsible for any updates, changes, or additions to the policies and procedures that may be needed in the future.

\* \* \* \* \* \* \* \* \* \*

**We have read this letter and understand all representations herein, or have obtained clarification from you, prior to being acknowledged and agreed on behalf of KALHD by:**

|  |  |
| --- | --- |
| By: |  |
|  | (Signature) |
| Name: | Dennis Kriesel |
|  | (Please Print) |
| Title: | Executive Director |
|  | (Please Print) |
| Date: | 4/29/2021 |

Introduction

The 2021 KALHD HIPAA Privacy Rule Handbook includes the following sample policies and procedures, updated to comply with the 2013 Omnibus HIPAA Final Rule and the Kansas Health Information Technology Act. The sample policies assume a Health Department is engaging in electronic health information exchange through an approved health information organization:

1. Notice of Privacy Practices
2. Uses and Disclosures of PHI
3. Personal Representatives for Purposes of Exercising HIPAA Privacy Rights
4. Requests for Restrictions on Uses and Disclosures of PHI
5. Requests for Alternative Means of Communication
6. Individual Requests for Access to PHI
7. Request for Amendment to PHI
8. Accounting of Disclosures of PHI
9. Breach Identification
10. Breach Notification
11. Business Associates
12. Workforce Training
13. Safeguarding PHI
14. Complaints and Grievance Process
15. Disclosure of PHI for Purposes of HIE
16. Access to PHI Through HIE
17. Responding to Inquiries Regarding HIE

**This handbook is provided for informational purposes only; the documents contained herein do not constitute legal advice.** As each health department’s operations are unique, your organization will need to develop policies tailored to its operations. Those policies should be reviewed and approved by qualified individuals and updated regularly based on changes to legal requirements and business operations.

Sample Policy and Procedure No. 1

Notice of Privacy Practices

Purpose:

The purpose of this policy is to ensure Department makes available its Notice of Privacy Practices to patients as required by the HIPAA Privacy Rule.

Policy Statement:

Department shall make available the current version of its Notice of Privacy Practices pursuant to the requirements of the HIPAA Privacy Rule [and the Kansas Health Information and Technology Act].

References to the Privacy Officer include his or her designee. References to an individual include his or her personal representative as authorized by law.

Procedure:

1. Department participates in [*Name of HIE*] (“[HIE Abbreviation] HIE Abbreviation”) under the terms of a written Participation Agreement (“Agreement”). Pursuant to the terms of the Agreement, Department is required to incorporate into its HIPAA Notice of Privacy Practices a notice regarding electronic health information (“HIE”) at least thirty (30) days prior to the date on which Department first participates in electronic health information exchange through [HIE Abbreviation][HIE Abbreviation]. ]

2. A copy of the current version of Department’s Notice of Privacy Practices (“the Notice”) effective [insert date] is attached as **Exhibit A**.

3. The Privacy Officer shall have overall responsibility for ensuring proper distribution of the Notice as required by the HIPAA Privacy Rule.

4. Department shall give copy of the current Notice and obtain a written acknowledgement of receipt of the Notice from each new patient. It is not necessary for the Department to give the current Notice to a patient from whom a written acknowledgement of receipt has been previously obtained even if the patient acknowledged receipt of a prior version of the Notice.

5. Each time a patient is seen at Department’s facility, the workforce member responsible for registering the patient shall review the patient’s record to determine whether the patient previously has provided a written acknowledgement of receipt of the Notice. If the patient has not provided such acknowledgement, the workforce member shall give the patient (or patient representative) a copy of the current Notice, and obtain the signature of the patient on the acknowledgement form, a copy of which is attached as **Exhibit B**. The workforce member then shall place the signed acknowledgement in the patient’s medical record. If the patient refuses to sign the acknowledgement, or the workforce member otherwise is unable to obtain an acknowledgement from the patient, the workforce member shall document in the record the good faith efforts to obtain the acknowledgement on the form attached hereto as **Exhibit C**.

6. If the process outlined in the preceding section cannot be completed prior to treating the patient due to an emergency situation, that process shall be completed as soon as possible.

7. The Privacy Officer shall ensure either (a) a full copy of the current Notice is posted in a clear and prominent location in the reception area, or (b) a summary of the Notice is posted in such location *and* a copy of the current Notice is maintained in Department’s facility in a notebook clearly labeled “Notice of Privacy Practices” available to any visitor to Department’s facility.

8. The Privacy Officer shall ensure that the current version of the Notice is posted on Department’s website available from a link appearing on the home page of such website.

9. Any member of Department’s workforce who receives an inquiry concerning the Notice shall direct such inquiry to the Privacy Officer. The Privacy Officer shall be responsible for handling all such inquiries. Upon request, the Privacy Officer shall provide a copy of the current Notice to any person who requests a copy of the document.

EXHIBIT A

NOTICE OF PRIVACY PRACTICES  
EFFECTIVE [insert date]

**THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN OBTAIN ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.** You have the right to a paper copy of this Notice; you may request a copy at any time.

Department is required by law to maintain the privacy of protected health information, to provide individuals with notice of its legal duties and privacy practices with respect to protected health information, and to notify affected individuals following a breach of unsecured protected health information.

Department provides health care to patients in partnership with physicians and other professionals and organizations. The information in this Notice of Privacy Practices will be followed by all the following entities, sites, and locations of Department:

* All individuals employed by Department
* All Department inpatient and outpatient departments
* Volunteers working at any Department facility
* Medical, nursing, and other students present at any Department facility
* Any health care professional who treats you at any Department facility
* [list out the physician offices and other “stand alone” offices/clinics]

**HOW DEPARTMENT MAY USE AND DISCLOSE HEALTH INFORMATION ABOUT YOU.**

Department may use and disclose your health information for the following purposes without your express consent or authorization.

***Treatment*.** We may use your health information to provide you with medical treatment. We may disclose information to doctors, nurses, technicians, medical students, or other personnel involved in your care. We also may disclose information to persons outside Department involved in your treatment, such as other health care providers, family members, and friends.

We may use and disclose health information to discuss with you treatment options or health-related benefits or services or to provide you with promotional gifts of nominal value. We may use and disclose your health information to remind you of upcoming appointments. Unless you direct us otherwise, we may leave messages on your telephone answering machine identifying Department and asking for you to return our call. We will not disclose any health information to any person other than you except to leave a message for you to return the call.

***Payment.*** We may use and disclose your health information as necessary to collect payment for services we provide to you. We also may provide information to other health care providers to assist them in obtaining payment for services they provide to you.

***Health Care Operations.*** We may use and disclose your health information for our internal operations. These uses and disclosures are necessary for our day-to-day operations and to make sure patients receive quality care. We may disclose health information about you to another health care provider or health plan with which you also have had a relationship for purposes of that provider’s or plan’s internal operations.

***Business Associates****.* Department provides some services through contracts or arrangements with business associates. We require our business associates to appropriately safeguard your information.

***Creation of de-identified health information*.** We may use your health information to create de-identified health information. This means that all data items that would help identify you are removed or modified.

***Uses and disclosures required by law.*** We will use and/or disclose your information when required by law to do so.

***Disclosures******for public health activities*.** We may disclose your health information to a government agency authorized (a) to collect data for the purpose of preventing or control disease, injury, or disability; or (b) to receive reports of child abuse or neglect. We also may disclose such information to a person who may have been exposed to a communicable disease if permitted by law.

***Disclosures about victims of abuse, neglect, or domestic violence*.** Department may disclose your health information to a government authority if we reasonably believe you are a victim of abuse, neglect, or domestic violence.

***Disclosures for judicial and administrative proceedings*.** Your protected health information may be disclosed in response to a court order or in response to a subpoena, discovery request, or other lawful process if certain legal requirements are satisfied.

***Disclosures for law enforcement purposes*.** We may disclose your health information to a law enforcement official as required by law or in compliance with a court order, court-ordered warrant, a subpoena, or summons issued by a judicial officer; a grand jury subpoena; or an administrative request related to a legitimate law enforcement inquiry.

***Disclosures regarding victims of a crime*.** In response to a law enforcement official’s request, we may disclose information about you with your approval. We may also disclose information in an emergency situation or if you are incapacitated if it appears you were the victim of a crime.

***Disclosures to avert a serious threat to health or safety***. We may disclose information to prevent or lessen a serious threat to the health and safety of a person or the public or as necessary for law enforcement authorities to identify or apprehend an individual.

***Disclosures for specialized government functions*.** We may disclose your protected health information as required to comply with governmental requirements for national security reasons or for protection of certain government personnel or foreign dignitaries.

***Disclosures for fundraising***. We may disclose demographic information and dates of service to an affiliated foundation or a business associate that may contact you to raise funds for Department. You have a right to opt out of receiving such fundraising communications.

**OTHER USES AND DISCLOSURES**

We will obtain your express written authorization before using or disclosing your information for any other purpose not described in this notice. For example, authorizations are required for use and disclosure of psychotherapy notes, certain types of marketing arrangements, and certain instances involving the sale of your information. You may revoke such authorization, in writing, at any time to the extent Department has not relied on it.

**YOUR RIGHTS REGARDING YOUR HEALTH INFORMATION.**

**Right to Inspect and Copy.** You have the right to inspect and copy health information maintained by Department. To do so, you must complete a specific form providing information needed to process your request (preferably utilizing Department’s standard authorization form for use and disclosure of PHI). If you request copies, we may charge a reasonable fee. We may deny you access in certain limited circumstances. If we deny access, you may request review of that decision by a third party, and we will comply with the outcome of the review.

**Right To Request Amendment.** If you believe your records contain inaccurate or incomplete information, you may ask us to amend the information. To request an amendment, you must complete a specific form providing information we need to process your request, including the reason that supports your request.

**Right to an Accounting of Disclosures Report.** You have the right to request a list of disclosures of your health information we have made, with certain exceptions defined by law. To request an accounting report, you must complete a specific written form providing information we need to process your request.

**Right to Request Restrictions.** You have the right to request a restriction on our uses and disclosures of your health information for treatment, payment, or health care operations. You must complete a specific written form providing information we need to process your request. Department’s Privacy Officer is the only person who has the authority to approve such a request. Department is not required to honor your request for restrictions, except if (a) the disclosure is for purposes of carrying out payment or health care operations and is not otherwise required by law, and (2) the protected health information pertains solely to a health care item or services for which you or any person (other than a health plan on your behalf) has paid Department in full.

**Right to Request Alternative Methods of Communication.** You have the right to request that we communicate with you in a certain way or at a certain location. You must complete a specific form providing information needed to process your request. Department’s Privacy Officer is the only person who has the authority to act on such a request. We will not ask you the reason for your request, and we will accommodate all reasonable requests.

**Rights Relating to Electronic Health Information Exchange.** Department participates in electronic health information exchange, or HIE. New technology allows a provider or a health plan to make a single request through a health information organization, or HIO, to obtain electronic records for a specific patient from other HIE participants for purposes of treatment, payment, or health care operations.

You have two options with respect to HIE. First, you can permit authorized individuals to access your electronic health information through an HIO. If you choose this option, you do not have to do anything. Second, you can restrict access to all of your electronic health information (except access by properly authorized individuals as needed to report specific information as required by law). If you wish to restrict access, you must complete and contact the appropriate HIE and/or submit a specific form available through the HIE website as indicated below:

[list contact information for each applicable HIE][[1]](#footnote-1)**.**

You cannot restrict access to certain information only; your choice is to permit or restrict access to all of your information.

If you have questions regarding HIE or HIOs, please visit [the](file:///\\pya_atl\shared\CAS%20SERVICE%20LINE%20FILES\Client%20Files\2021\5082%20Kansas%20Association%20of%20Local%20Health%20Departments\2021%20HIPAA%20Privacy%20Compliance\04%20Working\%20the) appropriate HIE website for additional information:

[list each applicable HIE website]

Your decision to restrict access through an HIO does not impact other disclosures of your health information. Providers and health plans may share your information directly through other means (e.g., facsimile or secure e-mail) without your specific written authorization.

If you receive health care services in a state other than Kansas, different rules may apply regarding restrictions on access to your electronic health information. Please communicate directly with your out-of-state health care provider about what action, if any, you need to take to restrict access.]

**COMPLAINTS**

If you believe your rights with respect to health information have been violated, you may file a complaint with Department or with the Secretary of the Department of Health and Human Services. To file a complaint with Department, please contact Privacy Officer, [insert contact information]. All complaints must be submitted in writing. **You will not be penalized for filing a complaint.**

Department reserves the right to change the terms of this Notice and to make the revised Notice effective with respect to all protected health information regardless of when the information was created.

**EXHIBIT B**

ACKNOWLEDGEMENT OF  
RECEIPT OF REVISED NOTICE OF PRIVACY PRACTICES

I acknowledge that I have received a copy of Department’s Notice of Privacy Practices effective [insert date].

Signature of Patient/Patient Representative Date

Relationship to Patient

**Original to be maintained in Patient’s permanent medical record.**

**EXHIBIT C**

DOCUMENTATION OF GOOD FAITH EFFORTS

Patient Name:

Date:

The patient presented to the facility on this date and was provided with a copy of Department’s Notice of Privacy Practices. A good faith effort was made to obtain from the patient (or the patient’s representative) a written acknowledgement of his/her receipt of the Notice. However, such acknowledgement was not obtained because:

* + Patient/patient representative refused to sign.
  + Patient/patient representative was unable to sign because:

□ Patient had a medical emergency, and an attempt to obtain the acknowledgement will be made at the next available opportunity.

□ Other reason (describe below):

Signature of Employee Completing Form:

**Original to be maintained in Patient’s permanent medical record.**

Sample Policy and Procedure No. 2

Uses and Disclosure of  
Protected Health Information

Purpose:

The purpose of this policy and procedure is to ensure members of Department’s workforce use and disclose protected health information (“PHI”) in compliance with the HIPAA Privacy Rule and related legal requirements.

Policy Statement:

No workforce member shall use or disclose an individual’s PHI (including individuals who have been deceased for less than fifty years) without obtaining a specific written authorization from an individual (or his or her personal representative) unless one of the exceptions specified herein applies. A workforce member who uses or discloses PHI in a manner not consistent with this policy and procedure shall be subject to disciplinary action, up to and including termination.

References to the Privacy Officer include his or her designee. References to an individual include his or her personal representative as authorized by law.

Reference:

Pursuant to the Kansas Health Information and Technology Act, any provision of Kansas law regarding the confidentiality, privacy, security, or privileged status of any protected health information (including any statute, regulation, Attorney General opinion, court decision, or agency interpretation) that conflicts with, is contrary to, or more stringent than the provisions of the HIPAA Privacy Rule regarding use and disclosure, safeguarding, and access to PHI have been preempted. This includes, but is not limited to, state laws imposing greater restrictions on disclosures of behavioral or mental health information.

Procedures:

1. **Privacy Officer.** Any workforce member with a question concerning whether an authorization must be obtained prior to using or disclosing PHI or relating to the completion of the authorization form shall request guidance from the Privacy Officer. The Privacy Officer shall respond to such inquiries in a timely manner and prepare and maintain appropriate documentation of such inquiries and responses. As necessary, the Privacy Officer shall consult with legal counsel in developing a response to such an inquiry.
2. **Related Policies and Procedures.**
   1. ***Individual’s Right of Access.*** The right of an individual (or his/her personal representative) to access PHI about the individual for purposes of inspection and copying is the subject of a separate policy and procedure entitled *Individual Requests for Access to Protected Health Information*, and the procedures set forth herein are not applicable to disclosures of PHI in connection with an individual’s (or personal representative’s) exercise of that right.
3. ***[Electronic Health Information Exchange.*** The disclosure of electronic PHI for purposes of electronic health information exchange is the subject of a separate policy and procedure entitled *Disclosure of Protected Health Information for Purposes of Electronic Health Information Exchange.* The use and disclosure of electronic PHI accessed through an approved health information organization is the subject of a separate policy and procedure entitled *Access to Protected Health Information Through Electronic Health Information Exchange.]*
4. **Required Authorization Form.**
   1. If it is necessary to obtain a signed authorization prior to using or disclosing PHI regarding an individual (*i.e.*, none of the exceptions listed in Section 5 apply to the specific use or disclosure), a workforce member shall not engage in such use or disclosure unless and until the individual has completed the authorization form attached as **Exhibit A** in its entirety with the appropriate level of specificity.
   2. A workforce member may rely upon an authorization form other than the one attached as **Exhibit A** only if the Privacy Officer has confirmed such alternative form satisfies all requirements of 45 CFR 164.508.
   3. A person may execute an authorization as an individual’s personal representative only if such person (a) is the parent or legal guardian of a minor who lacks legal authority to consent to his/her own medical treatment, (b) has been given authority by a court of proper jurisdiction to act on the individual’s behalf, including execution of an authorization for use and disclosure of PHI; or (c) has been formally appointed by the individual as his or her durable power of attorney and/or durable power of attorney for health care and the individual has an impairment that prevents him/her from making decisions on his/her own behalf. *See* policy and procedure entitled *Personal Representatives for Purposes of Exercising HIPAA Privacy Rights*. A workforce member with a specific question regarding an individual’s authority to execute an authorization form on behalf of another individual shall address the matter with the Privacy Officer.
   4. A written authorization for use or disclosure of PHI cannot be combined with any other document (*e.g.*, consent for treatment) to create a compound authorization, except an authorization for the use or disclosure of PHI for a research study may be combined with any other type of written permission for the same or another research study.
   5. A written authorization for use of disclosure of PHI may cover multiple types of PHI, multiple purposes for the use and/or disclosure, and/or identify multiple persons or entities to which the PHI may be disclosed. However, an authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for use or disclosure of psychotherapy notes.
   6. A workforce member who uses or discloses and individual’s PHI pursuant to a written authorization form shall ensure such completed form is placed in the individual’s medical record [or specify other location].
   7. A workforce member who obtains an individual’s signature on an authorization form shall provide a copy of the completed form to the individual.
5. **No Conditioning Upon Authorization.** Department shall not condition treatment for an individual on the provision of an authorization for use or disclosure of PHI, except as follows:
   1. Department may condition the provision of research-related treatment on authorization to use or disclose PHI for research purposes.
   2. Department may condition the provision of health care that is solely for the purpose of creating PHI for disclosure to a third party on provision of an authorization for the disclosure of such PHI to such third party (*e.g.*, pre-employment physical). Notwithstanding Section 3.E above, such an authorization must be limited in scope to that specific use or disclosure.
6. **Uses and Disclosures of PHI Without Authorization.**

Department shall not use PHI (*i.e.*, the sharing, employing, applying, utilizing, examining, or analyzing of PHI by or among members of Department’s workforce) or disclose PHI (*i.e.*, the releasing, transferring, providing access to, or divulging in any other manner of PHI to a third party (including a business associate)) without the individual’s or personal representative’s authorization **except** if the purpose of such use or disclosure is one of the following (subsections A – DD).

Certain disclosures of PHI without an authorization must be logged for purposes of providing an accounting of disclosures to an individual upon request. Those disclosures are identified in a separate policy and procedure entitled *Accounting of Disclosures of Protected Health Information.*

Except as noted otherwise, all uses and disclosures shall be limited to the minimum necessary information to accomplish the purpose of the use or disclosure.

1. ***Secretary of DHHS*.** Disclosures to the Secretary of the U.S. Department of Health and Human Services, or his/her designee, for purposes of determining Department’s compliance with the HIPAA Privacy Rule. The minimum necessary disclosure rule does not apply to these disclosures.
2. ***Treatment, Payment, and Health Care Operations*.**
3. Department may use or disclose PHI for the following purposes without an authorization. With respect to disclosures for treatment purposes, the minimum necessary rule does not apply.
   1. for the purpose of its own treatment, payment, and health care operations.
   2. for the purpose of treatment activities of another health care provider (regardless of whether that health care provider qualifies as a covered entity).
   3. for the purpose of payment activities of another covered entity or health care provider (regardless of whether that health care provider qualifies as a covered entity).
   4. for the purpose of certain health care operations of another covered entity that receives the PHI, subject to the following limitations:
      1. the health care operations for which such disclosures are permitted are limited to quality assessment and improvement activities; patient safety activities under the Patient Safety and Quality Improvement Act of 2005 (PSQIA); population-based activities relating to improving health or reducing health care costs, protocol development, case management, and care coordination; conducting training programs; accreditation, certification, licensing, or credentialing activities; health care fraud and abuse detection; and compliance programs.
      2. such disclosures are permitted only to the extent that each party has, or has had, a relationship with the individual who is the subject of the information being requested.
   5. for the purposes of communicating with an individual not currently present at Department’s facilities concerning that individual’s own care (*e.g.*, appointment reminders, prescriptions ready for pick-up), including communicating with individuals at their homes, through mail, by telephone (including voice mail), or electronic means such as email or text message. For any such communication, Department shall reasonably safeguard such communication and disclose only the minimum necessary information (*e.g.*, leaving only name, number, and any other necessary information on a voice mail to confirm an appointment).
4. ***Marketing*.**
5. Marketing Defined. “Marketing” is a communication about a product or service that encourages recipient to purchase or use the product or service. Marketing does not include:
   1. communications promoting health in general, which do not promote a product or service from a particular provider; or
   2. communications about government and government-sponsored programs, such as Medicare or Medicaid.
6. Marketing Exception. Department shall not use or disclose PHI for marketing purposes without an authorization EXCEPT if the purpose of the use or disclosure is:
7. Treatment of the individual, which includes (but is not limited to) case management or care coordination for the individual and directing or recommending alternative treatments, therapies, healthcare providers, or settings of care to the individual;
8. Case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment; and
9. To communicate to an individual information regarding a health-related product or service furnished by Department (including payment for such product or service). For example, Department may use its patient list to announce the arrival of a new specialty group (*e.g.*, orthopedic) or the acquisition of new equipment (*e.g.*, x-ray machine or magnetic resonance image machine) through a general mailing or publication.
10. Limitation on Marketing Exception. This marketing exception, however, does not apply (and thus an authorization is required) if Department receives direct or indirect payment from (or on behalf of) a third party whose product or service is being described.
11. “Direct or indirect payment” does not include (a) payment for treatment of an individual or (b) non-financial or in-kind benefits.
12. If Department receives direct or indirect payment, the authorization for use or disclosure must disclose that fact. Such authorization for subsidized marketing communications does not have to be specific to a single communication; it may cover all such communications for a specified time period, so long as the authorization properly discloses the purposes of such communications
13. Examples:
    * 1. An authorization would be required for Department to use or disclose PHI for purposes of communicating to patients its acquisition of new state of the art medical equipment if the equipment manufacturer paid the covered entity to send that communication. The limitation cannot be avoided by the parties characterizing the manufacturer’s payment as a “charitable donation” rather than funding for the mailings; the limitation extends to indirect payments.
      2. However, no authorization would be required in the same scenario if a local charitable organization, such as a breast cancer foundation, funded Department’s mailing to patients about new state of the art mammography screening equipment. In this case, the payment is being made by a party other than the party whose good or service is being marketed.
      3. No authorization would be required if Department sent flyers to its patients announcing the opening of a new wing where the funds for the new wing were donated by a third party, since the financial remuneration to the Department from the third party was not in exchange for the mailing of the flyers.
      4. if a third party provides financial remuneration to Department to implement a program, such as a disease management program, Department could provide individuals with communications about the program without obtaining individual authorization as long as the communications are about the covered entity’s program itself. There, the communications would only be encouraging individuals to participate in Department’s disease management program and would not be encouraging individuals to use or purchase the third party’s product or service.
      5. If a third party furnishes materials describing its product or service to Department and no payment was made by the entity relating to the mailing or distribution of the materials, Department may provide the material to individuals without first obtaining an authorization.
14. Exceptions to the “No Direct or Indirect Payment” Requirement. In three specific circumstances, Department may use or disclose PHI without an authorization even if it receives direct or indirect payment:
15. Face-to-face communication with the individual (*e.g.*, a health care provider, in a face-to-face conversation with an individual, verbally or by handing a written pamphlet to the individual, recommends that the individual take a specific alternative medication, even if the provider is otherwise paid by a third party to make such communications);
16. Distribution of a promotional gift of nominal value to the individual (*e.g.*, Department receives payment from manufacturer for distributing baby formula to new mothers); and
17. Sending to an individual refill reminders or other non-face-to-face communication about a drug or biologic that is currently being prescribed for the individual.
    * 1. However, the direct or indirect payment received from a third party limited to an amount reasonably related to Department’s cost for making such communication. The third party cannot make an incentive payment to encourage Department to make such communication.
      2. This exception includes communications relating to the generic equivalent of a drug being prescribed to an individual; adherence communications encouraging individuals to take their prescribed medications; and all aspects of a drug delivery system (including, for example, an insulin pump) for a self-administered drug or biologic that has been prescribed for an individual.
18. ***Family and Friends Involved In Patient Care or Payment*.** Disclosures to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, of PHI directly relevant to such person’s involvement with the individual’s care or payment related to the individual’s care, provided that:
    * + 1. if the individual is present for, or otherwise available prior to, such disclosure and has the capacity to make health care decisions, the individual agrees to such disclosure or does not object to the disclosure upon being provided an opportunity to do so, or one can reasonably infer from the circumstances that the individual does not object to the disclosure; or
        2. if the individual is not present for, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual’s incapacity or an emergency circumstance, Department may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the PHI that is directly relevant to the person’s involvement with the individual’s health care.

In the case of a deceased individual, Department may disclose PHI to family members and others who were involved in the care or payment for care of the decedent prior to death (in addition to the decedent’s personal representative), unless doing so would be inconsistent with any prior expressed preference of the individual that is known to Department.

1. ***Family and Caretakers for Notification Purposes*.** Uses and disclosures to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual’s location, general condition, or death (including disclosures to a public or private entity authorized by law or by its charter to assist in disaster relief efforts) provided that:
   1. if the individual is present for, or otherwise available prior to, such disclosure and has the capacity to make health care decisions, the individual agrees to such disclosure or does not object to the disclosure upon being provided an opportunity to do so, or one can reasonably infer from the circumstances that the individual does not object to the disclosure; or
   2. if the individual is not present or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual’s incapacity or an emergency circumstance, a workforce member may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the PHI that is directly relevant to the person’s involvement with the individual’s health care.

With respect to disclosures to disaster relief organizations, the requirements specified in D (1) and (2) apply only if a member of the workforce, in the exercise of professional judgment, determines those requirements do not interfere with the ability to respond to the emergency circumstances.

1. ***Business Associates*.** Department may disclose PHI to its business associate without authorization for the same purposes Department may use PHI without an authorization, but only if Department has entered into an appropriate written agreement with the business associate concerning use and disclosure of PHI. Such purpose must be specifically described in the written agreement, as well as the manner in which the business associate will use the PHI disclosed by Department. [The approved health information organization in which Department participates, [*specify Kansas Health Information Network or Lewis and Clark Information Exchange*] qualifies as Department’s business associate.]
2. ***Imminent and Serious Threat to Health or Safety*.** Uses and disclosures necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public if such disclosure is made to a person or persons reasonably able to prevent or lessen the treat, including the target of the threat.
3. ***Persons or Entities Under Jurisdiction of Food and Drug Administration*.** Disclosures made to a person under the jurisdiction of the Food and Drug Administration with respect to an FDA-regulated product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety, or effectiveness of such FDA-regulated product or activity. Such purposes include:
   1. to collect or report adverse events (or similar reports with respect to food or dietary supplements), product defects, or problems, or biological product deviations;
   2. to track FDA-regulated products;
   3. to enable product recalls, repairs, replacements, or lookbacks including locating and notifying individuals who have received products regarding product recalls, withdrawals, lookbacks, or other problems; or
   4. to conduct post-marketing surveillance.
4. ***Employers*.** Disclosures made to an employer about a person who is a member of the employer’s workforce if the following conditions are met:
   1. Department provides health care to the individual at the request of the employer, and the health care services are provided either to conduct an evaluation relating to medical surveillance of the workplace or to evaluate whether the individual has a work-related illness or injury;
   2. the disclosed PHI concerns workplace-related medical surveillance or a work-related illness or injury;
   3. the employer needs the PHI to comply with its obligations to carry out responsibilities for workplace medical surveillance or to record work-related illness or injury, as required by the Occupational Safety and Health Administration (OSHA) or the Mine Safety and Health Administration (MSHA); and
   4. Department gives written notice to the individual (either by giving a copy of the notice to the individual at the time the health care is provided, or, in situations where the health care is provided at the employer’s work site, by posting the notice in a prominent place at the location where the health care is provided) that PHI relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer.

Disclosures to an employer concerning an employee for purposes of the employer’s compliance with U.S. Department of Transportation regulations, the Family Medical Leave Act, and the Americans With Disabilities Act must be made pursuant to an authorization executed by the employee.

1. ***Kansas Statutes and Regulations***. Disclosures required by Kansas statute or regulation so long as such disclosures are made in compliance with the specific requirements of the specific statute or regulation and are limited to the relevant requirements of such law. Otherwise, the minimum necessary disclosure rule is not applicable to such disclosures.

Any such disclosure shall be made in writing to the appropriate state agency or designated individual (or made orally and followed up with a written notice).

The list of mandated reporting requirements under Kansas statutes and regulations may be found in **Exhibit B**.

1. ***Federal Statutes and Regulations*.** Disclosures to persons and entities other than the federal government required by federal statutes and regulations, including but not limited to the following. Such disclosure must comply with such law and be limited to the relevant requirements of such law.
2. disclosures to consumer reporting agencies pursuant to the Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq.;
3. disclosures to collective bargaining representatives pursuant to the National Labor Relations Act, 21 U.S.C. § 151 et seq.;
4. disclosures to employees, unions, and other persons or entities required by record-keeping and reporting requirements of the Occupational Safety and Health Administration (“OSHA”) regulations, including but not limited to 29 C.F.R. § 1904.
5. ***Federal Public Health Authorities*.** Disclosures to Federal public health authorities authorized by law to collect or receive PHI for the purpose of preventing or controlling disease, injury, or disability, including but not limited to disclosures to OSHA pursuant to that agency’s record-keeping and reporting requirements, including but not limited to 29 C.F.R . § 1904.
6. ***Health Oversight Agencies*.** Disclosures to a state or federal health oversight agency for oversight activities authorized by law (*i.e.*, regulation of health care providers), including audits, investigations, inspections, and administrative, civil, or criminal action. This does not include an investigation or other activity in which the individual whose PHI is to be disclosed is the subject of the investigation or other activity and such investigation or other activity is not directly related to:
7. the receipt of health care;
8. a claim for public benefits related to health; or
9. qualification for, or receipt of, public benefits or services when a patient’s health is integral to the claim for public benefits or services.
10. ***Adult Victims of Abuse, Neglect, or Domestic Violence*.** Disclosures about adult victims of abuse, neglect, or domestic violence made to a government authority authorized by law to receive such reports (other than those disclosures specifically required by Kansas statutes and regulations described above), but only if:
    1. the individual agrees to the disclosure, and such agreement is documented in the medical record; or
    2. the disclosure is expressly authorized by statute or regulation; and
11. Department believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or
12. if the individual is unable to agree because of incapacity, the official authorized to receive the report represents that the PHI is not intended to be used against the individual and that enforcement activities would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

If such a disclosure is made, Department must promptly inform the individual of the disclosure unless it is believed informing the individual would place him/her at risk of serious harm, or the disclosure would be made to a personal representative who is responsible for the abuse, neglect, or other injury and that informing such person would not be in the best interests of the individual. Such notification (or the reasons for not providing notification) shall be documented in the medical record.

1. ***Judicial and Administrative Proceedings*.**
2. Disclosure in response to a court order, but only that information specifically identified in the order; or
3. Disclosure in response to a subpoena issued by an attorney or a document request, but only if one of the following conditions are satisfied:
4. The requestor provides satisfactory assurances (*i.e.*, a written statement with supporting documentation) that the person who is the subject of the request has received written notice of the request and had an opportunity to object, and that the time for raising an objection has passed.
5. The requestor provides satisfactory assurances, *i.e.*, a written statement with supporting documentation, that the parties have agreed to a qualified protective order, or that the requestor has requested such an order from the appropriate court. A “qualified protective order” is a court order which prevents the parties from using or disclosing the information for any purposes other than the litigation and requires the return of the information to Department at the conclusion of the litigation or the destruction of the information.
6. If no such assurances are provided by the requestor, Department may release the information if it makes reasonable efforts to notify the subject of the request or obtains a qualified protective order from the appropriate court.
7. ***Cadaveric Organ, Eye, or Tissue Donation Purposes*.** Uses and disclosures relating to potential donors or recipients for purposes of arranging or coordinating cadaveric organ, eye, or tissue donations.
8. ***Law Enforcement Officials – Order, Warrant, Subpoena, Etc*.** Disclosures to law enforcement officials in compliance with and as limited by the relevant requirements of a court order, court-issued warrant, subpoena, or summons issued by a judicial officer, grand jury subpoena, or administrative request provided that:
9. such information is relevant and material to a legitimate law enforcement inquiry;
10. the request is specific and limited in scope; and
11. de-identified information could not reasonably be used.
12. ***Law Enforcement Officials – Response to Request*.**
13. To Identify/Locate Suspect, Fugitive, Witness, or Missing Person. Disclosures made in response to law enforcement requests for information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, subject to the following restrictions.
    * + 1. Only the following information may be disclosed without an authorization for this purpose: name and address; date and place of birth; social security number; ABO blood type and rh factor; type of injury; date and time of treatment; date and time of death, if applicable; and a description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.
        2. The following information may be disclosed for this purpose only with a proper authorization from the individual: information relating to an individual’s DNA or DNA analysis; dental records; or typing, samples, or analysis of body fluids or tissue (other than blood).
14. Information About Victim of Crime. Disclosures made in response to law enforcement requests for information about an individual who is suspected to be or is the victim of a crime if:
15. the individual consents to the disclosure (no written authorization is required); or
16. Department cannot obtain such consent because of the individual’s incapacity or other emergency circumstances, provided that:
17. the law enforcement official represents that the PHI to be disclosed is needed to determine whether a violation of law has occurred and the information will not be used against the individual;
18. the law enforcement official represents that immediate law enforcement activity depends on the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and
19. Department staff determines, in their professional judgment, that the disclosure is in the best interests of the individual.
20. ***Law Enforcement Officials – Participant In Violent Crime*.** Disclosures to law enforcement officials to identify or apprehend an individual because of a statement by an individual admitting participation in a violent crime that Department reasonably believes may have caused serious physical harm to the victim, unless Department learned the information in the course of treatment to affect the propensity to commit the criminal conduct that is the basis for the disclosure, or counseling or therapy, or through a request by the individual to initiate or to be referred to such treatment, counseling, or therapy.
21. ***Law Enforcement Officials – Escapee*.** Disclosures to law enforcement officials to identify or apprehend an individual where it appears from all the circumstance that the individual has escaped from a correctional institution or from lawful custody.
22. ***Law Enforcement Officials – Death Resulting From Violent Crime*.** Disclosures to law enforcement officials about a person who has died but only if Department has a suspicion that the death may have resulted from criminal conduct.
23. ***Law Enforcement Officials – Crime on Premises*.** Disclosures to law enforcement officials of information that Department in good faith believes constitutes evidence of criminal conduct that occurred on Department’s premises.
24. ***Law Enforcement Officials/Correctional Institutions – Persons In Custody*.** Disclosures to a correctional institution or a law enforcement official having lawful custody over an individual concerning that individual if the institution or official represents the information is necessary for:
25. the provision of health care to such individual;
26. the health and safety of such individual or other inmates;
27. the health and safety of persons responsible for transporting inmates;
28. law enforcement on the premises of the correctional institution; or
29. the administration and maintenance of the safety, security, and good order of the correctional institution.

Such disclosures are not permitted without authorization after the individual is no longer in lawful custody.

1. ***Decedents*.** Disclosures about decedents made to coroners, medical examiners, and funeral directors as necessary for these persons to carry out their duties.
2. ***Specialized Government Functions*.** Disclosures for specialized government functions including military and veterans activities, for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056 or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879.
3. ***Worker’s Compensation*.** Disclosures permitted under the Kansas Worker’s Compensation Act, K.S.A. § 44-501 *et seq*., specifically K.S.A. 44-515, as well as disclosures under the Federal Employee Compensation Act, 5 U.S.C. §§ 8101-8193, and its implementing regulations, 20 C.F.R. Parts 1- 25.
4. ***Certain Types of Research Activities*.** Disclosures for research purposes do not require an authorization if one of the following preconditions is satisfied:
5. Documented approval by an Institutional Review Board or a privacy board of an alteration to or waiver, in whole or in part, of the individual authorization required by the HIPAA Privacy Rule. Such approval must meet specific requirements set forth in the rule.
6. With respect to reviews preparatory to research, Department obtains from the researcher representations that:
   * + 1. use or disclosure is sought solely to review PHI as necessary to prepare a research protocol or for similar purposes preparatory to research;
       2. no PHI is to be removed from the researcher by the researcher in the course of the review; and
       3. the PHI for which use or access is sought is necessary for the research purposes.
7. With respect to research on decedent’s information (if deceased for less than fifty years), Department obtains from the researcher:
8. representation that the use or disclosure sought is solely for research on the PHI of decedents;
9. documentation, at the request of Department, of the death of such individuals; and
10. representation that the PHI for which the use or disclosure is sought is necessary for the research purposes.

The disclosure of PHI for all other types of research (including subject recruitment) requires an authorization. For example, because development or use of research databases falls within the definition of "research," Department may disclose PHI in a database to sponsors for subject recruitment only pursuant to an authorization or a waiver.

1. ***Limited Data Sets*.**
   * 1. Department may disclose a limited data set without an authorization if certain conditions are met for the purpose of research, public health, or health care operations. PHI contained in a limited data set would be stripped of any direct identifiers, but would maintain certain indirect identifiers, *i.e.*, admission, service, and discharge dates, date of death, age, and five-digit zip code.
     2. To disclosure a limited data set for the aforementioned purposes, Department must enter into a data use agreement with the recipient of the information. The agreement may take the form of a formal contract if the relationship is with a business associate, but a Department that wants to create and use a limited data set for its own research purposes, for example, could meet the standard by requiring members of its workforce to sign a confidentiality agreement. The agreement must meet detailed requirements including specifying permitted uses and disclosures, identifying who may use or receive the limited data set, and restricting further use and disclosure.
2. ***Schools*.** Department may disclose PHI to a school about a student or prospective student if (1) the PHI is limited to proof of immunization, (2) the school is required by State or other law to have such proof of immunization, and (3) Department obtains the agreement to disclosure from either a parent or guardian for an unemancipated minor or the individual if the individual is an emancipated minor. (Reporting immunization information to government agencies (including reporting made through electronic health information exchange) without an authorization is permitted under other exceptions detailed herein.)
3. ***Fundraising*.** Department may use or disclose to a business associate or related foundation the following PHI without an authorization for fundraising purposes: (1) demographic information relating to the individual; and (2) dates of health care provided to an individual. However, as a condition of such use or disclosure, Department must (1) provide notice of such use or disclosure in its Notice of Privacy Practices; (2) with each such fundraising communication, Department must provide the individual with a clear and conspicuous opportunity to elect not to receive any further fundraising communications in a manner that will not cause the individual to incur an undue burden or more than a nominal cost; (3) Department does not condition treatment or payment on the individual's choice with respect to the receipt of fundraising communications; and (4) Department does not send fundraising communications to an individual who has elected not to receive such communications.
4. **Drug and Alcohol Abuse Programs, 42 C.F.R. Part 2.**
   1. Notwithstanding the foregoing, PHI concerning the identity, diagnosis, prognosis, or treatment of a patient in a federally assisted drug and alcohol abuse program may not be disclosed unless:
      1. the patient authorizes the disclosure in writing, and the purpose for such disclosure is provided;
      2. the disclosure is allowed by court order; or
      3. the disclosure is made to medical personnel in a medical emergency or to qualified personnel for research, audit, or program evaluation.
   2. Any disclosure of such information (with or without authorization) shall be accompanied by the statement that the party to whom the disclosure is made is under the obligation not to re-disclose the information unless specifically permitted by law.
   3. To the extent such records contain the following information, they are not subject to the aforementioned protections:
      1. information about a crime committed by a patient either at the program or against any person who works for the program or about any threat to commit such a crime; or
      2. information about suspected child abuse or neglect, such records are not subject to the aforementioned protections.
   4. An authorization describing the records to be disclosed as “all records” does not include these types of records; such records must be separately identified, *e.g.*, “all records including drug and alcohol treatment program records.”
5. **Psychotherapy Notes.** Notwithstanding the foregoing, Department must obtain an authorization for any use or disclosure of psychotherapy notes, except:
   1. to carry out the following treatment, payment, and health care operations purposes:
      1. use by the originator of the notes for treatment;
      2. use or disclosure by Department for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; or
      3. use or disclosure by Department to defend itself in a legal action or other proceeding brought by the individual.
   2. use or disclosure for purposes of oversight of the originator of the notes.

An authorization for use or disclosure of psychotherapy notes cannot be combined with an authorization for use or disclosure of any other type of PHI. Thus, if one wants an individual’s authorization to use or disclosure psychotherapy notes and other PHI relating to the individual, one must obtain two separate authorization forms from the individual.

1. **Sale of PHI.** Notwithstanding the foregoing (*i.e.*, even if the disclosure of PHI would be permissible without an authorization), Department must obtain an authorization for any disclosure of PHI by Department when Department makes such disclosure in exchange for direct or indirect remuneration from or on behalf of the recipient of the PHI. Such authorization must state the disclosure will result in remuneration to Department. This requirement does not apply in the following specific circumstances:
   1. for public health purposes;
   2. for research purposes (*see* Section 5.AA), where the only remuneration received is a reasonable cost-based fee to cover the cost to prepare and transmit the PHI for such purposes;
   3. for treatment and payment purposes (*see* Section 5.AA);
   4. for the sale, transfer, merger, or consolidation of all or part of Department and related due diligence;
   5. to or by a business associate for activities the business associate undertakes on behalf of Department and the remuneration is provided by Department for the performance of such activities (*see* Section 5.F);
   6. to an individual when requested;
   7. as required by law; or
   8. where the only remuneration received by Department is a reasonable cost-based fee to cover the cost to prepare and transmit the PHI for one of the above purposes or a fee otherwise expressly permitted by law.

**EXHIBIT A**

**AUTHORIZATION FOR USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION**

|  |  |  |
| --- | --- | --- |
| **Patient’s Name** | **Birth Date** | **Address** |
| **CHECK ONE:**  **□** I hereby authorize DEPARTMENT to use PHI concerning the above-named person.  **□** I hereby authorize DEPARTMENT to disclose PHI concerning the above-named person to \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.  **□** I hereby authorize \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ to disclose PHI concerning the above-named person to DEPARTMENT. | | |
| **COMPLETE THE FOLLOWING:**  For treatment date(s): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  For the following purpose(s): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  ***If request is initiated by the individual completing the form, insert “at the request of individual”, otherwise, describe purpose of the use or disclosure.*** | | |
| **CHECK TYPE OF INFORMATION AUTHORIZED TO BE USED AND/OR DISCLOSED:** | | |
| **□** Demographic Information  **□** Progress Notes  **□** Test Results  **□** Billing Records | Other \_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | **□** Entire Record (will not include Billing Records or records not prepared by or on behalf of DEPARTMENT unless those items also are selected).  **□** Records not prepared by or on behalf of DEPARTMENT. DEPARTMENT cannot be responsible for the completeness or accuracy of such records. |
| This authorization shall remain in effect until \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (date) or \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (occurrence of specified event) at which time this authorization to disclose the identified health information expires, but no later than one year from the date listed below. If this item is left blank, the authorization shall remain effective for 60 days after the date listed below. | | |
| I understand that the records to be used or disclosed pursuant to this authorization may contain records relating to participation in any federally assisted drug and alcohol abuse program. I understand that such information is subject to special protections under federal law. By my initials, I authorize the use or disclosure of records containing such information if they are otherwise included within the scope of this authorization. \_\_\_\_\_\_\_\_\_\_ *(initial here)* | | |
| I understand that treatment is not conditioned upon the execution of this authorization. I understand that if the person or entity that receives the information is not a health care provider or health plan covered by federal privacy regulations, the information described above may be re-disclosed and no longer protected by those regulations. I understand that fees may be charged for preparing and sending copies of records, including a charge for labor and supplies of up to $\_\_\_\_\_\_\_\_ per request, a copying charge of up to $0.\_\_\_\_\_ for the first \_\_\_\_\_ pages and $0.\_\_\_\_\_ for additional pages, and the reasonable cost of all duplications of records that cannot be routinely duplicated on a standard photocopy machine. If this authorization is for the sale of my protected health information, I understand that this authorization will result in remuneration to DEPARTMENT. I understand that I may revoke this authorization at any time (except to the extent that action has been taken in reliance upon it) by mailing or hand-delivering written notification to the following person: **[*insert name of Privacy Officer, Address, City, State, Zip Code*]**. | | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  *Date* | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  *Patient’s Signature* | |
| *If the person giving this authorization is acting as the patient’s personal representative, complete the information below:* | | |
| *\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*  *Date* | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  *Personal Representative’s Signature* | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  *Printed Name of Representative* | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  *Representative’s Address and Telephone Number* | |
| **Relationship to Patient [check applicable box]**  **□** I am the parent or legal guardian of the minor patient who lacks legal authority to consent to his/her own medical treatment.  **□** I have been given authority by a court of proper jurisdiction to act on the patient’s behalf, including execution of this authorization.  **□** I have been formally appointed by the patient as his or her durable power of attorney and/or durable power of attorney for health care and the patient has an impairment that prevents him/her from making decisions on his/her own behalf. | | |

EXHIBIT B

MANDATORY REPORTING REQUIREMENTS UNDER KANSAS LAW[[2]](#footnote-2)

1. Vital Statistics. Reports to the Kansas Department of Health and Environment’s (“KDHE”) Division of Vital Statistics as required by the Kansas Uniform Vital Statistics Act. K.S.A. §§ 65-2401 – 2438 and K.A.R. §§ 28-17-1 – 28-17-21.

2. Infectious and Contagious Diseases. Reports to KDHE of incidents of certain diseases. K.S.A. §§ 65-118 – 65-119, 65-6015 – 65-6017 and K.A.R. §§ 28-1-2, 28-1-4, 28-1-18. (The current list of reportable diseases and the reporting form can be found on the KDHE’s website, http://www.kdheks.gov)

3. HIV and AIDS. Reports to KDHE concerning HIV testing, HIV status, and AIDS. K.S.A. § 65-6002

4. Blood Tests for Pregnant Women. Reports to KDHE, and to the submitting physician or person attending a pregnant woman, of all positive or reactive blood tests for the detection of syphilis and hepatitis b. K.S.A. § 65-153f.

5. Genetic Diseases. Reports to KDHE of genetic diseases detected as a result of mandatory newborn infant screening tests. K.S.A. § 65-183.

6. Child Abuse. Reports to the Kansas Department of Children and Families (or local law enforcement, if the report must be made at a time during which the Department is not open for business) relating to a child that an individual has reason to believe has been injured as a result of physical, mental, or emotional abuse or neglect or sexual abuse. K.S.A. § 38-2223.

7. Medical Care for Disabled Infant. Reports to the local social and rehabilitation services office concerning a disabled infant with a life-threatening condition for whom an individual reasonably believes medically indicated treatment is being withheld. K.A.R. §§ 30-45-11 and 30-45-12.

8. Abuse of Adults Residing in Certain Facilities. Reports to the Kansas Department of Children and Families or KDHE relating to a resident of a medical care facility, adult care home, state psychiatric Department, or state institution for the mentally retarded who a member of Participant’s workforce has reason to believe is being or has been abused, neglected, or exploited, or is in a condition which is the result of such abuse, neglect, or exploitation or is in need of protective services. K.S.A. §§ 39-1401 and 39-1402.

9. Abuse of Adults Not Residing in Certain Facilities. Reports to the Kansas Department of Children and Families concerning an adult alleged to be unable to protect his/her own interest who a member of Participant’s workforce has reason to believe is being harmed or threatened with harm through action or inaction by either another individual or through their own action or inaction is being or has been abused, neglected, or exploited or is in need of protective services. K.S.A. §§ 39-1430 and 39-1431.

10. Kansas Advocacy and Protective Services, Inc. Disclosures made in response to requests from the Kansas Advocacy and Protective Services, Inc., concerning persons with developmental disabilities or mental illness to whom the Participant has furnished care and treatment. K.S.A. § 74-5515.

11. Wounds. Reports to the city’s chief of police or the county’s sheriff of (1) any bullet wound, gunshot wound, powder burn, or other injury arising from or caused by the discharge of a firearm or (2) any wound which is likely to or may result in death and is apparently inflicted by a knife, ice pick, or other sharp or pointed instrument. K.S.A. § 21-6319.

12. Burns. Reports to the Kansas fire marshal of second-and third-degree burn wounds involving 20 percent or more of the victim's body and requiring Departmentization. K.A.R. § 22-5-6.

13. Trauma. Reports to the Kansas trauma registry maintained by KDHE. K.S.A. § 75-5666.

14. Infant Eye Disorders. Reports to the county or joint board of health of any swelling or redness in, or discharge from, the eyes of an infant less than six months old. K.S.A. § 65-153c.

15. Reportable Incidents Under the Kansas Risk Management Statute. Reports made by Participant or a member of Participant’s workforce directly involved in the delivery of health care services with knowledge that a health care provider has committed a “reportable incident,” *i.e.*, has engaged in an act that (1) is or may be below the applicable standard of care and has a reasonable probability of causing injury to a patient or (2) may be grounds for disciplinary action by the appropriate licensing agency. K.S.A. § 65-4923.

16. Reports to Kansas Board of Healing Arts. Reports to the Kansas Board of Healing Arts of information appearing to show that a person licensed to practice the healing arts has committed an act which may be ground for disciplinary action under K.S.A. § 65-2836.

17. Mental Health Technicians. Reports to the Kansas Board of Nursing of information appearing to show that a mental health technician has committed an act that may be ground for disciplinary action under K.S.A. § 65-4209. K.S.A. § 65-4216.

18. Overexposure to Radiation. Reports to KDHE by radiation licensees regarding excessive exposure to radiation. K.A.R. § 28-35-230a.

19. Insurers Providing PIP Benefits. Reports to a self-insurer or insurer providing personal injury protection benefits, upon request by the insurer concerning the treatment of an injured person claiming personal injury protection benefits. K.S.A. § 40-3114.

20. Visually Handicapped**.** Reports by Department to KDHE regarding sight handicapped and blind persons, unless the person is an adult and objects to the report. K.S.A. § 39-739.

21. Cancer Registry. Reports by Department to the cancer registry maintained by the KDHE. K.S.A. §§ 65-1,168 – 65-1,174 and K.A.R. § 28-70-2.

22. Fetal Alcohol Syndrome**.** Reports by Department to KDHE of congenital malformations in infants under one year of age and fetal alcohol syndrome. K.A.R § 28-1-4.

Sample Policy and Procedure No. 3

Personal Representatives for Purposes Of Exercising  
HIPAA Privacy Rights

Purpose:

The purpose of this policy is to ensure Department properly identifies an individual’s personal representative with the authority to exercise the individual’s HIPAA Privacy Rights.

Policy Statement:

An individual may act as a personal representative for another person with respect to the exercise of HIPAA Privacy Rights only if that individual has authority under Kansas law to consent to treatment on behalf of that person. Department shall not accept the authority of an individual to act on behalf of another individual unless and until Department confirms such authority. Such confirmation shall be appropriately documented in the patient’s records. An individual who serves as a personal representative for an individual may have access to the patient’s medical record in a manner consistent with the authority of the individual to act on behalf of the individual and the procedures outlined herein. Department should not release any records to a personal representative if the individual being represented has any unresolved concerns relating to the representative’s authority to represent him or her without first obtaining guidance from [risk manager/privacy officer/legal counsel].

Additionally, any workforce member with a question regarding whether an individual has such authority shall direct such matter to Department’s [risk manager/privacy officer/legal counsel].

Personal Representatives for Adults

The following individuals may exercise another person’s HIPAA Privacy Rights on his or her behalf:

1. An individual who has been given authority by a court of proper jurisdiction to act on a person’s behalf (*e.g*., legal guardian) unless the terms of such grant of authority are limited in such a way not to include exercise of HIPAA Privacy Rule rights. An individual who has been given power of attorney for a patient for purposes other than healthcare (*e.g.*, power of attorney to close on real estate) does not have any right to access the patient’s medical records, except with respect to deceased individuals (see discussion below).

If, however, Department reasonably believes that the individual, including an unemancipated minor, has been or may be subjected to domestic violence, abuse, or neglect by the personal representative, or that treating a person as an individual’s personal representative could endanger the individual, Department may choose not to treat that person as the individual’s personal representative if, in the exercise of professional judgment, doing so would not be in the best interests of the individual. Department shall direct such matter to Department’s [risk manager/privacy officer/legal counsel].

2. An individual who has been formally appointed by the person as his or her durable power of attorney and/or durable power of attorney for health care and the person has an impairment that prevents him or her from making decisions on his or her own behalf.

3. An individual who has been appointed as executor of a deceased person’s estate or a person who is otherwise legally authorized to act on behalf of the deceased individual or his/her estate, as a personal representative, and thus provide access to the deceased individual’s medical record in a manner consistent with the procedures outlined herein.

Personal Representatives for Minors

1. Under Kansas law, any person under age 18 is a minor unless (1) he/she is 16 or older and is or has been married; or (2) a court has conferred rights of majority upon the person pursuant to state statute.

2. There is a presumption that a minor’s parent/legal guardian must consent for examination and treatment for the minor. The law identifies specific circumstances in which the minor may consent for his/her own treatment. The same rules that determine who may provide consent for examination and treatment of a minor determine who may exercise the minor’s HIPAA Privacy Rule rights.

3. Either parent may exercise those rights on behalf of his/her minor child’s PHI.

A. The requesting parent does not have to be a joint or sole custodian of the child. However, if a person’s parental rights have been terminated by court order, or if the parent is not legally competent to consent for his/her own treatment, he/she cannot exercise those rights.

B. Unless court order to the contrary (*e.g*., divorce decree which awards sole custody and decision-making authority for a child to one parent), parents have equal decisional rights, and either may provide authorization without knowledge or consent of the other parent. If, however, Department knows the other parent objects to such exercise of rights, a workforce member shall make good-faith effort to resolve conflict prior to acting on one parent’s directive.

C. A parent who is a minor may authorize use or disclosure of his/her child’s PHI. That same minor, however, may be unable to exercise HIPAA Privacy Rule rights for himself or herself.

D. A stepparent may not exercise rights for his or her stepchild without authority granted by the parent. A workforce member should require written proof of such authorization.

4. Certain persons other than a minor’s parent may exercise rights on behalf of the minor in certain limited circumstances.

A. Parent has given written consent for another person to consent to examination and treatment of the parent’s minor child, and the written document is presented to Department. Examples include:

(1) Written consent given to friend, relative, or stepparent; or

(2) Signed and notarized written consent given to SRS when a child enters foster care from the child’s biological or adoptive parent(s). If Department staff has a question whether a foster parent can give consent in a particular situation, staff should contact the case manager, the SRS social worker, or the guardian ad litem assigned to the case. The foster parent should be able to provide contact information.

B. By court order presented to Department;

(1) The court itself may exercise such rights on behalf of the minor; or

(2) The court may grant custody or guardianship to another person, who then has the legal ability to consent to medical treatment for the minor (and thus exercise HIPAA Privacy Rule rights).

5. “Mature minor” exception.

The Kansas Supreme Court has recognized that in certain circumstances a minor should be permitted to consent to his/her own medical treatment, even if one of the aforementioned exceptions to the general rule requiring parental consent is not applicable.

A. The following factors are relevant to this determination: (a) age and maturity; (b) degree to which minor is dependent on his or her parents or others for support; (c) minor’s familial situation; and (d) degree of potential health hazards associated with the particular treatment provided.

B. Department should rely on “mature minor” exception to permit a minor to exercise HIPAA Privacy Rule rights only if confirmed in writing by a treating health care provider.

6. Other exceptions.

Kansas law also permits a minor to consent to certain types of treatment, *e.g*., pregnancy, venereal disease, mental health. To the extent a minor may consent to a certain type of treatment, the minor also may control the PHI relating to that treatment to the exclusion of any parent or other legal guardian.

7. Age of majority.

Upon reaching the age of majority and otherwise becoming emancipated, an individual gains control over his/her PHI, including PHI relating to examination and treatment provided while the individual was a minor. The parent, legal guardian, or other person who consented to such treatment may not access or otherwise exercise control over such PHI once the individual reaches the age of majority.

1. Required Documentation

All correspondence and associated documentation related to patient access, including denials, of a designated record set must be maintained for six years.

Sample Policy and Procedure No. 4

Requests For Restrictions On Uses and Disclosures  
of Protected Health Information  
For Which an Authorization Is Not Required

Purpose:

To ensure an individual the right to request restrictions on the use or disclosure of his/her protected health information (“PHI”) in those circumstances in which the PHI may be used or disclosed without authorization as required by the HIPAA Privacy Rule.

Policy:

An **i**ndividual shall have the right to request restrictions on Department’s use and disclosure of PHI in those circumstances in which Department may use or disclose such PHI without authorization. Requests for such restrictions must be made in writing to the Privacy Officer. Department has the right to deny any such request except as specifically provided herein. If Department agrees to a requested restriction, the restriction must be honored except in emergency situations.

References to the Privacy Officer include his or her designee. References to an individual include his or her personal representative as authorized by law.

Procedure:

Requests for Restrictions and Timely Action.

1. An individual shall have the right to request a restriction on Department’s use and disclosure of PHI in those circumstances in which an authorization is not specifically required for Department’s use or disclosure of such information (*e.g*., uses and disclosures for treatment, payment and health care operations (“TPO”); uses and disclosures for purposes other than TPO requiring an opportunity for the patient to agree or object). An explanation of such right shall be included in (Insert Entity Name)’s Notice of Privacy Practices.

2. An individual seeking such restriction shall submit a written request to the Privacy Officer. Such requests for restrictions must be submitted in writing, preferably on the form attached below as Exhibit A. If a patient makes such request to a (Insert Entity Name) employee, the employee shall ask the patient to complete the attached form. Department is not obligated to take action on oral requests for restrictions (except as necessary to accommodate an individual with a disability). Any workforce member receiving such a request from an individual shall direct the individual to the Privacy Officer.

3. The Privacy Officer shall be the only individual who may agree to any such restriction. The Privacy Officer shall review each request and determine whether it is feasible for Department to accept the request. Except as provided in Section 4, Department does not have any legal obligation to accept any such request.

4. Department shall agree to an individual’s request to restrict disclosure of PHI about the individual to a health plan if (a) the disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law; and (b) the PHI pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid Department in full. The Privacy Officer shall coordinate with Department’s business office to implement such requested restriction.

5. The Privacy Officer shall provide a written response to an individual requesting a restriction within 30 days of receipt of the request. If Department is unable to act on a request for restrictions in 30 days, the Privacy Officer shall provide the patient with a written statement outlining the reasons for the delay and the date by which a response will be provided.

[6. In those cases in which the Privacy Officer accepts such a request on behalf of Department (including restrictions on disclosures to health plans as described in Section 4), the written response from the Privacy Officer shall inform the individual that his/her e-PHI still shall be available through electronic health information exchange unless and until he/she also submits a request for restrictions to the Kansas Health Information Exchange, Inc., to restrict disclosures of his/her e-PHI through electronic health information exchange. In such circumstances, the Privacy Officer shall direct the individual to the appropriate HIE website for purposes of requesting such restriction:

[list each applicable HIE website][[3]](#footnote-3).

7. If the Privacy Officer agrees to a requested restriction on behalf of Department, the Privacy Officer shall be responsible for making appropriate notations in the relevant records and informing the appropriate persons of the restriction. All workforce members shall abide by any such restriction upon its acceptance. Any workforce member with a question or concern relating to a restriction shall contact the Privacy Officer for clarification.

8. Department shall maintain the individual’s request and the letter notifying the patient of the Privacy Officer’s decision on behalf of Department for a period of six (6) years.

9. In an emergency situation, information that is subject to a restriction may be disclosed to a treatment provider for emergency treatment. In disclosing such information, Department shall request that the provider not further use of disclose the information.

Terminating a Restriction.

1. Department may terminate its agreement to a restriction, if:

A. The individual agrees to or requests the termination in writing;

B. The individual orally agrees to the termination and the oral agreement is documented; or

C. Department informs the individual that it is terminating its agreement to a restriction, except that such termination is only effective with respect to PHI created or received after it has so informed the individual.

2. The Privacy Officer shall be the only person who may take action to terminate Department’s agreement to a restriction. Upon termination, the Privacy Officer shall be responsible for making appropriate notations in the relevant records and informing the appropriate persons of the termination.

3. Department shall maintain documentation of termination for a period of six (6) years following such termination.

EXHIBIT A

REQUESTS FOR RESTRICTIONS ON USES AND DISCLOSURES  
OF PROTECTED HEALTH INFORMATION

**PATIENT PLEASE NOTE: [ORGANIZATION NAME] IS NOT REQUIRED TO AGREE TO YOUR REQUEST. PLEASE SEE OUR NOTICE OF PRIVACY PRACTICES FOR MORE INFORMATION REGARDING SUCH REQUESTS.**

Patient Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date of Birth:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Patient Address:

Street

Apartment Number

City, State Zip

Type of PHI to be restricted or limited (please check all that apply):

Home phone number

Home address

Occupation

Name of employer

Visit notes

Hospital notes

Prescription information

Patient history

Office address

Office phone #

Spouse’s name

Spouse’s office phone #

Other \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

How would you like use (and/or disclosure of) your PHI restricted?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature of Patient or Legal Guardian Date

FOR INTERNAL PURPOSES ONLY:

Date Request Received: \_\_\_\_\_\_\_\_\_\_\_\_

Sample Policy and Procedure No. 5

Patient Request For Alternative Means of Communication

Purpose:

To ensure patients the right, pursuant to the Federal Standards for Privacy of Individually Identifiable Health Information, to request that their protected health information (PHI ) be communicated in a particular manner (*e.g.*, request that correspondence be directed to a particular address, telephone calls made to a certain number).

Policy:

Patients will be provided the opportunity to request that communications concerning their PHI be handled in a particular manner by (Insert Entity Name). (Insert Entity Name) shall comply with all reasonable requests for such restrictions.

Procedure:

Requests for Alternative Means of Communication and Timely Action

1. Patients shall have the right to request that communications concerning their PHI be handled in a particular manner by (Insert Entity Name). An explanation of such right shall be included in (Insert Entity Name)’s Notice of Privacy Practices.

2. Such requests should be submitted in writing, preferably on the form attached hereto as Exhibit A. If a patient makes such request to a (Insert Entity Name) employee, the employee shall ask the patient to complete the attached form. All such requests shall be forwarded to the Privacy Officer. (Insert Entity Name) employee shall not inquire concerning the reason for a patient’s request for alternative means of communication.

3. The Privacy Officer shall be the only individual who may agree to any request for alternative means of communication. The Privacy Officer shall review and accept any reasonable request. Reasonableness shall be determined by administrative considerations only.

4. The Privacy Officer must act on a request for alternative means of communication as soon as practicable. The Privacy Officer shall inform the patient of the decision concerning the request for alternative means of communication in writing. If the request is denied, such written communication must explain why (Insert Entity Name) cannot practically limit communications with the patient in the manner requested.

5. Upon approval of such request, the Privacy Officer shall be responsible for making appropriate notations in the relevant records and informing the appropriate persons of the restriction. All (Insert Entity Name) employees shall abide by any such restriction upon its acceptance. Any employee with a question or concern relating to a restriction shall contact the Privacy Officer for clarification.

6. The patient’s request and the letter notifying the patient of the Privacy Officer’s decision shall be maintained for a period of six years.

Changing or Terminating a Restriction

1. If a patient requests a change to or termination of an approved alternative means of communication, such request shall be handled in the same manner as an initial request for alternative means of communication.

2. The Privacy Officer shall be responsible for making appropriate notations in the relevant records and informing the appropriate persons of the change or termination.

3. Documentation of any change or termination shall be maintained by (Insert Entity Name) for a period of six years.

Exhibit A Sample Request for Alternative Means of Communication  
Protected Health Information

***Please complete the following information:***

1. Today’s Date
2. Patient Full Legal Name
3. Patient Birth Date
4. Name of Person Submitting Request (if other than Patient)

Relationship to Patient

1. Describe requested alternative means of communication

Signature of Patient/personal representative:

**FOR (Insert Entity Name) USE ONLY**

Action on request (circle one) Accepted Denied Date letter sent to Patient:

If request denied, reason for denial:

Signature of Privacy Officer:

Date:

Sample Policy and Procedure No. 6

Individual Requests for Access To  
Protected Health Information

Purpose:

To permit patients to inspect and/or obtain a copy of their protected health information (“PHI”) maintained by Department in a designated record set as required by the HIPAA Privacy Rule.

Definition:

“Designated record set” refers to paper and electronic files maintained by Department under an individual’s name. [*If Department has specifically defined what constitutes an individual’s designated record set for purposes of compliance with the HIPAA Privacy Rule, insert such definition here.*]

Policy:

Department shall provide an individual with access to his/her PHI maintained in a designated record set in the form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable hard copy form or such other form and format as agreed to by Department and the individual. Department may deny a request for access only in specified circumstances set forth herein.

References to the Privacy Officer include his or her designee. References to an individual include his or her personal representative as authorized by law.

Procedure:

Request for Access and Timely Action.

1. Any workforce member to whom a request is made by an individual (either orally or in writing) for access to the individual’s PHI (paper and/or electronic) shall direct the request to the Privacy Officer for appropriate action. The Privacy Officer shall be responsible for responding to individuals’ requests for access to their PHI and questions regarding the process for obtaining such access.

2. The Privacy Officer shall direct an individual to submit a written request for access (preferably utilizing Department’s standard authorization form for use and disclosure of PHI). For verification purposes, Department shall require requests for access to be submitted by an individual in writing (with appropriate accommodations for persons with disabilities).

3. Department shall provide an individual with access to his/her PHI maintained in a designated record set in the form and format requested by the individual (*i.e*., paper or electronic), if it can be readily produced in such form and format. Otherwise, Department shall produce PHI to the individual in a readable hard copy form or such other form and format as agreed to by Department and the individual. [*Revise as appropriate at such time patient portal becomes available*.] A summary format may be provided if the patient agrees to the format and the associated fees.

4. Department shall offer the individual a convenient time and place to inspect or obtain a copy of the requested records or, at the individual’s request, make arrangements to deliver the records to the individual by regular mail or encrypted e-mail. Department shall charge uniform, reasonable copying, labor, and supplies charges and actual postage fees. Department may condition the production of such copies on pre-payment of such charges. Department shall waive such charges for persons who qualify under Department’s financial assistance policy.

5. If an individual’s request for access directs Department to transmit the requested records directly to a person designated by the individual, Department shall provide copies to the designated person, provided such request has been made in writing, signed by the individual, and clearly identifies the designated person and where to send the copy of the records.

6. Notwithstanding the foregoing, if the PHI that is the subject of a request is maintained in one or more designated record sets electronically and if the individual requests an electronic copy of such information, Department shall provide the individual with access to the PHI in the electronic form and format requested by the individual, if it is readily producible in such form and format. Otherwise, such PHI shall be produced in a readable electronic form and format as agreed to by Department and the individual.

7. In response to an appropriate request, Department shall provide an individual with access to PHI regarding the individual made available by Department through electronic health information exchange (“HIE”), *e.g.,* a CCD (continuing care document). However, Department shall not provide access to PHI available to Department from third parties through HIE, except to the extent Department previously incorporated such PHI into Department’s designated record set for the individual. As appropriate, the Privacy Officer shall direct an individual seeking such third-party information to make a request for access to PHI to such third party.]

8. Except as outlined below, Department shall respond to a request within thirty (30) days of receipt. If Department is unable to respond within that time period, the Privacy Officer shall provide the individual with a written statement outlining the reasons for the delay and the date by which the request will be fulfilled.

9. If requested records have been destroyed in accordance with Department’s record retention policies, the Privacy Officer or designee shall provide the patient with a written statement advising that the request cannot be fulfilled.

Denial of Access.

1. Department may deny access in the following circumstances. These are unreviewable grounds for denial.

A. The information requested consists of psychotherapy notes or information compiled for use in civil, criminal or administrative actions.

B. If Department is acting under the direction of a correctional institution and the information could jeopardize the health, safety, security, custody or rehabilitation of the individual, any officer, employee, or other inmates.

C. In the course of research that includes treatment, provided the individual has agreed to the denial of access when consenting to participate. The right of access will be reinstated upon completion of the research.

D. If the information that is contained in the records is subject to the Privacy Act, 5 U.S.C. Section 522a, and the denial meets the requirements of that law.

E. Department does not maintain the information; however, if Department knows where the information is maintained, Department should inform the individual where to direct his or her request, if known.

2. Department may deny an individual access, provided that the individual is given a right to have such denials reviewed as described below, in the following circumstances:

A. A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;

B. The PHI makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or

C. The request for access is made by the individual’s personal representative, and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

3. Department shall, to the extent possible, provide any other PHI after excluding the information to which Department has a reviewable or unreviewable basis to deny access. The Privacy Officer shall inform the individual in writing if any portion of the individual’s request for access is denied. Such notice shall state whether the denial of access is reviewable or unreviewable and, if reviewable, the procedure to obtain such review.

4. An individual may request a review of a denied request for access only under circumstances outlined in 2.A-C. Department shall promptly refer the request for review to a licensed health care professional who is designated by Department to act as a reviewing official and who did not participate in the original decision to deny access. The reviewing official shall determine, in a reasonable period of time, whether to deny the access requested, and Department shall be bound by that determination. The Privacy Officer or designee shall promptly send a written notice to the individual outlining the outcome of the review.

Sample Policy and Procedure No. 7

Request For Amendment To  
Protected Health Information

Purpose:

To ensure individuals the right to request an amendment to protected health information (“PHI”) maintained in the designated record set as required by the HIPAA Privacy Rule.

Definition:

“Designated record set” refers to paper and electronic files maintained by Department under an individual’s name. [*If Department has specifically defined what constitutes an individual’s designated record set for purposes of compliance with the HIPAA Privacy Rule, insert such definition here.*]

Policy:

Individuals will be provided the right to request Department amend their PHI that is contained within the designated record set for as long as the information is maintained by Department.

Department may deny an individual’s request for amendment, if it determines that the PHI that is the subject of the request:

1. was not created by Department, unless the originator of the information is no longer available to act on the requested amendment;

2. is not part of the designated record set;

3. would not be available for access pursuant to the separate policy and procedure entitled *Individual Requests for Access to Protected Health Information*; or

4. is complete and accurate.

If Department denies the request for amendment, the Privacy Official must provide the individual with a written denial that states the reason for the denial.

References to the Privacy Officer herein include his or her designee. References to an individual include his or her personal representative as authorized by law.

Procedure:

Requests for Amendment and Timely Action.

1. Department shall permit an individual to request an amendment to PHI as contained in the designated record set. Department shall require requests for amendment to be presented in writing. The attached sample Request for Amendment form should be used. All such requests shall be forwarded to the Privacy Officer for appropriate action. Any individual with a question relating to the amendment process shall be referred to the Privacy Officer.

2. Department must act on a request to amend within 60 days of its receipt. If Department is unable to act on a request to amend the record in 60 days, the Privacy Officer must provide the individual with a written statement outlining the reasons for the delay and the date by which the request will be met.

Accepting the Amendment.

1. The Privacy Officer or designee shall make the appropriate amendment to the PHI by, at a minimum, identifying the records in the designated record set that are affected and appending or otherwise providing a link to the location of the amendment. In the case where the information is stored in another medium (*e.g*., microfilm, microfiche) a record of the link will be filed.

2. The Privacy Officer shall inform the individual in writing in a timely manner that the amendment has been accepted.

3. The Privacy Officer shall make reasonable efforts to inform and provide the amendment in a reasonable time to:

A. Persons identified by the individual as needing the amendment; and

B. Persons, including business associates, whom Department knows have the unamended information and who may have relied or foreseeably could rely on such information to the detriment of the individual. To the extent possible, the Privacy Officer shall communicate this information to an entity’s privacy officer.

4. Upon acceptance of the amendment, the Privacy Officer shall request from [*Kansas Health Information Network/Lewis & Clark Information Exchange*] (“[HIE Abbreviation][HIE Abbreviation]”) an audit log documenting each occasion on which the individual’s e-PHI has been accessed through [HIE Abbreviation] for purposes of HIE for the three-year period prior to the request. Based on the information made available through the audit log, the Privacy Officer shall identify those HIE participants who have accessed the individual’s PHI through HIE since the time the to-be amended information was included in the individual’s designated record set by Department. The Privacy Officer shall communicate with each such participant via DIRECT or other secure messaging information regarding the amendment to the individual’s PHI.]

5. The Privacy Officer or designee shall communicate to the appropriate person(s) in the billing office amendments regarding payments made on behalf of the individual for review of potential billing issues.

Denying the Amendment.

1. If Department denies the request, a timely, written denial to the individual shall be provided by Privacy Officer utilizing the attached Denial Letter.

2. Statement of Disagreement.

A. If the individual submits a statement of disagreement, the Privacy Officer may provide a response statement to the individual based on the particular circumstances.

B. Department shall append or link the individual’s request for amendment, the denial, the statement of disagreement, and the written rebuttal to the specified designated record set.

C. Any future disclosures shall include both the request for amendment and its denial and the statement of disagreement.

Accepting Forwarded Amendments.

If Department is informed by another entity of an amendment, Department shall accept the amendment into its designated record set. The Privacy Officer shall be responsible for making the appropriate change to the record set.

Required Documentation.

1. Department shall document and retain the following:

A. The designated record sets that are subject to amendment by individuals.

B. The titles of the persons or offices responsible for receiving and processing requests for amendment by individuals.

2. All correspondence and associated documentation related to amendment of the designated record set must be retained for six years.

Exhibit A

Sample Request For Amendment of  
Protected Health Information

**(Insert Entity Name)**

***Please complete the following information:***

1. Today’s Date

2. Patient Full Legal Name

3.

4. Patient Birth Date

5. Name of Person Submitting Request (if other than Patient)

Relationship to Patient

6. Describe type(s) of information to be amended

7. Date(s) of information to be amended (*e.g.*, date of payment, office visit, treatment, or other services)

8. What is your reason for making this request?

9. How is the entry incorrect or incomplete?

10. **Please attach written amendment.**

11. Do you know of anyone who may have received or relied on the information in question (such as your doctor or health plan)? (circle one) Yes No

If yes, please specify the name(s) and address(es) of the organization(s) or individual(s).

12. If amendment is accepted, do we have your permission to share the amendment with individuals who have received this information? (circle one) Yes No

Signature of patient/personal representative:

**FOR (Insert Entity Name) USE ONLY**

Amendment has been: Accepted Denied

Signature of Privacy Officer:

Date:

* + Patient has not filed a Statement of Disagreement, but requests that any future releases include the requested amendment and denial information.
  + Patient has filed a Statement of Disagreement that **must** be released along with other documentation with any future releases of information.
  + (Insert Entity Name) appended written response to Statement of Disagreement and forwarded to patient.
  + (Insert Entity Name) did not provide a response/rebuttal

Sample Policy and Procedure No. 8

Accounting of Disclosures of  
Protected Health Information

Purpose:

To permit individuals to obtain an accounting of certain disclosures of protected health information (“PHI”) by Department.

Policy:

Department shall properly record disclosures of PHI and provide an accounting of such disclosures upon proper request by an individual.

References to the Privacy Officer include his or her designee. References to an individual include his or her personal representative as authorized by law.

Procedure:

Recordation of Disclosures.

1. Department shall maintain systems to generate a written record of each and every disclosure of PHI that falls into one of the following categories:

A. Disclosures not in compliance with Department policies implementing HIPAA Privacy Rule requirements.

B. For public health activities (unless such disclosure is required by law and excepting reports of child abuse or neglect).

C. For judicial or administrative proceedings.

D. For law enforcement purposes.

E. To avert a serious threat to health or safety (unless such disclosure is required by law).

F. For military and veterans’ activities, the Department of State’s medical suitability determinations, and government programs providing public benefits (unless such disclosure is required by law).

G. For workers’ compensation (unless such disclosure is required by law).

For clarification regarding these categories, see separate policy and procedure entitled *Uses and Disclosures of Protected Health Information*.

2. Such written record shall include the following information regarding the disclosure:

A. The date of the disclosure, if known; or if not, the approximate date (month and year) during which the disclosure occurred.

B. The name of the entity or natural person who received the PHI and, if known, such entity’s or person’s address.

C. A brief description of the PHI disclosed.

D. A brief description of the purpose for the disclosure that demonstrates the basis for the disclosure

3. The workforce member responsible for authorizing a particular disclosure also shall be responsible for ensuring the disclosure is appropriately recorded. Recordation of disclosures shall be made immediately upon disclosure, but in no event shall such recordation be made more than five business days following the disclosure.

Request for Accounting of Disclosures

1. Any workforce member who receives a request from an individual for an accounting of disclosures shall direct such individual to the Privacy Officer. The Privacy Officer shall direct such individual to complete a written request for an accounting of disclosure. Department shall not take action on any oral request for an accounting of disclosures. Department shall provide an individual with the option of limiting the requested accounting of disclosures to a specific time period, type of disclosure, or recipient.

2. Within thirty (30) days of receipt of a written request for an accounting of disclosures, the Privacy Officer shall provide the individual with the requested accounting. If the request cannot be fulfilled within thirty (30) days, the Privacy Officer shall provide the individual with a written statement of the reasons for the delay and the date by which the Department will provide the accounting, not to exceed sixty (60) days from the receipt of the written request.

3. Notwithstanding the foregoing, if Department is informed in writing by a law enforcement official that providing an accounting of disclosures to the law enforcement official would be reasonably likely to impede the law enforcement agency’s activities and specifies the time for which a delay is required, Department shall delay providing an accounting of disclosures to law enforcement for the specified time period. If such request is made orally, Department shall document the request (including the identity of the official making the request) and shall delay providing the individual with an accounting of disclosures to law enforcement for up to thirty days, unless a written statement is received from the law enforcement during that time period.

4. To the fullest extent possible, Department shall provide the accounting in such form and format as requested by the individual. Otherwise, Department shall provide the accounting in a readable hard copy form or such other form and format as agreed by Department and the requesting individual.

5. Department shall provide the first accounting to an individual in any twelve (12)- month period without charge. Upon producing such accounting, Department shall inform the individual that there will be a fee for each subsequent request for an accounting within the twelve (12)-month period. For subsequent requests by the same individual within the twelve (12)-month period, Department shall impose a reasonable, cost-based fee, provided Department (a) informs the individual of the fee at the time the request for accounting is made, and (b) affords the individual the opportunity to withdraw or modify the request to avoid or reduce the fee.

6. The Privacy Officer shall be responsible for maintaining a copy of the written accounting of disclosures provided to any individual, as well as the titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.

Sample Policy and Procedure No. 9

Breach Identification

Purpose:

The purpose of this policy is to ensure Department identifies those unauthorized uses or disclosures of protected health information (“PHI”) which constitute a breach of unsecured PHI (“UPHI”) for which Department must provide notice in compliance with the HIPAA Privacy Rule.

Policy:

Any member of Department’s workforce (including directors, officers, employees, independent contractors, volunteers, and trainees) who becomes aware of any possible unauthorized use or disclosure of PHI shall report such matter to the Privacy Officer immediately. Any form of retaliation against a person who in good faith makes such a report is strictly prohibited.

The Privacy Officer shall be responsible for investigating any such report received from any person or entity. The [specify responsible committee, *e.g*., Corporate Compliance Committee, Risk Management Committee] (“Committee”) (or, in certain circumstances, the Privacy Officer) shall determine whether such use or disclosure constitutes a breach of unsecured PHI for which Department must provide notice pursuant to the separate policy and procedure entitled “Breach Notification.” The Privacy Officer shall be responsible for properly documenting such investigation and determination.

References to the Privacy Officer in the following procedures include his/her designee(s).

Procedure:

Report to Privacy Officer.

## 1. ***Duty to Report – Workforce Member.*** Any workforce member who becomes aware through any means of any possible unauthorized use or disclosure of PHI (including, but not limited to, reports or complaints received from business associates, patients, patients’ family members and other advocates, other workforce members, and personal observation) shall report such matter to the Privacy Officer immediately (a “Report”). Any workforce member who fails to make a timely Report shall be subject to disciplinary action, up to and including termination of his/her employment or other relationship with Department.

## 2. ***Reporting Mechanisms.*** A workforce member shall make a Report by either (1) contacting Department’s Privacy Officer in person, by telephone, or by e-mail; or (2) utilizing one of the anonymous reporting mechanisms specified in Department’s Corporate Compliance Program.

## 3. ***Prohibition on Retaliation.*** Department shall not tolerate retaliation of any type against any workforce member or agent who, in good faith, makes a Report. Any person who engages in retaliation shall be subject to disciplinary action, up to and including termination of his/her employment or other relationship with Department. The Privacy Officer and any person involved in any subsequent investigation, discussion, or decision-making shall maintain the confidentiality of the person making the Report to the fullest extent possible.

## 4. ***Training.*** Required HIPAA training for workforce members shall include, among other things, the following topics: identification of unauthorized uses and disclosures of PHI; the obligation to make Reports; the mechanisms available for making Reports; and the consequences for failing to make a Report.

## 5. ***Confidentiality Agreement.*** The written confidentiality agreement all workforce members are required to sign shall include, among other things, an agreement to make Reports, to cooperate with any investigation relating to a Report, and not to retaliate in any way against any person who makes or participates in the investigation or resolution of a Report.

## 6. ***Notice of Privacy Practices.*** Department’s Notice of Privacy Practices shall direct any person who has concerns regarding any possible unauthorized use or disclosure of PHI and/or any breach notification made by Department to communicate with the Privacy Officer using the contact information listed in the Notice.

Investigation and Investigation Form.

## 1. ***Investigation of Reports.*** The Privacy Officer shall assign a control number to and investigate each Report to gather such information necessary to determine whether the incident constitutes a breach of unsecured PHI. The Privacy Officer shall involve other persons in such investigations as he/she deems appropriate (*e.g*., the Security Officer or senior IT staff member for Reports involving electronic PHI). The Privacy Officer shall document each Report and subsequent investigation using the Investigation Form attached as **Exhibit A**.

## 2. ***Business Associate.*** If the Privacy Officer receives a report from a business associate, the Privacy Officer shall communicate with the business associate as soon as possible to obtain any information necessary to complete the Investigation Form that is not included in the report received from the business associate.

## 3. ***Date of Discovery.*** As part of the investigation, the Privacy Officer shall determine when the use or disclosure which is the subject of the Report was discovered, *i.e*., the first date on which a workforce member or agent (other than the person making such use or disclosure) knew, or by exercising reasonable diligence would have known, of such use or disclosure.

## 4. ***Cooperation.*** Any workforce member asked to provide information in connection with the investigation shall cooperate fully in locating and providing requested information.

## 5. ***Completion of Investigation Form.*** The Privacy Officer shall complete the Investigation Form as soon as possible, but no more than fifteen (15) business days following receipt of the Report (except in extraordinary circumstances). If additional information concerning a Report becomes available following completion of the Investigation Form, the Privacy Officer shall prepare a supplemental entry on the Investigation Form incorporating such additional information. The Investigation Form shall be maintained as a confidential document.

## 6. ***Accounting of Disclosures.*** If, following investigation, the Privacy Officer determines there has been an unauthorized disclosure of PHI (regardless of whether such disclosure is identified as a breach), the Privacy Officer shall record that disclosure pursuant to the policy entitled, “Accounting of Disclosures of Protected Health Information.”

**Committee Review.** Except in those cases requiring expedited review, the Committee shall determine whether a Report constitutes a breach of unsecured PHI for which notification must be provided (a “Breach”). The Committee will be composed of the following roles: [List the committee members]. Committee members shall participate in ongoing educational opportunities concerning the requirements and application of the HIPAA Privacy and Security Rules and related state privacy and notification laws.

## 1. ***Breach Determinations.***

### A. At each Committee meeting, the Privacy Officer shall provide a summary of each pending Report and related investigation and, if necessary and appropriate, distribute copies of the completed Investigation Form to Committee members. The Committee then shall determine whether the Report constitutes a Breach using the Breach Decision Tree attached as **Exhibit B**. The Committee may direct the Privacy Officer to conduct further investigation if members require additional information to make a determination.

### B. The Privacy Officer shall document the Committee’s evaluation and analysis of the Report on the Breach Decision Tree and shall retain such document with the completed Investigation Form for the Report. Committee members shall not retain copies of completed Investigation Forms or Breach Decision Trees.

## 2. ***Expedited Review.*** If (1) the Report indicates there is an urgent need to provide notice to impacted persons (*e.g*., immediate threat of misuse of PHI), or (2) the Report is made more than thirty (30) days following its discovery (as defined in Section 2.B above), the Privacy Officer shall promptly determine whether the Report constitutes a Breach using the Breach Decision Tree. To the extent possible, the Privacy Officer shall involve at least one Committee member in making such a determination. The Privacy Officer shall document his/her evaluation and analysis of the Report on the Breach Decision Tree and shall retain such document with the completed Investigation Form for the Report. At each Committee meeting, the Privacy Officer shall report to Committee members concerning such determinations since the last meeting.

## 3. ***Mitigation and Disciplinary Action.***

### A. With respect to each Report determined to involve an unauthorized use or disclosure of PHI (regardless of whether such Report is determined to be a Breach), the Committee shall evaluate and recommend to the Privacy Officer appropriate remedial measures to address any resulting harm and proactive steps to prevent similar unauthorized uses and disclosures in the future.

### B. The Privacy Officer shall document such recommendations on the Breach Decision Tree. The Privacy Officer, with the assistance of Committee members, shall implement such recommendations to the fullest extent possible.

### C. If the Committee determines an unauthorized use or disclosure involved a workforce member, the Privacy Officer shall report such matter to the Human Resources Director and the individual’s supervisor, who shall determine the appropriate disciplinary action based upon Department's established disciplinary procedures. Such discipline may include, but is not limited to, verbal warning, written warning, demotion, suspension, or discharge. A workforce member who improperly accesses the electronic medical record (including any status board) shall receive, at a minimum, a written warning. The Human Resources Director shall report to the Privacy Officer the disciplinary action taken against such individual.

### D. If the Committee determines an unauthorized use or disclosure involved a licensed individual, the Committee, working with the Privacy Officer, shall also recommend whether any report to the appropriate licensing agency may be required.

**Notification.** The Privacy Officer shall be responsible for providing and documenting appropriate notification for each Breach pursuant to the policy and procedure entitled Breach Notification.

**Record Retention.** The Privacy Officer shall retain paper or electronic copies of all completed Investigation Forms and Breach Decision Trees for a period of at least six (6) years.

Exhibit A

Confidential Investigation Form

**1. Brief description of what happened: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**2. Provide the following dates (if actual date unknown, list approximate date followed by “app”):**

Date of Report: \_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date of incident: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date incident discovered: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

**3. Identify the following (attach additional sheets as necessary):**

Person(s) making Report (include relationship to Department):[[4]](#footnote-4) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Manner in which Report was made: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Person(s) whose PHI may have been improperly used/disclosed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Person(s) responsible for improper use/disclosure (list job title/relationship to Department): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Other person(s) with knowledge: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Person(s) who improperly gained access to PHI (include category for each):[[5]](#footnote-5) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

PHI returned prior to having been accessed or unknown whether PHI was actually accessed (describe): \_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Efforts taken to minimize negative impact of any improper use/disclosure: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**4. Identify type of PHI involved or reasonably likely to be involved (check all that apply):**

\_\_\_ Patient’s full name, street address, and/or telephone number

\_\_\_ Diagnosis/identification of medical condition

\_\_\_ Nature of treatment received/medications prescribed

\_\_\_ Sensitive medical information (circle) mental health drug/alcohol abuse genetic information/ testing

HIV/AIDS/STDs other communicable disease

birth control/pregnancy other (describe)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_ Information that increases risk of identity theft (circle) account number mother’s maiden name

SSN other (describe) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**5. Indicate format of PHI improperly use/disclosed:**

\_\_\_\_ Paper (including facsimile)

\_\_\_\_ Electronic Portable Device (*e.g*., laptops, netbook, PDAs, tablet computers)

\_\_\_\_ Network Data (data residing in the organization’s system (*e.g*., folders, drives, servers)

\_\_\_\_ Oral (spoken)

\_\_\_\_ Other (specify) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**6. Identify persons interviewed during investigation:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**7. Describe and attach documentation created or provided during investigation**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature of Investigator Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Printed Name Job Title

Exhibit B

Confidential Breach Decision Tree

Date completed: \_\_\_\_ /\_\_\_\_ /\_\_\_\_\_\_\_ Completed by (check one)

\_\_ Committee

\_\_ Privacy Officer (reported to Committee on \_\_\_/\_\_\_/\_\_\_)

***I. Did the use/disclosure involve unsecured PHI?*** (*see* 45 CFR164.402)

**A. Electronic PHI**

1. Data at rest encrypted in manner consistent with NIST Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices* (encryption key stored on separate device than data).

2. Data in motion encrypted in manner consistent with NIST Special Publications 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementation*; 800-77, *Guide to Ipsec VPNs*; or 800-113, *Guide to SSL VPNs*, or other which are Federal Information Processing Standards (FIPS) 140-2 validated (encryption key stored on separate device than data).

3. Electronic media cleared, purged, or destroyed consistent with NIST Special Publication 800-88, *Guidelines for Media Sanitization*, such that PHI cannot be retrieved.

**B. Hard copy media**

Shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. (Redacted documents do not qualify.)

\_\_\_\_ **If yes to any of the above, PHI is secured, and no breach** (circle applicable provision).

\_\_\_\_ **If no to all of the above, go to Section II**

***II. Was the use/disclosure unauthorized?***

A. HIPAA-compliant authorization applicable to the use/disclosure? (attach copy or description):

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

B. Applicable exception under 45 CFR Part 164 Subpart E (identify):

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_ **If yes to either of the above, use/disclosure was authorized, and no breach.**

\_\_\_\_ **If no to both, go to Section III**.

***III. Did unauthorized use/disclosure compromise the security/privacy of the PHI?***

A. Good-faith unintentional use by workforce member or agent acting within scope of authority which results in no further unauthorized use/disclosure (45 CFR 164.402(2)(i)).

B. Good-faith inadvertent disclosure at Department by authorized person to another authorized person which results in no further unauthorized use/disclosure (45 CFR 164.402(ii)).

C. Disclosure to unauthorized person not reasonably able to retain information (45 CFR 164.402(2)(iii)).

\_\_\_\_ **If yes to any of the above, use/disclosure did not compromise security/privacy of PHI, and no breach** (circle applicable provision and summarize basis for conclusion below). **Go to Section V**.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_ **If no to all, go to Section IV**.

***IV. Can Department demonstrate that there is a low probability that the PHI has been compromised as a result of the unauthorized use/disclosure based on a risk assessment of the following factors? (Law presumes PHI is compromised as a result of any unauthorized use/disclosure; Department must have sufficient evidence to overcome this presumption)***

***For each relevant factor, summarize supporting evidence and attach supporting documentation to this form***

A. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

B. The unauthorized person who used the protected health information or to whom the disclosure was made

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

C. Whether the PHI was actually acquired or viewed by any person

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

D. The extent to which the risk to the PHI has been mitigated.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

E. Other relevant factors

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_ **If Department has sufficient evidence to overcome presumption that PHI has been compromised as documented herein, the unauthorized use/disclosure does not constitute a breach. Go to Section V.**

\_\_\_\_ **If Department does not have sufficient evidence to overcome presumption that PHI has been compromised, the unauthorized use/disclosure constitutes a breach. Privacy Officer must notify appropriate person(s) of breach pursuant to policy entitled “Breach Notification.” Go to Section V.**

**V. *Mitigation***

***Department must identify and take appropriate action to mitigate the impact of any unauthorized use/disclosure, regardless of whether it constitutes a breach.***

A. Recommended action to correct any harm resulting from unauthorized use or disclosure

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

B. Recommended action to prevent future unauthorized use or disclosure

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature of Investigator Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Printed Name Job Title

**Privacy Officer’s Report on Mitigation**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature Date

Sample Policy and Procedure No. 10

Breach Notification

Purpose:

The purpose of this policy is to ensure Department provides appropriate notification of any breach of unsecured protected health information (“UPHI”).

Policy:

Upon identification of a breach of UPHI pursuant to the policy procedure entitled “Breach Identification” (“Breach”), the Privacy Officer shall be responsible for providing notice to the appropriate person(s) in the form and manner required under the HIPAA Privacy Rule. The Privacy Officer shall be responsible for maintaining appropriate documentation of such notice.

References to the Privacy Officer in the following procedures include his/her designee(s).

Procedure:

# Toll-Free Number. Department shall maintain a toll-free number persons may call with questions and concerns relating to the privacy of their PHI, including questions regarding whether such information has been breached. The operator shall refer persons calling the toll-free number with such questions and concerns to the Privacy Officer.

# Timing of Notice.

## ***Sixty-Day Timeframe.*** Upon identification of a Breach, the Privacy Officer shall act promptly to provide the required notification as described herein. Such notification shall be made to the appropriate person(s) in the required manner as soon as possible, but not more than sixty (60) days following the date of discovery (as determined pursuant to the policy entitled *Breach Identification*).

## ***Incomplete Investigation.*** If the investigation to determine whether a Breach has occurred cannot be completed within sixty (60) days following the date of discovery, the Privacy Officer shall provide the required notice by the sixty (60)-day deadline, indicating to the recipient that Department’s investigation of the matter is ongoing. The Privacy Officer shall provide follow-up notice upon completion of the investigation as necessary to ensure all required information has been included in the notice provided.

* 1. ***Law Enforcement Request for Delay.*** If a law enforcement official provides a written statement to Department that notification otherwise required under this policy would impede a criminal investigation or cause damage to national security, the Privacy Officer shall delay providing such notification as directed by the official. If a law enforcement official provides such a statement orally, the Privacy Officer shall document the statement (including the official’s identity) and delay notification for no more than thirty (30) days from the date of the oral statement, unless a written statement is furnished by a law enforcement official during time period.

# Contact Information.

## A. The Privacy Officer shall have access to appropriate databases and other records maintained by Department to access patient contact information (including full name, address, telephone number, e-mail address, and whether a person has a personal representative (*i.e*., minors and other legally incapacitated persons)).

## B. For each identified Breach, the Privacy Officer shall obtain Department’s most current contact information for the person(s) impacted by such breach (or each such person’s personal representative, as appropriate). In the case of a deceased person, the Privacy Officer shall determine whether Department has contact information for such person’s personal representative or next of kin. As used hereafter, “Person” refers to a person impacted by a Breach or such person’s personal representative or, in the case of a deceased person, such person’s personal representative or next of kin.

## C. If Department does not have current contact information for a Person (with the exception of the personal representative or next of kin for a deceased Person), the Privacy Officer or his/her designee shall attempt to obtain such information using web-based services and other resources (*e.g*., [www.anywho.com](http://www.anywho.com), [www.peoplefinders.com](http://www.peoplefinders.com), [www.intelius.com](http://www.intelius.com)). Department shall subscribe to such web-based services as the Privacy Officer determines necessary for purposes of obtaining contact information.

## D. For those Persons for whom the Privacy Officer is able to locate current contact information, the Privacy Officer shall follow the procedures in Section IV. For those Persons for whom current contact information is not available, the Privacy Officer shall follow the procedures in Section V.

# Notice to Persons Whose Contact Information Is Available.

## A. ***Content of Notice.*** The Privacy Officer shall draft the notice to be delivered to a Person using plain language and including each of the following elements:

### 1. A brief description of what happened, including the date of the Breach and the date of discovery of the Breach, if known.

### 2. A description of the *types* of UPHI involved in the breach (*e.g.*, full name, SSN, date of birth, home address, account number). The actual information improperly used or disclosed should not be listed on the notice.

### 3. Any steps the Person should take to protect himself/herself from potential harm resulting from the Breach.

### 4. A brief description of what Department is doing to investigate the Breach, to mitigate harm to the Person, and to protect against future breaches.

### 5. Contact procedures for the Person to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Website, or postal address.

If Department is aware that a Person has limited English proficiency or a disability which limits his/her ability to read or understand such written notice, the Privacy Officer shall take steps that may be necessary to ensure effective communication with such Person.

## ***Notification by First-Class Mail.***

### 1. Except as permitted under Section IV.C, the Privacy Officer shall send by first-class mail the required notice to each Person for whom Department has a current mailing address.

### 2. The Privacy Officer shall maintain a copy of each such letter sent to a Person, as well as copies of any subsequent communication with any Person concerning the Breach, with the Investigation Report and Breach Decision Tree completed for the relevant Breach pursuant to the policy and procedure entitled *Breach Identification* (“Identification Forms”).

### 3. If any such letter is returned to Department as undeliverable, the Privacy Officer shall give notice to the Person as specified in Section V.

## ***Notification by E-Mail.***

### 1. If (and only if) the Privacy Officer confirms through review of Department’s records that a Person previously agreed in writing to receive breach notification by e-mail, and such agreement has not been withdrawn, the Privacy Officer may send the notice to that Person by e-mail. In addition to the elements listed in Section IV.A, any notice delivered by e-mail shall include the following statement: “You previously agreed to receive such notices from Department by e-mail as opposed to first-class mail.”

### 2. The Privacy Officer shall maintain a copy of each such e-mail message sent to a Person, as well as copies of any subsequent communication with any Person concerning the Breach, with the Identification Forms relating to the Breach.

### 3. If such e-mail message is returned as undeliverable, the Privacy Officer shall send notice to the Person by first-class mail as specified in Section IV.B., unless Department does not have a current mailing address for the Person, in which case notice shall be given as specified in Section V.

## D***. Confidential Communications.*** If a Person has requested confidential communications pursuant to 45 C.F.R. § 164.522(b), the Privacy Officer shall provide breach notification to that Person in the manner requested by the Person.

# Notice to Persons Whose Contact Information Is Not Available. If there is insufficient or out-of-date contact information for a Person that precludes written notification pursuant to Section IV, the Privacy Officer shall deliver a substitute form of notice as described in this Section V. Such notice shall be given as soon as reasonably possible after the Privacy Officer becomes aware that Department has insufficient or out-of-date contact information for such Person. Such substitute notice is not required, however, in the case of a Breach involving a deceased Person’s PHI if Department does not have adequate contact information for his/her personal representative or next of kin.

## A. ***Telephone.*** If Department obtains a current telephone number for the Person, the Privacy Officer shall attempt to speak to the Person by telephone. If the Privacy Officer has the opportunity to leave a message for the Person, the Privacy Officer shall leave a message stating his/her name, his/her affiliation with Department, his/her contact information, and that he/she has a very important message for the Person. If the Person returns the call, the Privacy Officer shall provide the Person with the information listed in Section IV.A. The Privacy Officer shall document such telephone communication(s), and attach such documentation to the Identification Forms relating to the Breach. If the Privacy Officer is unable to speak with or leave a message for the Person, the Privacy Officer shall give notice pursuant to Section V.C.

## B. ***E-Mail.*** If Department obtains an e-mail address for the Person, the Privacy Officer shall send an e-mail message stating his/her name, his/her affiliation with Department, his/her contact information, and that he/she has a very important message for the Person. It is not necessary for the Person to have given prior written permission to receive breach notification by e-mail for the Privacy Officer to send such communication to the Person. If the Person responds to the e-mail message, the Privacy Officer shall provide the Person with the information listed in Section IV.A, and shall document such communication. The Privacy Officer shall attach a copy of such e-mail message(s) and documentation relating to subsequent communications to the Identification Forms relating to the Breach. If the e-mail message is returned as undeliverable, the Privacy Officer shall give notice pursuant to Section V.C.

## C. ***Website Posting.***

##### Link to Notices. Department shall maintain in a prominent location (noticeable given its size, color, and graphic treatment in relation to other parts of the page) on the home page of its website (and the landing page or login page for existing account holders) a hyperlink entitled “**Information on HIPAA Privacy Rule Breach Notification**,” which shall refer the user to the following notice:

Federal law requires Department to provide notice to any person whose unsecured protected health information has been breached by Department or its business associates. If Department does not have current contact information for such an individual, Department must provide such notice on its website.

Department has identified the following breaches for which it does not have current contact information for persons whose protected health information was improperly used or disclosed. To learn whether your protected health information was involved in one of these breaches, please contact Department’s Privacy Officer by calling [telephone number] or sending an e-mail to [email address].

### Specific Notices. For each Breach for which there is one or more Persons whom the Privacy Officer cannot contact using the methods previously identified herein, the Privacy Officer shall post under the aforementioned notice a link to a .pdf document (or similar electronic document or file) containing that information listed in Section IV.A. Such document shall not include the name or, to the fullest extent possible, any other identifying information of the Person(s) impacted by the Breach. The link for each such document shall be labeled with the date on which the Breach occurred. Each such document shall remain posted on Department’s website for at least ninety (90) days. For recordkeeping purposes, the Privacy Officer shall attach a screen shot of the relevant web page to the Identification Forms relating to the Breach.

### The Privacy Officer shall respond to each individual who inquires whether his/her PHI (or the PHI of the person for whom the individual is a personal representative) is involved in any of the breaches for which notice is posted on Department’s website. The Privacy Officer shall confirm such person’s identity before furnishing information concerning the specific PHI involved in the breach. The Privacy Officer shall document such communications and attach such documentation to the Identification Forms relating to the Breach.

# Notification to the Media.

For a Breach involving more than 500 residents of a State, the Privacy Officer shall, following the discovery of the Breach, notify prominent media outlets serving that State. Such notice shall be provided in the same time frame and include the same information as the individual notice as discussed above.

Department is not required to incur any cost to print or run media notice regarding a Breach. There is no requirement that a media outlet who receives notification of a breach to print or run information about the breach. Posting a press release regarding the Breach on Department’s web site is not sufficient to meet this requirement; such press release must be provided directly to appropriate prominent media outlets.

# Notification to the Secretary of HHS.

A.***Breaches Involving 500 or More Individuals.*** For a Breach involving 500 or more individuals, the Privacy Officer shall provide notification to the Secretary of HHS in the manner specified at <http://ocrnotifications.hhs.gov/> within the time frame required for the individual notice as discussed above.

B.***Breaches Involving Fewer Than 500 Individuals.*** For each Breach involving fewer than 500 individuals, the Privacy Officer shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, shall provide notification to the Secretary of HHS in the manner specified at <http://ocrnotifications.hhs.gov/> for breaches discovered during the preceding calendar year.

# Recordkeeping. The Privacy Officer shall maintain all documentation relating to Breach notification (including Identification Forms, notices, follow-up communications) for a period of six (6) years.

Sample Policy and Procedure No. 11

Business Associates

Purpose:

The purpose of this policy is to ensure Department complies with those provisions of the HIPAA Privacy and Security Rules regarding business associates.

Policy Statement:

Department shall enter into and abide by HIPAA-compliant business associate agreements with each and every person or entity that qualifies as Department’s business associate and each and every person or entity for which Department qualifies as a business associate.

References to the Privacy Officer in the following procedures shall include his/her designee(s).

As used herein, the following terms shall have the same meaning as those terms in the HIPAA Privacy and Security Rules: protected health information, disclose and disclosure, Secretary, minimum necessary, and organized health care arrangement.

Procedure:

1. The Privacy Officer shall have primary responsibility for identifying each and every one of Department's business associates, as that term is defined in 45 CFR 160.103. Any member of Department’s workforce responsible for negotiating or contracting with third parties shall communicate with the Privacy Officer to determine whether a specific person or entity qualifies as Department’s business associate based on the parties’ contractual and/or business relationship.

Specifically, any person or entity entering into and maintaining the one or more of following relationships with Department qualify as Department’s business associate:

A. Any person or entity acting on Department’s behalf that performs, or assist in the performance of, a function or activity involving the use or disclosure of protected health information (“PHI”), including claims processing or administration; data analysis, processing, or administration; utilization review; quality assurance; patient safety activities listed at 42 CFR 3.20; billing; benefit management; practice management; and repricing.

B. Any person or entity that provides Department with legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services, where the provision of the service involves the disclosure of PHI from Department or from another business associate.

C. Any health information organization, e-prescribing gateway, or other person or entity that provides Department with data transmission services that requires access to PHI on a routine basis (vs. mere conduit, *e.g*., U.S. Postal Service, internet service provider).

D. Any person or entity that stores PHI in paper or electronic format on behalf of Department (except on a temporary basis in connection with data transmission).

E. Any person or entity that offers a personal health record to one or more individuals on behalf of Department.

F. Any subcontractor that creates, receives, maintains or transmits PHI on behalf of a business associate.

The following persons and entities *do not* qualify as Department’s business associates:

A. An individual acting in his/her capacity as a member of Department’s workforce.

B. A health care provider, with respect to disclosures of PHI by Department concerning treatment of an individual.

C. Department’s co-participants in an organized health care arrangement, to the extent the co-participant is performing a function or activity providing a service described above.

2. With respect to any business associate with which Department has a written business associate agreement in effect as of the Effective Date of this policy, the Privacy Officer shall take such action necessary for Department to enter into a new or amended written business associate agreement with such business associate in compliance with 45 CFR §§ 164.308(b), 164.314(a), 164.502(e), and 164.504(e), as amended (“HIPAA BAA Rules”), by no later than September 22, 2014, or upon renewal or modification of such agreement, whichever is earlier.

A. To the fullest extent possible, such new or amended business associate agreement shall contain provisions substantially similar to the standard agreement included as **Exhibit A**.[[6]](#footnote-6) If a business associate insists on the use of an agreement in a different form, the Privacy Officer shall be responsible for determining whether such agreement satisfies the aforementioned regulations.

B. Department shall not execute any business associate agreement that does not satisfy all of the HIPAA BAA Rules or that imposes any obligations on Department beyond those required by the HIPAA BAA Rules.

3. With respect to any business associate relationship into which Department enters following the Effective Date of this policy, the Privacy Officer shall take such action necessary for Department to enter into a written business associate agreement with the business associate in compliance with the HIPAA BAA Rules upon commencement of such relationship.

A. To the fullest extent possible, such business associate agreement shall contain provisions substantially similar to the standard agreement included as **Exhibit A**. If a business associate insists on the use of an agreement in a different form, the Privacy Officer shall be responsible for determining whether such agreement satisfies the aforementioned regulations.

B. Department shall not execute any business associate agreement that does not satisfy all of the HIPAA BAA Rules or that imposes any obligations on Department beyond those required by the HIPAA BAA Rules.

4. Department shall not enter into or continue any contractual or business relationship with any person or entity that qualifies as Department’s business associate if that person or entity fails or refuses to execute written business associate agreement in compliance with the HIPAA BAA Rules as specified in Sections 2 and 3.

5. Department shall disclose protected health information to a business associate only for the purposes specified in the parties’ written business associate agreement and only the minimum necessary information for those purposes.

6. If any member of Department's workforce has reason to believe a business associate has violated the terms of a business associate agreement with Department, such person shall report such information to the Privacy Officer as soon as possible.

A. The Privacy Officer shall investigate the matter and take reasonable steps to cure the breach or end the violation and, if such steps are unsuccessful, to take such action necessary to terminate the contract or arrangement.

B. If termination of the contract or arrangement is not feasible, the Privacy Officer shall report the matter in writing to the Secretary. Such communication shall contain a description of the business associate’s non-compliance and the reasons why termination of the relationship between the parties is not a viable alternative.

7. If Department enters into a relationship with a third party for which Department qualifies as the third party’s business associate, Department shall enter into a written business associate agreement in compliance with the HIPAA BAA Rules with that party. Department shall not execute any business associate agreement that does not satisfy the HIPAA BAA Rules or imposes any obligations on Department beyond those required by the HIPAA BAA Rules. The Privacy Officer shall be responsible for identifying those circumstances in which Department is required to execute a written business associate agreement as a business associate, ensuring such agreement complies with the HIPAA BAA Rules, and entering into any required written subcontractor agreement in compliance with 45 CFR 164.504(e)(5).

8. In disclosing information to a business associate or acting as a business associate to another covered entity, Department shall adhere to the terms of the written business associate agreement between the parties.

Exhibit A

HIPAA Business Associate Agreement

This HIPAA Business Associate Agreement (“**BAA**”) amends and is incorporated into [identify parties’ underlying agreement] (“**Agreement**”) by and between \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (“**Covered Entity**”) and \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(“**Business Associate**”) for purposes of compliance with the requirements of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5) (“ARRA”), and their implementing regulations set forth at 45 CFR Parts 160 and 164, as amended (the “HIPAA Rules”).

The following terms used in this BAA shall have the same meaning as those terms in the HIPAA Rules: breach, data aggregation, designated record set, disclose and disclosure, health care operations, individual, minimum necessary, Notice of Privacy Practices, protected health information (referred to herein as “PHI”), required by law, secretary, security incident, subcontractor, unsecured PHI, and use.

**1. Duties of Business Associate.** Business Associate agrees to:

1.1 Use or disclose PHI received from or on behalf of Covered Entity for the following purposes only:

(a) to perform those services specified in the Agreement, provided such use or disclosure is done in a manner that would not violate Subpart E of 45 CFR 164 if done by Covered Entity;

(b) to make a disclosure required by law; and

(c) for the proper management and administration of Business Associate or to carry out Business Associate’s legal responsibilities.

1.2 Make uses and disclosures and requests for PHI consistent with Covered Entity’s minimum necessary policies and procedures.

1.3 Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic PHI, to prevent use or disclosure of PHI other than as provided for herein;

1.4 Report to Covered Entity any use or disclosure of PHI not provided for herein of which Business Associate becomes aware, including breaches of unsecured PHI as required at 45 CFR 164.410, and any security incident of which Business Associate becomes aware;

1.5 In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of Business Associate agree to the same restrictions, conditions, and requirements that apply to Business Associate with respect to such information;

1.6 Make available PHI in a designated record set to Covered Entity as necessary to satisfy Covered Entity’s obligations under 45 CFR 164.524;

1.7 Make any amendment(s) to PHI in a designated record set as directed or agreed to by Covered Entity pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy Covered Entity’s obligations under 45 CFR 164.526;

1.8 Maintain and make available the information required to provide an accounting of disclosures to Covered Entity as necessary to satisfy Covered Entity’s obligations under 45 CFR 164.528;

1.9 To the extent Business Associate is to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to Covered Entity in the performance of such obligation(s); and

1.10 Make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.

**2. Notice to Business Associate Regarding Privacy Practices and Restrictions**

2.1 Covered Entity shall notify Business Associate of any limitation(s) in Covered Entity’s Notice of Privacy Practices under 45 CFR 164.520, to the extent that such limitation may affect Business Associate’s use or disclosure of PHI.

2.2 Covered Entity shall notify Business Associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her PHI, to the extent that such changes may affect Business Associate’s use or disclosure of PHI.

2.3 Covered Entity shall notify Business Associate of any restriction on the use or disclosure of PHI that Covered Entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect Business Associate’s use or disclosure of PHI.

**3. Permissible Requests by Covered Entity**

3.1 Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under Subpart E of 45 CFR Part 164 if done by Covered Entity.

**4.** **Term and Termination**

4.1 The term of this BAA shall be the same as the term of the parties’ Agreement, except Covered Entity may terminate this BAA for cause as authorized in Section 5.2

4.2 Business Associate authorizes termination of this BAA by Covered Entity, if Covered Entity determines Business Associate has violated a material term of the BAA and Business Associate has not cured the breach or ended the violation within the time specified by Covered Entity.

4.3 Upon termination of this BAA for any reason, Business Associate, with respect to PHI received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, shall:

(a) Retain only that PHI which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;

(b) Return to Covered Entity (or, if agreed to by Covered Entity at the time, destroy) the remaining PHI that the Business Associate still maintains in any form;

(c) Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic PHI to prevent use or disclosure of the PHI, other than as provided for in this Section, for as long as Business Associate retains the PHI;

(d) Not use or disclose the PHI retained by Business Associate other than for the purposes for which such PHI was retained and subject to the same conditions set out at above which applied prior to termination; and

(e) Return to Covered Entity (or, if agreed to by Covered Entity at the time, destroy) the PHI retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities.

The obligations of Business Associate under this Section 6.3 shall survive the termination of this BAA.

**5. Miscellaneous**

5.1 A reference in this BAA to a section in the HIPAA Rules means the section as in effect or as amended. The parties agree to take such action as is necessary to amend this BAA from time to time as is necessary for compliance with the requirements of the HIPAA Rules and any other applicable law. Any ambiguity in this BAA shall be interpreted to permit compliance with the HIPAA Rules.

5.2 The relationship between Covered Entity and Business Associate (including any subcontractor) is one of independent contractor only. Neither Business Associate nor any subcontractor shall be authorized to act as the agent of Covered Entity for any purpose. Covered Entity does not purport to control or direct the manner in which Business Associate (including any subcontractor) performs its contractual duties and obligations under this BAA.

5.3 Nothing in this BAA shall be construed to create any rights or remedies in any third parties or any agency relationship between the parties.

5.4 The terms and conditions of this BAA override and control any conflicting term or condition of the Agreement All non-conflicting terms and conditions of the Agreement remain in full force and effect.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **COVERED ENTITY:** | |  | **BUSINESS ASSOCIATE:** | |
| By: |  |  | By: |  |
|  | (Signature) |  |  | (Signature) |
| Name: |  |  | Name: |  |
|  | (Please Print) |  |  | (Please Print) |
| Title: |  |  | Title: |  |
|  | (Please Print) |  |  | (Please Print) |
| Date: |  |  | Date: |  |

Sample Policy and Procedure No. 12

Workforce Training

Purpose:

The purpose of this policy is to ensure Health Department provides appropriate training to members of its workforce who have access to Protected Health Information (“PHI”) as required by the HIPAA Privacy Rule.

Policy Statement:

All members of Health Department’s workforce who have access to PHI shall be required to complete training concerning the requirements of the HIPAA Privacy and Security Rules and Health Department’s policies and procedures relating to the privacy and confidentiality of PHI. As part of such training, members of the workforce shall be required to execute a Confidentiality Agreement.

Procedure:

1. All members of Health Department’s workforce who have access to PHI shall receive training concerning compliance with the HIPAA Privacy and Security Rules. Health Department’s workforce includes all employees, students, and volunteers, as well any trainees working with Health Department, regardless of whether such trainee is compensated by Health Department. The training shall provide an overview of Health Department’s treatment, payment, and health care operations, and stress the importance of PHI as it relates to these functions. Upon completion of the training, all members of Health Department’s workforce shall be able to identify what constitutes PHI, understand policies and procedures concerning safeguarding and the use and disclosure of PHI, and become familiar with individual rights and Health Department’s administrative responsibilities under the HIPAA Privacy Rule. Health Department shall document attendance at such training sessions, and maintain such documentation, along with any materials used during such training (*e.g.*, handouts, PowerPoint presentations, outlines) for a period of six (6) years.

2. Each workforce member shall participate in HIPAA training within thirty (30) days of commencement of work for the Health Department. Additionally, the Health Department shall provide training for its workforce members annually and each time there are substantive revisions to Health Department’s HIPAA policies and procedures for those workforce members whose job responsibilities are impacted by those revisions. Health Department may provide HIPAA training to some or all of its workforce members as an appropriate remedial or proactive measure to address a violation of the HIPAA Privacy or Security Rules.

3. All members of Health Department’s workforce shall be required to execute the Confidentiality Agreement attached as Exhibit 1. For each employee, Health Department shall retain the executed Confidentiality Agreement in the employee’s file. Each person executing the Confidentiality Agreement shall receive a copy of the document for his/her reference.

4. Participation in HIPAA Privacy Rule training and execution of the Confidentiality Agreement shall be a condition of employment by Health Department.

Exhibit A

**Printed Name:**

**Confidentiality Agreement**

As used herein, the following terms shall have the following meanings:

1. “**Confidential Information**” includes any information, regardless of the manner in which is communicated or maintained (*e.g.*, oral, paper, electronic), received by Health Department, or any of its agents, that falls into one or more of the following categories:

a. **Protected Health Information**: Information relating to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual. Protected Health Information includes demographic information, *e.g.,* address, telephone number, employer, date of birth, next of kin, identification numbers.

b. **Personnel Information**: Information relating to a person’s status as a member of Health Department’s workforce, including, but not limited to, compensation, employment records, accommodations, performance reviews, and disciplinary actions.

c. **Third Party Information**: Information belonging to a third party utilized by Health Department for limited purposes pursuant to an agreement with the third party, including, but not limited to, computer programs, client and vendor proprietary information source code, and proprietary technology.

2. “**Receive**,” “**Receiving**,” and “**Receipt**” means, with respect to Confidential Information, to come into possession, custody, or control; to perceive; to create; to gain the ability to come into possession, custody, or control; or to gain the ability to perceive Confidential Information in whatever form (oral, visual, written, electronic, or otherwise).

3. “**Use**” means, with respect to confidential information, accessing, reviewing, employing, applying, utilizing, examining, or analyzing such information, or sharing or discussing such information with other members of Health Department’s workforce.

4. “**Disclose**” means, with respect to Confidential Information, release, transfer, provision of access to, or divulging in any other manner such information to a person or entity who is not a member of Health Department’s workforce.

5. “**Health Department’s Workforce**” includes employees and other persons whose conduct, in the performance of work for Health Department, is under the direct control of Health Department, whether are not they are compensated by Health Department for such services. Business associates with which Health Department has entered into business associate agreements are not part of its workforce.

6. “**Computer Systems**” includes computer files, computer hard drives, local area network, wide area network, mainframe, electronic mail, internet access, intranet access, electronic medical records, and electronic order entry.

In performing your job duties, you may receive or create Confidential Information. As a condition of and in consideration of your receipt of Confidential Information, you agree to the following:

1. You understand that you have no right or ownership interest in any Confidential Information which you may receive. Health Department may, at any time and for any reason, revoke your password, access code, or any other authorization you have that allows you to receive Confidential Information in any form.

2. You understand that your obligations under this Agreement will continue after termination of your relationship (employment or otherwise) with Health Department. You understand that your privileges hereunder are subject to periodic review, revision, and, if appropriate, renewal.

3. The use and disclosure of Confidential Information is governed by Federal and State laws and regulations as well as Health Department’s policies and procedures. The purpose of these specific requirements is to guarantee that Confidential Information remains confidential, *i.e.,* such information shall be used and disclosed only as necessary to accomplish Health Department’s mission. You shall be familiar with and adhere to all of these requirements concerning Confidential Information.

4. You shall actively participate in educational opportunities made available to you concerning proper safeguards for Confidential Information and uses and disclosures of Confidential Information as part of your job duties.

5. If you have any question concerning whether certain information constitutes Confidential Information, you shall bring the matter to your supervisor or Health Department’s Privacy Officer for direction.

6. You shall use and disclose Confidential Information only to the extent necessary to perform your assigned job duties. Such use and disclosure shall be in a manner consistent with applicable Health Department policies and procedures. Your use or disclosure of Confidential Information for any reason other than the performance of your assigned job duties or your failure to conform to applicable policies and procedures shall constitute misuse of Confidential Information. You understand that any misuse of Confidential Information may be grounds for discipline (up to and including termination of your employment or other relationship with Health Department) and/or the initiation of legal action against you.

7. Health Department is committed to protecting the privacy of those persons for whom it provides services. To fulfill its commitment, Health Department prohibits members of its workforce from discussing any information relating to persons covered by the plan except as necessary to perform their specific job duties. You shall not discuss or disclose protected health information to any person except as needed to perform your specific job duties. You shall not engage in casual conversations concerning the fact that a person is or has been a patient of Health Department or concerning any information relating to such persons, *e.g.*, diagnosis, procedures, outcome, payment.

8. If you have any question concerning whether your assigned job duties permit you to use or disclose certain Confidential Information in a particular manner, you shall bring the matter to your supervisor or Health Department’s Privacy Officer for direction. If you have any question concerning the application of a particular policy or procedure to a particular use or disclosure of Confidential Information, you shall bring the matter to your supervisor or Health Department’s Privacy Officer for direction.

9. You shall appropriately safeguard Confidential Information so as to prevent any inappropriate use or disclosure of such information. If you have reason to believe the confidentiality of information may have been compromised, you shall report such concerns to your supervisor or Health Department’s Privacy Officer as soon as possible.

10. In performing your job responsibilities, you shall not knowingly include or cause to be included in any record or report a false, inaccurate, or misleading entry. Nor shall you make or cause to be made any false, inaccurate, or misleading statement to any person. If you become aware of false, inaccurate, or misleading information contained in any record or report, or a false, inaccurate, or misleading statement, you shall report the matter to your supervisor and cooperate in taking all steps necessary to correct the record, report, or statement pursuant to Health Department policies and procedures.

11. You shall comply with Health Department policies and procedures concerning the alteration, deletion, or destruction of Confidential Information in any form. If you have any question concerning such policies and procedures, you shall bring the matter to your supervisor for direction. If you have any reason to believe such policies and procedures have been violated, you shall report such concerns to your supervisor or Health Department Privacy Officer as soon as possible.

12. You understand that Health Department may monitor each and every time its computer systems are accessed. You understand that any action you take in these computer systems may be tagged with your unique identifier as established in you user profile, and such actions may be traced back to you.

13. You shall safeguard and shall not disclose to any person your computer password, access code, or any other authorization you have that allows you to access Health Department’s computer systems. You shall be responsible for all activities undertaken using your password, access code, and other authorization, and you shall be responsible for any misuse or wrongful disclosure of Confidential Information resulting from the use of your password, access code, or other authorization. You shall not utilize any other person’s computer password, access code, or any other authentication to access any computer system.

14. If you have reason to believe the security of your computer password, access code, or any authorization you have that allows you to access to Health Department’s computer systems has been compromised, you shall report such concerns to your supervisor as soon as possible.

15. You shall respect the ownership of proprietary software. For example, you shall not make unauthorized copies of any software for your own use, even if the software is not physically protected against copying, nor shall you operate any non-licensed software on any computer provided by Health Department.

By signing this document, you certify that you have reviewed the foregoing Confidentiality Agreement, have been provided with an opportunity to ask questions concerning its terms, and understand the duties and obligations it imposes on you. You hereby agree to the duties and obligations as stated in this Confidentiality Agreement. You understand that this signed and dated document will become part of your permanent personnel record.

Signature Date

Sample Policy and Procedure No. 13

Safeguarding Protected Health Information

Purpose:

The purpose of this policy is to ensure Health Department utilizes appropriate administrative, physical, and technical safeguards to prevent inadvertent or unauthorized disclosures of protected health information.

Policy Statement:

To prevent any inadvertent or unauthorized disclosure of protected health information, Health Department shall identify and utilize appropriate administrative, physical, and technical safeguards relating to workforce identification, paper records, computers, facsimiles, telephone communications, and other oral communications.

Irrespective of any specific provision of this policy and procedure, no employee shall utilize any safeguard, or lack therefor, to directly or indirectly permit himself/herself or any other person to access, view, distribute, or otherwise obtain unauthorized information.

The Privacy Officer shall be responsible for periodically reviewing Health Department’s safeguards for protected health information and for identifying and implementing new safeguards and/or procedures as might be necessary to the underlying purpose of this policy and procedure and applicable state and federal laws and regulations.

Procedure:

Workforce Identification.

1. While present at Health Department’s facility or providing outreach services on behalf of Health Department (*e.g.*, health fairs, home visits), all employees shall wear appropriate identification.

2. Any visitor to Health Department’s facility, other than persons present in the reception area, shall be escorted by an employee at all times. In the case of vendors providing services or making deliveries at the facility, an employee escort shall not be required if the vendor wears appropriate identification while at the facility.

Paper Records.

1. During regular business hours, access to all paper records containing protected health information shall be restricted in one of the following ways:

(a) An employee is present and immediately available to prevent any unauthorized person from having access to such record; or

(b) The record is contained in a file drawer, storage area, or work space to which non-employees are not permitted access.

2. During non-business hours, access to all paper records containing protected health information shall be restricted in one of the following ways:

(a) All doors to the facility shall be locked at the close of business hours and shall remain locked until the beginning of the next business day;

(b) Upon departure, employees should not leave paper documents containing protected health information visible in their work areas; and

(c) If persons not employed by Health Department enter the facility after regular business hours for purposes of cleaning the facility or providing security services, Health Department shall obtain a signed confidentiality agreement from the company providing such services representing that no employee of such company shall attempt to access any files or records of the facility.

3. No employee shall remove a paper record containing health information from the facility unless such transportation of a record is necessary for the employee to perform his/her job duties. Any employee who removes a record from the facility for such purposes shall appropriately safeguard the record while it is located outside the facility to prevent access by any third party (including family members), and promptly return the record to its proper location at the facility.

4. Any paper record containing protected health information shall be shredded prior to being discarded, or disposed of through a service which ensures that such records will be disposed of in such a manner that ensures that unauthorized persons will not obtain access to such records.

Computers.

Given the rapid advancements in technology, it is difficult to identify appropriate computer security measures at any given point in time. The following practices should be followed to provide a “baseline” level of security for protected health information maintained in electronic form. The Privacy Officer shall have ongoing responsibility for identifying particular computer security threats and risks to Health Department, and identifying and implementing additional and/or revised computer security measures for Health Department, which measures shall be memorialized in writing and distributed to all users.

1. Access to computer servers and computer workstations shall be restricted so that unauthorized persons do not gain physical or other access to such systems (or to the information visible on the screens of such systems). In order to access any computer, the operator will be required to enter her/his username and her/his password. Password- protected screen savers shall be installed on all computers so that when a user is away from their computer, unauthorized persons do not gain access to such computer or confidential information. Such password-protected screen savers shall be configured to activate after a short interval (and shall also be capable of being manually activated by a user) so that after such screen saver activates, the computer screen thereafter does not display any confidential information and the computer itself cannot be utilized again until a password is entered. The length of time before a screen saver activates shall be set to avoid disclosure of confidential information to unauthorized persons, as could happen if a user left their work area and forgot to manually activate the screen saver. Employees shall lock any computer terminal not in use if no employee is in the immediate vicinity of the terminal, and all employees shall be trained on how to activate the screen saver on all computers, so if they notice an operating computer with no employee in the immediate vicinity, they can immediately take steps to activate the screen saver on such computer. All computer monitors shall be positioned in such a manner so as to avoid inadvertent disclosures of information contained on the monitor. The Privacy Officer shall be responsible for reviewing the above procedures, and for submitting proposals so that new procedures can be implemented, as may be necessary, to ensure that unauthorized persons do not gain access to such systems.

2. Each member of Health Department’s workforce requiring access to protected health information maintained in electronic computer files to perform his/her job duties shall be granted access to the appropriate files through the use of a computer password. Such computer access shall be terminated immediately upon the termination of such person’s employment or other relationship with Health Department. Such password shall be at least seven digits and contain three of the following four types of characters: upper case alphabetic characters, lower case alphabetic characters, numeric characters, and special characters (e.g., &, #, @). Such password shall be changed at least every ninety (90) days. Users shall keep their password confidential. Users shall not provide their passwords to any other user in Health Department, and users shall never provide their password to anyone outside of Health Department, including family members. No user shall operate a computer logged on as another user, except under the following circumstances: (1) if a person logged onto a computer needs assistance, another person can help that logged on user so long as the logged on user is physically present, and all persons involved are authorized to view any information which is accessed during the period of such assistance; or (2) computer support staff shall only access accounts and passwords as are necessary to maintain the computer systems and shall always assure that their efforts do not lead to access of confidential information by unauthorized personnel, including themselves. The Privacy Officer shall be responsible for periodically reviewing the procedures regarding passwords, to ensure that the passwords being utilized (and the procedures regarding the same) are sufficient to prohibit unauthorized persons from logging on to Health Department’s computers or computer systems, and that such passwords are not being written down or stored in a manner which would permit unauthorized persons to gain access to such passwords.

3. Health Department shall utilize and maintain appropriate hardware and software to prevent unauthorized access to Health Department’s computer systems, and the data on such system. Health Department shall utilize firewalls, virus detection and prevention software, data encryption, and other appropriate hardware and software as might be required to prevent such unauthorized access. Such technology shall be updated on a regular basis to take advantage of technological advancements.

4. Employees’ personal use of Health Department’s computer systems, including e-mail and internet access, shall be limited and shall not be conducted in any manner that threatens the operations or integrity of such systems.

5. No employee shall post any protected health information on social media. All external bound email shall contain the following notice/disclaimer, and the email system shall be configured so that all external bound emails contain such a notice/disclaimer.

**Important: This email and any attachments may contain confidential information subject to protection under the HIPAA Privacy Rule. If it appears that this email was sent to you in error, (1) you are prohibited from utilizing or disseminating this email or any attachments; (2) please immediately delete it from your computer and any servers or other locations where it might be stored and email (sender’s email address) or call (sender’s name) at sender’s phone number) advising that you have done so. We appreciate your cooperation.**

6. Upon discontinuation of use of any computer equipment by Health Department, appropriate measures shall be taken to ensure any data contained on the equipment is removed.

7. Computer data, including backup tapes or other archive information, shall be stored in locked areas, or if stored offsite, stored in a location where the information will be treated in a confidential manner and not provided to unauthorized persons.

8 If it is necessary to grant users remote access to Health Department’s computer system, or to utilize mobile devices, such as laptop computers or personal digital assistant devices (PDAs), policies and procedures shall be developed to ensure that only authorized personnel obtain remote access, and that adequate safeguards are utilized to ensure that unauthorized persons do not gain access to confidential information.

9. Printers utilized to print confidential information shall be located in areas not accessible to unauthorized persons, and safeguards, such as removing documents from the printer shortly after they are printed, shall be utilized to ensure that unauthorized persons do not gain access to printed, confidential information.

Facsimile.

1. To the extent reasonably possible, Health Department shall take reasonable safeguards to protect facsimile transmissions, including, but not limited to:

(a) locating the fax machine in a low-traffic area not accessible by visitors;

(b) limiting access to the fax machine to certain employees; and

(c) immediately removing from the fax machine documents sent and received and distributing such documents to the appropriate person.

2. Employees shall take reasonable steps to ensure facsimile transmissions are sent to their intended recipients, including, but not limited to:

(a) refraining from sending highly confidential information via facsimile;

(b) double-checking facsimile numbers prior to dialing;

(c) utilizing the pre-programmed number function as much as possible;

(d) periodically reminding regular facsimile recipients to provide updated information; and

(e) if an employee becomes aware that a facsimile has been misdirected, contacting the recipient personally and requesting that the facsimile be discarded.

3. All facsimile transmissions should include a cover sheet containing the following statement:

**Important: The documents in this facsimile transmission may contain confidential information subject to protection under the HIPAA Privacy Rule. This information is intended only for the use of the individual or entity named above. If it appears that this facsimile transmission was sent to you in error, (1) you are prohibited from utilizing or disseminating any information contained herein; (2) please immediately destroy this facsimile and email (sender’s email address) or call (sender’s name) at (sender’s phone number) advising that you have done so. We appreciate your cooperation.**

Telephone Communications.

1. No member of the workforce shall communicate protected health information over the telephone to any person without confirming the person receiving the information is an appropriate recipient of such information.

2. Telephone communications concerning protected health information shall be conducted in such a manner that they are not overheard by any third person, *i.e.*, telephone calls should be made and received in a non-public area in the facility.

3. Other than a request for an individual to return a call to the Health Department, no message containing protected health information shall be left on an individual’s voice mail unless specifically authorized by the patient or, if necessary, in a medical emergency.

Other Oral Communications.

1. Conversations between members of Health Department’s workforce or between a member of Health Department’s workforce and the person who is the subject of the information or is authorized to receive such information shall be conducted in such a manner that such conversations are not overheard by any third person, regardless of whether they are conducted inside or outside Health Department’s facility.

2. Members of Health Department’s workforce shall not discuss protected health information with friends, family members, or other third persons to whom disclosure of such information is not authorized.

Sample Policy and Procedure No. 14

Complaints and Grievance Process

Purpose:

To ensure individuals have the opportunity to file complaints with Health Department concerning the handling of their protected health information (“PHI”) by Health Department, and that Health Department properly responds to such complaints.

Policy:

Health Department shall provide individuals the opportunity to file complaints with Health Department concerning Health Department’s handling of their PHI, shall properly investigate such complaints, and shall take remedial action as appropriate to correct any inappropriate handling of PHI.

Procedure:

Prohibition on Retaliation and Waiver.

1. No member of Health Department’s workforce shall intimidate, threaten, coerce, discriminate against, or take any other retaliatory action against any individual for exercising his/her rights under federal or state laws concerning PHI, including, but not limited to, the filing of any complaint against Health Department, a member of Health Department’s workforce, or a business associate of Health Department.

2. In no circumstance shall Health Department require any person to waive his/her rights under federal or state laws concerning PHI for any purpose, including, but not limited to, the provision of services by Health Department.

Filing Complaints.

1. Health Department’s Notice of Privacy Practices shall state the manner in which an individual may file a complaint concerning Health Department’s privacy practices.

2. Any member of Health Department’s workforce receiving an inquiry from an individual indicating a desire or intent to file a complaint or an inquiry concerning the process for filing complaints shall direct such patient to the Privacy Officer for further information.

3. The Privacy Officer shall be responsible for responding to individuals’ questions concerning the complaint process and for receiving, acknowledging, and processing complaints concerning Health Department’s privacy practices.

4. To the extent possible, the Privacy Officer should endeavor to obtain a written statement from each individual filing a complaint. If the individual communicates his/her complaint orally, and is unwilling or unable to provide a written statement, the Privacy Officer shall reduce such complaint to writing. To the fullest extent possible, the Privacy Officer should obtain the following information from the individual filing a complaint with Health Department: a sufficient description of the act or omission about which the individual complains; the persons involved; how the individual became aware of the problem; and the remedy sought by the person submitting the complaint, if any.

5. If an individual asks for information concerning the filing of a complaint with the Department of Health and Human Services or other government entity, the Privacy Officer shall provide the following information to the individual:

A. The individual has a right to file a complaint with the Department of Health and Human Services if he/she believes Health Department, a member of its workforce, or a business associate of Health Department has failed to comply with the requirements of federal law concerning the privacy and confidentiality of PHI.

B. All such complaints must be filed in writing, either on paper or electronically. Paper filings should be sent to the following address:

Office of Civil Rights

U.S. Department of Health and Human Services

200 Independence Avenue, S.W.

Room 509F, HHH Building

Washington, D.C. 20201

For electronic filings, the complaint should be sent via e-mail to:

[ocrmail@hhs.gov](mailto:ocrmail@hhs.gov)

C. The complaint should identify Health Department and describe the acts or omissions believed to be in violation of federal law.

D. The complaint must be filed within 180 days of when the person knew or should have known that the act or omission occurred to guarantee consideration by the Department. The Department may consider complaints filed outside this time period based on good cause shown.

The Privacy Officer shall request that the individual who expresses an intention to submit a complaint to the Department of Health and Human Services submit a copy of the complaint to Health Department.

Response to Complaints.

1. The Privacy Officer shall be responsible for investigating any complaint filed by an individual concerning Health Department’s privacy practices. If the Privacy Officer identifies what he/she believes to be a violation of federal or state law, the Privacy Officer shall, with the assistance and involvement of management, correct the violation, mitigate any harmful effects of such violation, and take appropriate action to prevent future violations, including disciplinary action, development, and implementation of revised policies and procedures, and/or training and education. The Privacy Officer shall appropriately document such investigation and corrective action, if any. As necessary, the Privacy Officer shall involve legal counsel in the investigation and/or development and implementation of corrective action.

2. The Privacy Officer shall be responsible for informing in writing the individual who submitted the complaint of the outcome of the investigation undertaken as a result of the complaint.

3. The Privacy Officer shall maintain all documentation relating to a particular complaint for a period of six (6) years following notification to the individual of the outcome of the investigation.

Sample Policy and Procedure No. 15

Disclosure of Protected Health Information  
for Purposes of Electronic Health Information Exchange

Purpose:

The purpose of this policy is to ensure Department participates in electronic health information exchange (“HIE”) in a manner that protects the privacy rights of those individuals whose protected health information is exchanged.

Policy Statement:

Department shall comply with the Kansas Health Information and Technology Act (“KHITE”) and the terms of its Participation Agreement with an approved health information organization (“approved HIO”) in disclosing an individual’s electronic protected health information (“e-PHI”) for purposes of HIE.

Background:

Pursuant to KHITE, a health care provider cannot disclose an individual’s e-PHI for purposes of HIE unless:

1. the provider obtains a HIPAA-compliant authorization from the individual (or his/her personal representative) prior to the disclosure; or

2. the disclosure is made through an approved HIO, with which the provider has a written participation agreement, and:

A. the disclosure is consistent with the approved HIO’s established procedures;

B. prior to the disclosure, the provider either delivers the required notice regarding HIE to the individual (or his/her personal representative) or confirms the notice has been delivered to the individual by a third party; and

C. the provider otherwise adheres to the terms of the participation agreement with the approved HIO.

Notwithstanding the foregoing, an individual’s e-PHI shall not be disclosed through an approved HIO if the individual (or his/her personal representative) has restricted such disclosures utilizing the process maintained by the Kansas Department of Health and Environment (“KDHE”).

Scope:

This policy applies to disclosures of e-PHI through an approved HIO for purposes of HIE. It does not apply to disclosures of e-PHI made through DIRECT or other secure messaging or disclosures made via the patient portal in Department’s electronic health records. Such disclosures are subject to and shall comply with Department’s HIPAA Privacy and Security Rules policies. Disclosures of e-PHI for purposes of HIE also are subject to such HIPAA policies, as well as the requirements of this policy.

Procedure:

1. Department shall include in its HIPAA-required Notice of Privacy Practices the required notice regarding HIE. The specific content of the required notice and the manner of its distribution is the subject of a separate policy, *Maintenance and Distribution of Notice of Privacy Practices*.

2. Department participates in [*specify Kansas Health Information Network or Lewis and Clark Information Exchange*] (“[HIE Abbreviation]”) under the terms of a written Participation Agreement (“Agreement”). Department shall comply with all applicable terms and conditions of the Agreement including, but not limited to, specifications regarding the manner in which Department will provide [HIE Abbreviation] with access to e-PHI maintained in Department’s electronic health records.

3. As part of the Agreement, [HIE Abbreviation] has assumed the role of Department’s business associate and all related responsibilities as defined by the HIPAA Privacy Rule. Specifically, [HIE Abbreviation] has assumed the role of managing e-PHI on behalf of Department to facilitate HIE. As such, Department shall permit [HIE Abbreviation] to access Department’s electronic health records solely for those purposes specified in the Agreement. Department shall permit [HIE Abbreviation] such access via a HIPAA-compliant interface with Department’s electronic health records. Department shall properly manage and regularly audit the security of such interface pursuant to Department’s HIPAA Security Rule policies regarding security risk analysis and risk management plan.

4. Through the Agreement, Department has secured [HIE Abbreviation]’s agreement to prohibit disclosure of any e-PHI from Department’s electronic health record via HIE (*i.e.,* in response to a query from another participant) unless and until the individual who is the subject of the e-PHI (or his/her personal representative) has received from Department or a third party the required written notice regarding HIE. Additionally, [HIE Abbreviation] has agreed to prohibit disclosure of an individual’s e-PHI for purposes of HIE if the individual (or his/her personal representative) has restricted such disclosures utilizing the process maintained by KDHE. Other than distributing the aforementioned Notice of Privacy Practices, Department does not have any role or responsibility with respect to the securing, enforcement, or revocation of such restrictions on disclosures for purposes of HIE.

5. Through the Agreement, Department has secured [HIE Abbreviation]’s agreement to make available to Department within ten (10) days of a written request an audit log documenting each occasion on which an individual’s e-PHI has been accessed through [HIE Abbreviation] for purposes of HIE for the three-year period prior to the request. Such log shall include the name of the person whose e-PHI was accessed, the date and time of such access, the person and/or entity who gained such access, and a description of the e-PHI that was accessed. To the extent an individual has requested the name of those persons who have gained access the individual’s e-PHI (as opposed to the entity only) and such audit log only lists the entity, Department shall work with [HIE Abbreviation] to identify those specific persons (*e.g*., contacting the entity and requesting assistance in identifying the individual).

6. The Privacy Officer shall be responsible for submitting such requests to [HIE Abbreviation] for purposes of (1) responding to an individual’s request for an accounting of disclosures pursuant to the separate policy entitled *Accounting of Disclosures of Protected Health Information and Provision of Electronic Access Report*; and (2) performing audits and investigations pursuant to Department’s HIPAA Privacy and Security Rules policies.

Sample Policy and Procedure No. 16

Access To Protected Health Information  
Through Electronic Health Information Exchange

Purpose:

The purpose of this policy is to ensure Department fully participates in electronic health information exchange (“HIE”) in a manner that protects the privacy rights of those individuals whose protected health information is exchanged.

Policy Statement:

No member of Department’s workforce shall attempt to access an individual’s electronic protected health information (“e-PHI”) through HIE except in compliance with this policy and procedure.

Scope:

This policy addresses workforce members’ attempts to access an individual’s e-PHI through HIE. It does not apply to attempts to access an individual’s e-PHI through other means, *e.g*., DIRECT, other secure messaging.

Procedure:

1. Department participates in [*Name of HIE*] (“[HIE Abbreviation]”) under the terms of a written Participation Agreement (“Agreement”). Pursuant to the terms of the Agreement, Department may query [HIE Abbreviation] to access e-PHI regarding a specific individual (versus submitting a single query seeking e-PHI for multiple individuals, which is not permitted). Department shall comply with the terms of the Agreement in submitting queries and using and further disclosing any e-PHI accessed through [HIE Abbreviation]

2. Only those workforce members who have completed required training and have received unique user identification may query [HIE Abbreviation] to access e-PHI regarding a specific individual. No workforce member shall permit another individual to utilize his/her user identification to access e-PHI.

3. A workforce member shall not query [HIE Abbreviation] to access e-PHI regarding an individual for any purpose other than treatment, payment, and health care operations (as those terms are defined by the HIPAA Privacy Rule, specifically 45 CFR 164.502(a)).

1. A workforce member who accesses an individual’s e-PHI for treatment purposes through [HIE Abbreviation] shall be responsible for incorporating that e-PHI relied upon in treating the individual into the individual’s electronic health record, including the identity of the participant from which the e-PHI was obtained through HIE. Such e-PHI shall be incorporated in the same manner as similar information received directly from the individual, a payer, or another provider.

5. In connection with an audit or investigation conducted pursuant to Department’s HIPAA Privacy and Security Rule policies, the Privacy Officer may submit a written request to [HIE Abbreviation] for an audit log identifying each occasion on which a specific member of Department’s workforce s has accessed an individual’s e-PHI maintained by a third party through [HIE Abbreviation] for the three-year period prior to the request. Through the Agreement, Department has secured [HIE Abbreviation]’s agreement to make available to Department within ten (10) days of a written request an audit log that includes the name of the person whose e-PHI was accessed, the date and time of such access, and a description of the e-PHI that was accessed.

6. Except as provided in the following section,[[7]](#footnote-7) a workforce member who submits a query to [HIE Abbreviation] regarding an individual and receives from [HIE Abbreviation] an electronic message that access to the individual’s e-PHI has been restricted shall not otherwise attempt to access the individual’s e-PHI through [HIE Abbreviation]. The workforce member may attempt to obtain the individual’s PHI through other means, *e.g.,* direct inquiries to providers that have furnished care for the individual.

7. In certain limited situations, a workforce member may attempt to access restricted e-PHI through KHIN.

A. If, in an emergency situation, (i) a physician or mid-level practitioner determines in his/her professional judgment that gaining access to an individual’s e-PHI is necessary to properly treat the individual, and (ii) the individual or his/her personal representative, after having been advised of the provider’s determination, consents to such access orally (or, if an oral response is not possible, by gesture), a properly authorized workforce member may “break the glass” to access such information through KHIN.

B. If, in such emergency situation, the individual is unable to communicate and no personal representative is available, a properly authorized workforce member may “break the glass” *only if* the physician or mid-level practitioner determines access to the individual’s e-PHI is necessary to save the individual’s life or prevent permanent disability.

* 1. If a physician or mid-level practitioner determines in his/her professional judgment that gaining access to an individual’s e-PHI is necessary to fulfill his/her legal duty to report specific information to a government agency (*e.g.*, report of suspected child abuse), a properly authorized workforce member may “break the glass” solely for the purpose of obtaining that information relevant to the reporting obligation.

An authorized workforce member may “break the glass” by accessing a patient record through KHIN’s provider portal only; such access is not permitted by KHIN through an individual’s electronic health record. The workforce member shall indicate the basis for the security override in attempting to access the restricted e-PHI through KHIN. The workforce member shall document in the patient’s record the basis for accessing restricted e-PHI, including the patient’s consent (if any).

Sample Policy and Procedure No. 17

Responding to Inquiries Regarding  
Electronic Health Information Exchange

Purpose:

The purpose of this policy is to ensure Department properly addresses an individual’s inquiry regarding electronic health information exchange (“HIE”), including a request for restrictions on disclosure of electronic protected health information (“e-PHI”) for purposes of HIE.

Policy Statement:

Members of Department’s workforce shall refer individuals’ inquiries regarding HIE and requests for restrictions on disclosure of PHI for purposes of HIE to the Kansas Department of Health and Environment (“KDHE”).

Background:

Department’s participation agreement with [*name of applicable HIE(s)*] requires Department to provide written notice to an individual regarding HIE, including the individual’s right to request restrictions on disclosures of e-PHI for purposes of HIE. That agreement also requires Department to post a written notice regarding HIE at its facility.

An individual who wishes to request restrictions is required to submit a completed form to [list contact information for each applicable HIE][[8]](#footnote-8). Such a restriction will prevent the disclosure of any e-PHI relating to the individual to any person or entity for any purpose (with the exception of mandatory reporting requirements). An individual cannot limit restrictions to certain information or specific providers.

The approved health information organizations in Kansas (“approved HIOs”), in cooperation with KDHE, are responsible for implementing such restrictions. Except as specified herein, Department is not required to take any action to assist an individual in requesting a restriction, to answer questions regarding restrictions, or to implement or reverse a restriction.

Procedure:

1. Department shall include in its HIPAA-required Notice of Privacy Practices the required notice regarding HIE. The specific content of the required notice and the manner of its distribution is the subject of a separate policy and procedure entitled *Maintenance and Distribution of Revised Notice of Privacy Practices*.

2. Department shall make available to individuals at its facilities copies of printed materials distributed by KDHE and/or approved HIOs providing information regarding HIE.

3. Department shall post the notice regarding HIE attached as Exhibit A at its facility in the same location(s) as other patient notices required by law (excluding EMTALA-required notices).

4. Department shall not be responsible for soliciting, receiving, processing, or implementing an individual’s request for restrictions on disclosures of e-PHI for purposes of HIE. Any workforce member who receives a question regarding HIE or a request for restrictions on disclosures of e-PHI for HIE shall refer the individual to the [list contact information for each applicable HIE][[9]](#footnote-9) website, or, alternatively, the Privacy Officer. A workforce member is not expected or required to answer such questions regarding HIE or otherwise assist an individual seeking to request restrictions.

5. A written request for restrictions received by KDHE shall be processed by KDHE and implemented by the approved HIOs. Neither Department nor any member of its workforce shall be responsible for implementing such restrictions, and may rely on KDHE and the approved HIOs to do so.

Exhibit A

HIE Notice Poster

**YOUR RIGHTS REGARDING**

**ELECTRONIC HEALTH INFORMATION EXCHANGE**

We participate in the electronic exchange of health information with other health care providers and health plans in the State of Kansas through an approved health information organization. Unless you direct otherwise, your electronic health records will be accessible through the exchange to properly authorized users for purposes of treatment, payment, and health care operations only.

***If you want to restrict access to your records through the***

***exchange, you must submit a request for restriction through   
the Kansas Department of Health and Environment***

***Visit*** [***www.kdhe.org***](http://www.kdhe.org) ***for more information.***

Even if you restrict access, your information still will be available through the exchange by a properly authorized individual as necessary to report specific information to a government agency as required by law (for example, reporting of certain communicable diseases or suspected incidents of abuse).

*For your protection, each request for restrictions is subject to verification procedures. Please allow sufficient time for your request to be processed. Your failure to provide all information required for verification may result in additional delay or denial of your request.*

1. [KHIE - <http://www.khie.org/for-consumers/opt-out> ]

   [LACIE - [info@lacie-hie.com](mailto:info@lacie-hie.com)]

   [MHC - <https://www.mhc-hie.org/your-option-2/>]

   [other HIEs] [↑](#footnote-ref-1)
2. Refer to agency website and regulatory updates for any changes to the mandatory reporting requirements. [↑](#footnote-ref-2)
3. [KHIE - http://www.khie.org/for-consumers/opt-out ]

   [LACIE - info@lacie-hie.com]

   [MHC - https://www.mhc-hie.org/your-option-2/]

   [other HIEs] [↑](#footnote-ref-3)
4. *e.g*., workforce member (include job title), agent, patient, personal representative, patient friend or family member, business associate. [↑](#footnote-ref-4)
5. Categories include workforce, business associate, other covered entity, other third party, and unknown. [↑](#footnote-ref-5)
6. Based on the January 25, 2013, Sample Business Associate Agreement Provisions published by the US Department of Health and Human Services Office of Civil Rights (available at <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html>). [↑](#footnote-ref-6)
7. Paragraph 7 concerns “break the glass,” *i.e*., accessing restricted e-PHI. LACIE does not permit such access in any circumstance; if Department participates in LACIE, Department’s policy would not provide for any exception to the rule stated in Paragraph 6. KHIN permits such access, but Department must define the specific circumstances in which it will permit a workforce member to “break the glass” based on Department’s own risk management analysis. By way of example only, Paragraph 7 identifies three circumstances in which Department may permit access to restricted e-PHI. [↑](#footnote-ref-7)
8. [KHIE - http://www.khie.org/for-consumers/opt-out ]

   [LACIE - info@lacie-hie.com]

   [MHC - https://www.mhc-hie.org/your-option-2/]

   [other HIEs] [↑](#footnote-ref-8)
9. [KHIE - http://www.khie.org/for-consumers/opt-out ]

   [LACIE - info@lacie-hie.com]

   [MHC - https://www.mhc-hie.org/your-option-2/]

   [other HIEs] [↑](#footnote-ref-9)