HAYSVILLE USD 261

HIPAA MEDICAL PRIVACY POLICIES AND PROCEDURES

Haysville USD 261 Organized Health Care Arrangement

HIPAA Privacy Policy and Procedures

Introduction

Haysville USD 261 (the "Company") sponsors the Haysville USD 261 Organized Health Care Arrangement (the "OHCA"). The OHCA consists of the Haysville USD 261 Medical Plan, the Haysville USD 261 Dental Plan, and the Haysville USD 261 Health Flexible Spending Account. An organized health care arrangement ("OHCA") is authorized to issue a joint Notice of Privacy Practices and develop one set of policies and procedures applicable to all group health plans that are members of the OHCA. Group health plans that are members of an OHCA are authorized to share protected health information with each other as necessary to carry out treatment, payment or health care operations and as necessary to manage and operate the organized health care arrangement. This policy sets forth the situations in which the Company, through its employees and other agents, may obtain *protected health information* from the OHCA and the procedures that must be followed if such information is obtained.

A. "Protected Health Information"

The term "*protected health information*" means information that relates to:

(1) the past, present, or future physical or mental health or condition of an individual;

(2) the provision of health care to an individual; or

(3) the past, present, or future payment for the provision of health care to an individual.

Additionally, in order for that information to constitute *protected health information*, it must either identify the individual or else there must be a reasonable basis to believe the information can be used to identify the individual. *Protected health information* includes information that relates to persons who are both living and deceased.

B. "Authorized Employees"

It is the policy of the Company and the OHCA to comply fully with the requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as set forth in the regulations issued by the Department of Health & Human Services ("HHS"). To that end, access to *protected health information* shall be strictly limited to the following employees of the Company (referred to herein as "Authorized Employees"):

Superintendent of Schools
Assistant Superintendent for Business/Finance
Benefits Clerk

In addition to the Authorized Employees listed above, upon the occurrence of an unusual and unanticipated event, for a limited time and for a limited purpose, certain employees may have access to protected health information where such access is necessary to complete one of their job functions. For example, it may be necessary for a member of the information technology ("IT") staff to access a database containing protected health information where there is a computer virus or similar problem, a defect in hardware, or other system failure. If such access is required by someone not listed above, the Privacy Officer will ensure that such individual's access to protected health information is limited in scope and time and that such individual is appropriately trained and complies with these policies and procedures. The Privacy Officer shall identify in writing at the time of the unanticipated and unforeseeable event the designation of the individual (by name, job title or other appropriate means) who may temporarily have access to protected health information.

Authorized Employees may use and disclose *protected health information* for plan administrative functions, and they may disclose *protected health information* to other Authorized Employees for plan administrative functions (but the disclosure must be limited to the minimum amount necessary to perform the plan administrative function).

Authorized Employees may not disclose *protected health information* to other employees (other than Authorized Employees) unless an authorization is in place or the disclosure otherwise is in compliance with this Policy.

C. Prohibited Actions

No employee of the company, including Authorized Employees, may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for exercising their rights, filing a complaint, participating in an investigation, or opposing any improper practice under HIPAA. No individual shall be required to waive his or her privacy rights under HIPAA as a condition of treatment, payment, enrollment or eligibility.

D. Privacy Officer / Contact Person / Security Officer

The Privacy Officer for the OHCA is the Assistant Superintendent for Business/Finance. The Privacy Officer is responsible for the development and implementation of policies and procedures relating to privacy, including but not limited to this Privacy Policy and the Company's use and disclosure procedures. In addition, the Privacy Officer shall have the specific responsibilities set forth in this Policy.

The Contact Person is Assistant Superintendent for Business/Finance. The Contact Person will answer questions and provide information about the OHCA's privacy policies and procedures. The Contact Person will also be responsible for the specific duties and responsibilities set forth in this Policy.

The Security Officer is Assistant Superintendent for Business/Finance. The Security Officer is responsible for ensuring the confidentiality, integrity, and availability of all electronic *protected health information* that the OHCA creates, receives, maintains, or transmits.

I. The Notice of Privacy Practices

The Privacy Officer shall prepare and maintain a Notice of Privacy Practices ("Notice") describing the legal duties and privacy practices of the OHCA (or the individual plans which comprise the OHCA) with respect to the protected health information. A copy of the OHCA's current Notice (or a copy of the OHCA member-plan's current Notice) shall be attached to this Policy as Exhibit 1. A copy of the current Privacy Notice(s) as well as a copy of any prior versions of the Privacy Notice(s) shall be retained in accordance with the OHCA's "Documentation" policy and procedure (see Section IV. A. below).

The distribution requirements for the Privacy Notices vary depending on whether the plans, which are members of the OHCA, are fully insured or self-funded. The distribution requirements are as follows:

(1) *Notice of Privacy Practices for the Haysville USD 261 Medical Plan and Haysville USD 261 Dental Plan.* The Privacy Officer shall prepare and maintain a Notice of Privacy Practices for the Haysville USD 261 Medical Plan and the Haysville USD 261 Dental Plan. This Notice only needs to be provided to a participant if the participant requests it. In these instances, the Contact Person shall provide the requested Notice by first class mail, through hand-delivery, or via e-mail.

(2) *Notice of Privacy Practices for the Haysville USD 261 Health Flexible Spending Account.* In addition to the Notice of Privacy Practices described in (1) above, the Privacy Officer shall prepare and maintain a Notice of Privacy Practices for the Haysville USD 261 Health Flexible Spending Account.

The Contact Person shall provide a copy of this Privacy Notice to all employees who are enrolled in the Haysville USD 261 Health Flexible Spending Account or that is part of the OHCA at the time they become covered under the group health plan.

If the Privacy Notice is modified or revised, a copy of the modified or revised Notice shall be provided to all employees enrolled in the plan that is part of the OHCA within 60 days of the modification or revision. The Contact Person shall also provide a copy of the current Privacy Notice upon request to a covered employee or to a person, such as a spouse or dependent, who is covered through the employee.

In lieu of sending out a Reminder Notice every three years, informing covered employees that a Privacy Notice is available, the Contact Person shall provide a copy of this Privacy Notice to all covered employees on an annual basis.

Delivery of the Notice for the USD 261 Health Flexible Spending Account:

Depending on the distribution event, the Privacy Notice will be distributed according to the table below. There are check marks in the columns which indicate a method of delivering the Privacy Notice. If one method of delivery is preferred over another, the methods will be ranked in the table below with numbers, "1" being the most preferred delivery method.

		Distribution Events for the Haysville USD 261 Health Flexible Spending Account			
		Newly Covered Employee (e.g. new hires)	**Material Modification or Revision to Notice**	**Request from Participant**	**Reminder Notice**
Distribution Methods	**First Class Mail**		X	X	n/a
	Hand-Delivery		X	X	n/a
	Interoffice Mail System				n/a
	Pay Stub				n/a
	E-mail		X	X	n/a
	Website (cannot be the only method)				n/a
	With SPD				n/a
	Included in New Hire Packet	X			n/a
	Included with Enrollment Packet				n/a
	Other Method:				n/a

II. Use and Disclosure of Protected Health Information

The Company and the OHCA will use and disclose protected health information only as permitted under HIPAA. If the Company creates, receives, maintains, or transmits any electronic *protected health information* (other than enrollment / disenrollment information and summary health information, which are not subject to restrictions) on behalf of the OHCA, it will implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic *protected health information*, and it will ensure that any agents (including subcontractors) to whom it provides such electronic *protected health information* agree to implement reasonable and appropriate security measures to protect the information. The Company will report any security incident of which it becomes aware.

For purposes of the these policies and procedures, the term "use" means the sharing, utilization, review, examination, or analysis of individually identifiable health information by an Authorized Employee or by a Business Associate (defined in B.2. below) of the OHCA. The term "disclosure" means any release, transfer, provision of access to, or divulging in any other manner of individually identifiable health information to a person other than an Authorized Employee.

A. Use and Disclosure For Treatment, Payment & Health Care Operations

The OHCA is authorized to disclose protected health information to a health care provider for its provision, coordination or management of health care and related services to an individual enrolled in a group health plan that is part of the OHCA. In addition, the OHCA is authorized to disclose protected health information for its own payment purposes as well as to another covered entity for the payment purposes of that covered entity. "Payment" includes activities undertaken to obtain plan contributions or to determine or fulfill the OHCA's responsibility for provision of benefits under the OHCA, or to obtain or provide reimbursement for health care. Payment also includes:

- eligibility and coverage determinations including coordination of benefits and adjudication (e.g., claim administration) or subrogation of health benefit claims;
- risk adjusting based on enrollee status and demographic characteristics; and
- billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess loss insurance) and related health care data processing.

Finally, the OHCA is authorized to disclose protected health information for purposes of the OHCA's own health care operations (if any) and/or to another covered entity for purposes of the other covered entity's quality assessment and improvement, case management, or health care fraud and abuse detection programs.

All disclosures of protected health information for treatment, payment and health care operations as described above must comply with the "Minimum Necessary" standard (see Section IV.D. below) and be documented in accordance with the OHCA's "Documentation" policy and procedure (see Section IV.A. below).

B. Other Permitted Uses and Disclosures of Protected Health Information

In addition to uses and disclosures relating to treatment, payment and health care operations, the OHCA is authorized to disclose protected health information to the Company for plan administration functions, to business associates if certain conditions are first satisfied, and for legal and public policy purposes, as more fully described below.

(1) *Disclosures to Plan Sponsor.* No disclosure shall be made to employees of the Company unless and until the Company amends the plan document and certifies to the Plan, in writing, that it will only use the information in the manner permitted by HIPAA. In addition, any and all disclosures to the Company for plan administration functions must comply with the "Minimum Necessary" standard (see Section IV.D. below).

(2) *Disclosures To Business Associates.* Any and all disclosures or protected health information to a "business associate" must be made in accordance with a valid business associate agreement. A "business associate" is an entity that performs or assists in performing a plan function or activity involving the use and disclosure of protected health information (including claims processing or administration, data analysis, underwriting, etc.) or provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services, where the performance of such services involves giving the service provider access to protected health information. Before providing protected health information to a business associate, Authorized Employees must contact the Privacy Officer and verify that a business associate contract is in place. In addition, any and all disclosures to a business associate must be consistent with the terms of the business associate contract, must comply with the OHCA's "Minimum Necessary" standard (see Section IV.D. below) and must be documented in accordance with the OHCA's "Documentation" policy and procedure (see Section IV.A. below).

(3) *Disclosures for Legal and Public Policy Purposes.* Requests for disclosures of protected health information for the following purposes and/or in response to the following requests must be approved by the Privacy Officer, must comply with the OHCA's "Minimum Necessary" standard (see Section IV.D. below) and must be documented in accordance with the OHCA's "Documentation" policy and procedure (see Section IV.A. below):

- Requests needed to avert a serious threat to the health or safety of an individual or the general public.
- Requests by military command authorities.
- Requests necessary to comply with worker's compensation laws.
- Requests by organizations that handle organ donor procurement or transplantation.
- Requests relating to public health activities.
- Requests by a health oversight organization for activities authorized by law.
- Requests in the form of a court or administrative order, subpoena, discovery request, or other lawful process.
- Requests by law enforcement officials.
- Requests by a coroner, medical examiner or funeral director (as necessary to carry out their duties).

- Requests by federal officials for national security activities authorized by law.

- Requests by correctional institutions.

C. Mandatory Disclosures of Protected Health Information

Subject to the exceptions described in HIPAA, the OHCA shall disclose protected health information when requested by (i) the individual to whom the information relates or (ii) the United States Department of Health and Human Services.

(1) *Request Made By Individual.* Upon receiving a request from an individual (or an individual's representative) for disclosure of the individual's own protected health information, follow the procedure for "Right of Access to Protected Health Information" (see Section III.A. below).

(2) *Request Made by Department of Health and Human Services.* Upon receiving a request from an official of the United States Department of Health and Human Services, follow the procedures for verifying the identity of a public official set forth in the OHCA's "Verification of Identity" policy and procedure (see Section IV.B. below) and document the disclosure in accordance with the OHCA's "Documentation" policy and procedure (see Section IV.A. below).

D. Use and Disclosures Pursuant to Authorizations

The OHCA shall not use or disclose protected health information for any purpose not expressly authorized under paragraphs A, B and C immediately above unless the individual to whom the information relates has provided an authorization for such use or disclosure. If the authorization is requested by the OHCA, the Company, or an individual enrolled in a group health plan that is part of the OHCA, the authorization shall be requested on the "Authorization For Release of Protected Health Information" developed by the OHCA for this purpose, a copy of which is attached hereto as Exhibit 2.

Upon the receipt by the Contact Person of an authorization, whether the same is submitted on the OHCA's "Authorization For Release of Protected Health Information" or otherwise, the Contact Person (or Authorized Employee acting under the direction and supervision of the Contact Person) shall verify the identity of the individual giving the authorization (or individual's representative) in accordance with the OHCA's "Verification of Identity" policy and procedure (see Section IV.B. below) and review the authorization to ensure it is valid. A valid authorization is one that:

- Is signed and dated by the individual or the individual's representative;

- Has not expired or been revoked;

- Contains a description of the information to be used or disclosed;

- Contains the name of the entity or person authorized to use or disclose the protected health information;

- Contains the name of the recipient of the protected health information;

- Contains a statement regarding the individual's right to revoke the authorization and the procedures for revoking authorizations; and

- Contains a statement regarding the possibility for a subsequent re-disclosure of the information.

All uses and disclosures made pursuant to an authorization must be consistent with the terms and conditions of the Authorization and must be documented in accordance with the OHCA's "Documentation" policy and procedure (see Section IV.A. below).

III. Individual Rights

HIPAA confers upon individuals certain rights with respect to their own protected health information that is maintained by or for the OHCA as a "designated record set." Specifically, individuals have the right to inspect and copy their protected health information; to request amendments to their protected health information; to request an accounting of disclosures of their protected health information; to request restrictions on the use and disclosure of protected health information; and to request confidential communications.

A "designated record set" is a group of records that includes the enrollment, payment, and claims adjudication record of an individual maintained by or for the OHCA and all other protected health information used, in whole or in part, by or for the OHCA to make coverage decisions about an individual.

A. Right of Access To Protected Health Information

Subject to the exceptions noted immediately below, individuals have a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set for as long as the information is maintained in the designated record set. However, and notwithstanding the foregoing, individuals do not have a right of access to inspect and obtain a copy of protected health information about the individual when:

- the information is psychotherapy notes;

- the information has been compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative proceeding;

- the information is subject to the Clinical Laboratory Improvements Amendments Act of 1988, 42 U.S.C. 263a, and access to such information is prohibited under such law;

- the information is subject to the Privacy Act, 5 U.S.C. 552a and denial of access satisfies the requirements of that law;

- the information was obtained from someone other than a health care provider under a promise of confidentiality; or

- disclosing the information is determined by a health care professional to be likely to cause harm.

All requests by an individual (or the parent of a minor or a personal representative) for access to that individual's protected health information must be in writing and signed by the individual (or the parent of a minor or a personal representative). The OHCA has developed a "Request For Access to Protected Health Information," a copy of which is attached hereto as Exhibit 3 that should be used whenever possible.

Upon receiving a request from an individual (or from a minor's parent or an individual's personal representative) for access to that individual's protected health information, the Contact Person (or Authorized Employee acting under the direction and supervision of the Contact Person) shall:

(1) Ensure that the request is signed and dated.

(2) Verify the identity of the individual (or parent or personal representative) submitting the request in accordance with the OHCA's "Verification of Identity" policy and procedure (see Section IV.B. below).

(3) Review the request to determine whether the requested information is held in the individual's designated record set. If it appears that the requested information is not held in the individual's designated record set, contact the Privacy Officer. No request for access may be denied without approval from the Privacy Officer.

(4) Review the request to determine whether an exception to the disclosure requirement might exist. If there is any question about whether one of the exceptions applies, contact the Privacy Officer. No request for access may be denied without approval from the Privacy Officer.

(5) Respond to the request, in writing, using the OHCA's "Response to Request For Access to Protected Health Information," a copy of which is attached hereto as Exhibit 4 (the "OHCA's Response"), within 30 days (60 days if the information is maintained off-site). If the requested protected health information cannot be accessed within the 30 day (or 60 day) period, the deadline may be extended for 30 days by providing written notice to the individual within the original 30 or 60 day period of the reasons for the extension and the date by which the Company will respond.

(6) If the request is not valid or is incomplete, indicate on the OHCA's Response the specific information necessary to make the request valid and/or complete and mail the Response to the individual.

(7) If the request is denied, indicate on the OHCA's Response the basis for the denial and mail the Response to the individual. No request for access may be denied without approval from the Privacy Officer.

(8) If the request is granted and the individual requested that the information be mailed to him or her, include the information with the OHCA's Response and mail it to the individual. If the individual did not request that the information be mailed to him or her, the OHCA's Response directs the individual to contact the Contact Person to arrange a mutually convenient time for the individual to review and/or copy the requested information.

All disclosures made under the forgoing procedure must be documented in accordance with the OHCA's "Documentation" policy and procedure (see Section IV.A. below).

The OHCA will not impose cost-based copying and postage charges in connection with fulfilling an individual's request for copies of his or her protected health information.

B. Right to Request Amendment to Protected Health Information

HIPAA gives individuals the right to request to have their protected health information amended. All requests by an individual (or the parent of a minor or a personal representative) for an amendment to that individual's protected health information must be in writing and signed by the individual (or the parent of a minor or a personal representative). The OHCA has developed a "Request to Amend Protected Health Information," a copy of which is attached hereto as Exhibit 5 that should be used whenever possible.

Upon receiving a request from an individual (or a minor's parent or an individual's personal representative) for amendment of an individual's protected health information held in a designated record set, the Contact Person (or Authorized Employee acting under the direction and supervision of the Contact Person) shall:

(1) Follow the procedures for verifying the identity of the individual (or parent or personal representative) in accordance with the OHCA's "Verification of Identity" policy and procedure (see Section IV.B. below).

(2) Review the request to determine whether the protected health information at issue is held in the individual's designated record set. See the Privacy Officer if it appears that the requested information is not held in the individual's designated record set. No request for amendment may be denied without approval from the Privacy Officer.

(3) Review the request for amendment to determine whether the information would be accessible to the individual under paragraph A above. See the Privacy Officer if there is any question about whether one of these exceptions applies. No request for amendment may be denied without approval from the Privacy Officer.

(4) Review the request for amendment to determine whether the amendment is appropriate - that is, determine whether the information in the designated record set is accurate and complete without the amendment.

(5) Respond to the request, in writing, using the OHCA's "Response to Request to Amend Protected Health Information," a copy of which is attached hereto as Exhibit 6 (the "OHCA's Response"), within 60 days. If the determination cannot be made within the 60 day period, the deadline may be extended for 30 days by providing written notice to the individual within the original 60 day period of the reasons for the extension and the date by which the Company will respond.

(6) When a request for amendment is accepted, make the change in the designated record set, and provide appropriate notice to the individual and all persons or entities listed on the individual's amendment request form, if any, and also provide notice of the amendment to any persons/entities who are known to have the particular record and who may rely on the uncorrected information to the detriment of the individual.

(7) When a request for amendment is denied, the OHCA's Response shall be approved by the Privacy Officer. The OHCA's response must set forth (1) the basis for the denial; (2) information about the individual's right to submit a written statement disagreeing with the denial and how to file such a statement; (3) an explanation that the individual may (if he or she does not file a statement of disagreement) request that the request for amendment and its denial be included in future disclosures of the information; and (4) a statement of how the individual may file a complaint concerning the denial. If, following the denial, the individual files a statement of disagreement, include the individual's request for an amendment; the denial notice of the request; the individual's statement of disagreement, if any; and the Company's rebuttal/response to such statement of disagreement, if any, with any subsequent disclosure of the record to which the request for amendment relates. If the individual has not submitted a written statement of disagreement, include the individual's request for amendment and its denial with any subsequent disclosure of the protected health information only if the individual has requested such action.

C. Right to Request Accounting

An individual has the right to obtain an accounting of certain disclosures of his or her own protected health information made after April 14, 2004. This right to an accounting extends to disclosures made in the last six years, other than disclosures:

- to carry out treatment, payment or health care operations; however, if the disclosure involves a disclosure of an electronic record of health-related information on an individual that is created, gathered, managed and consulted by authorized healthcare clinicians and staff, this must be accounted for and records maintained for three (3) years;

- to individuals about their own protected health information;

- incident to an otherwise permitted use or disclosure;

- pursuant to an authorization;

- for purposes of creation of a facility directory or to persons involved in the patient's care or other notification purposes;

- as part of a limited data set; or

- for other national security or law enforcement purposes.

All requests by an individual (or the parent of a minor or a personal representative) for an accounting of disclosures of that individual's protected health information must be in writing and signed by the individual (or the parent of a minor or a personal representative). The OHCA has developed a "Request For Accounting of Disclosures of Protected Health Information," a copy of which is attached hereto as Exhibit 7, that should be used whenever possible.

Upon receiving a request from an individual (or a minor's parent or an individual's personal representative) for an accounting of disclosure of an individual's protected health information, the Contact Person (or Authorized Employee acting under the direction and supervision of the Contact Person) shall:

(1) Follow the procedures for verifying the identity of the individual (or parent or personal representative) in accordance with the OHCA's "Verification of Identity" policy and procedure (see Section IV.B. below).

(2) Respond to the request, in writing, using the OHCA's "Response to Request For Accounting of Disclosures of Protected Health Information," a copy of which is attached hereto as Exhibit 8, within 60 days by enclosing the accounting (as described in more detail below), or informing the individual that there have been no disclosures that must be included in an accounting. If the accounting cannot be provided within the 60 day period, the deadline may be extended for 30 days by providing written notice to the individual within the original 60 day period of the reasons for the extension and the date by which the Company will respond.

(3) The accounting must include disclosures (but not uses) of the requesting individual's protected health information made by the OHCA and any of its business associates during the period requested by the individual up to six years prior to the request. (Note: the OHCA is not required to account for any disclosures made prior to the compliance date.)

(4) If any business associate of the OHCA or a group health plan that is part of the OHCA has the authority to disclose the individual's protected health information, the Contact Person shall request an accounting of disclosure from such business associate.

(5) The accounting must include the following information for each reportable disclosure of the individual's protected health information:

- the date of disclosure;
- the name (and if known, the address) of the entity or person to whom the information was disclosed;
- a brief description of the protected health information disclosed; and
- a brief statement explaining the purpose for the disclosure. (The statement of purpose may be accomplished by providing a copy of the written request for disclosure, when applicable.)

Accountings must be documented in accordance with the OHCA's "Documentation" policy and procedures (see Section IV.A. below).

The OHCA will not impose cost-based charges in connection with the production, copying and mailing of an individual's request for an accounting of disclosures of his or her protected health information.

D. Right to Request Alternative Communications

Individuals may request to receive communications regarding their protected health information by alternative means or at alternative locations. For example, an individual may ask to be called only at work rather than at home. Such requests may be honored if, in the sole discretion of the Company, the requests are reasonable. However, the Company shall accommodate such a request if the individual clearly provides information that the disclosure of all or part of that information could endanger the individual. The Privacy Officer has responsibility for administering requests for confidential communications.

All requests by an individual (or the parent of a minor or a personal representative) for alternative communications must be in writing and signed by the individual (or the parent of a minor or a personal representative). The OHCA has developed a "Request For Confidential Communications," a copy of which is attached hereto as Exhibit 9, that should be used whenever possible.

Upon receiving a request from an individual (or a minor's parent or an individual's personal representative) to receive communications of protected health information by alternative means or at alternative locations, the Contact Person (or Authorized Employee acting under the direction and supervision of the Contact Person) shall:

(1) Follow the procedures for verifying the identity of the individual (or parent or personal representative) in accordance with the OHCA's "Verification of Identity" policy and procedure (see Section IV.B. below).

(2) Determine whether the request contains a statement that disclosure of all or part of the information to which the request pertains could endanger the individual. Requests for confidential and/or alternative communications must be honored by the OHCA if the individual states that disclosure could endanger the individual.

(3) Respond to the request, in writing, using the OHCA's "Response to Request For Confidential Communications," a copy of which is attached hereto as Exhibit 10 and indicate on the OHCA's Response whether the request will be accommodated.

(4) If a request will not be accommodated, the OHCA's Response shall explain why the request cannot be accommodated.

(5) All Requests for Confidential Communications and responses thereto shall be reviewed by the Privacy Officer.

Requests and their dispositions must be documented in accordance with the OHCA's "Documentation" policy and procedure (see Section IV.A. below).

E. Right to Request Restrictions

An individual may request restrictions on the use and disclosure of the individual's protected health information. It is the Company's policy to attempt to honor such requests if, in the sole discretion of the Company, the requests are reasonable.

All requests by an individual (or the parent of a minor or a personal representative) for restrictions on the use and disclosure of the individual's protected health information must be in writing and signed by the individual (or the parent of a minor or a personal representative). The OHCA has developed a "Request For Restrictions to Protected Health Information," a copy of which is attached hereto as Exhibit 11, that should be used whenever possible.

Upon receiving a request from an individual (or a minor's parent or an individual's personal representative) to restrict access to an individual's protected health information, the Contact Person (or Authorized Employee acting under the direction and supervision of the Contact Person) shall:

(1) Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in the "Verification of Identity" policy and procedure (see Section IV.B. below).

(2) Respond to the request, in writing, using the OHCA's "Response to Request For Restrictions to Protected Health Information," a copy of which is attached hereto as Exhibit 12 and indicate on the OHCA's Response whether the request will be accommodated.

(3) If a request will not be accommodated, the OHCA's Response shall explain why the request cannot be accommodated. Note, however, if the request relates to restricting the disclosure of PHI to another health plan and it pertains solely to a health care item or service for which the health care provider has been paid out-of-pocket in full and where the purpose of the disclosure is for carrying out payment or health care operations, the OHCA must agree to the request for restrictions to such PHI.

(4) All Requests for Restrictions to Protected Health Information and responses thereto shall be reviewed by the Privacy Officer.

Requests and their dispositions must be documented in accordance with the OHCA's "Documentation" policy and procedure (see Section IV.A. below).

IV. Administrative Provisions and Safeguards

A. Documentation

The OHCA shall maintain copies of the OHCA's Notice of Privacy Practices and Individual Authorizations for a period of at least six years from the date the documents were created or were last in effect, whichever is later. In addition, when a disclosure of protected health information is made, the Authorized Employees making such disclosure shall indicate on the OHCA's "Disclosure Report" form, a copy of which is attached hereto as Exhibit 13: (i) the date of the disclosure; (ii) the name of the entity or person who received the protected health information and, if known, the address of such entity or person; (iii) a brief description of the information disclosed; (iv) a brief statement of the purpose of the disclosure; and (v) any other documentation required under the Use and Disclosure policies and Procedures (as applicable).

B. Verification of Identity

The OHCA must take steps to verify the identity of individuals who request access to protected health information. The OHCA must also verify the authority of any person to have access to protected health information if the identity or authority of such person is not known. Separate procedures are set forth below for verifying the identity and authority, depending on whether the request is made by the individual, a parent seeking access to the protected health information of his or her minor child, a personal representative, or a public official seeking access.

(1) *Request Made by Individual.* When an individual requests access to his or her own protected health information, unless the Authorized Employee knows from personal experience that the individual is who or she purports to be, the following steps should be followed:

(a) Request a form of identification from the individual. The OHCA will accept a valid driver's license, passport or other photo identification issued by a government agency.

(b) Verify that the identification matches the identity of the individual requesting access to the protected health information. If there is any doubt as to the validity or authenticity of the identification provided or the identity of the individual requesting access to the protected health information, the Privacy Officer should be contacted.

(c) Make a copy of the identification provided by the individual and file it with the individual's designated record set.

(d) If the individual requests protected health information over the telephone, instruct the individual that it is the OHCA's policy that all requests for access to protected health information must be submitted in writing to the Contact Person.

(2) *Request Made by Parent of a Minor Child.* When a parent requests access to the protected health information of the parent's minor child, unless the Authorized Employee knows from personal experience that the individual is the parent of the minor child to whom the information relates, request verification of the person's relationship with the child. Such verification may take the form of confirming enrollment of the child in the parent's plan as a dependent. Make a copy of the documentation provided and file it in the individual's designated record set.

(3) *Request Made by Personal Representative*. When a personal representative requests access to an individual's protected health information, request a copy of appropriate documentation such as a valid power of attorney. If there are any questions about the validity of this document, seek review by the Privacy Officer. Make a copy of the documentation provided and file it in the individual's designated record set.

(4) *Request Made by Public Official.* If a public official requests access to protected health information, and if the request is for one of the purposes set forth above in Section II.B.3. (relating to disclosures for legal and public policy purposes) or Section II.C.2 (relating to disclosures to the Department of Health and Human Services), the following steps should be followed to verify the official's identity and authority:

(a) If the request is made in person, request presentation of an agency identification badge, other official credentials or other proof of government status. Make a copy of the identification provided and file it in the individual's designated record set.

(b) If the request is in writing, verify that the request is on the appropriate government letterhead;

(c) If the request is by a person purporting to act on behalf of a public official, request a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

(d) Request a written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority. If the individual's request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal, contact the Privacy Officer.

(e) Obtain approval for the disclosure from the Privacy Officer.

(5) *Request Made by Spouse, Family Member or Friend.* The OHCA and Company will not disclose protected health information to family and friends of an individual except as required or permitted by HIPAA. The OHCA will not disclose an individual's protected health information to any person, including a spouse, family member or friend, unless the individual to whom the information relates is present (and does not object) or the OHCA or group health plan that is part of the OHCA has received a valid authorization. If the individual to whom the information relates is not present or is not capable of consenting to the disclosure because of the individual's incapacity or emergency circumstances, the OHCA may disclose protected health information to the spouse, family member or friend of an individual, if, in the exercise of professional judgment, the OHCA determines it is in the best interests of the individual to make the disclosure.

If the Contact Person (or Authorized Employee acting under the direction and supervision of the Contact Person) receives a request for disclosure of an individual's protected health information from a spouse, family member, or personal friend of an individual, and the spouse, family member, or personal friend is either (1) the parent of the individual and the individual is a minor child, or (2) the personal representative of the individual, then follow the applicable "Verification of Identity" policy and procedure (see Section IV.B. above). Once the identity of a parent or personal representative is verified, follow the OHCA's "Right of Access to Protected Health Information" policy and procedure (see Section III.A. above). All other requests from spouses, family members, and friends must be authorized by the individual whose protected

health information is involved in accordance with the OHCA's policy and procedures for "Use and Disclosures Pursuant to Authorizations" (see Section II.D. above).

C. Record Storage and Access

The Company is required to establish, on behalf of the OHCA, appropriate technical and physical safeguards to prevent protected health information from intentionally or unintentionally being used or disclosed in violation of HIPAA's requirements. Technical safeguards include limiting access to information by creating computer firewalls. Physical safeguards include locking doors or filing cabinets.

(1) *Physical Safeguards*. All designated records sets shall be maintained separately and secured separately from all employee records. Designated record sets shall not be commingled with employment records of any kind. To ensure that paper files will be safeguarded from unauthorized public view, Authorized Employees shall store designated record sets in locked filing cabinets or in a locked file room. Only Authorized Employees with authorization from the Contact Person or Privacy Officer shall have access to the locked file cabinets and/or locked area. While unattended, the file system will not be left open.

(2) *Technical Safeguards*. Any and all protected health information stored on computers will be password protected. Only Authorized Employees with authorization from the Contact Person or Privacy Officer will have access to any and all of such computer files. Any protected health information copied onto removable media, including backup media, will be protected in the same manner as paper files, as outlined above. Any material that contains protected health information will, while in use, be protected from deliberate or casual oversight by passers-by. Computer screens displaying protected health information will be turned away from public areas so as not to be visible to passers-by in public areas.

(3) *Disposal*. Any and all handwritten notes such as phone messages and reminder slips containing protected health information must be shredded as soon as they are no longer needed. Dictation tapes containing protected health information must be erased after the material is transcribed. All unwanted or duplicate papers containing protected health information must be shredded immediately after it is determined that they are no longer needed. Diskettes containing protected health information must be reformatted when the data is no longer required. Hard drives must be reformatted when an office computer is sold, or when Authorized Employees no longer use it to access protected health information. If they contain protected health information, CDs must be destroyed when the data is no longer required.

D. Minimum Necessary Standard

HIPAA requires that when protected health information is used or disclosed, the amount disclosed generally must be limited to the "minimum necessary" to accomplish the purpose of the use or disclosure. “Minimum necessary” means (1) for electronic information, reviewing, forwarding, or printing out only those fields and records relevant to the user’s need for information, and (2) for non-electronic information, the selective copying of relevant parts of protected health information.

The "minimum necessary" standard does not apply to any of the following:

- uses or disclosures made to the individual;
- uses or disclosures made pursuant to a valid authorization;
- disclosures made to the United States Department of Health and Human Services;
- uses or disclosures required by law; and
- uses or disclosures required to comply with HIPAA.

With respect to requests for information from business associates, the OHCA shall limit the use or disclosure of, and requests for, protected health information to the minimum necessary to accomplish the intended purpose. In addition and whenever possible, the OHCA shall use de-identified information if the purpose of the disclosure could be reasonably accomplished with information that is not identifiable. De-identified information is information with all of the following elements removed:

- Names;
- All geographic subdivisions smaller than a state, except a three-digit zip code may be used under certain circumstances;
- All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social security numbers;

- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code.

The OHCA shall not disclose an individual's entire designated record set unless the request for disclosure includes an explanation of why the purpose of the disclosure could not reasonably be accomplished without the entire designated record set. Similarly, the OHCA shall not disclose an individual's entire designated record set in response to a request for more limited data. In the day-to-day operation of the OHCA and the Company, physical access to protected health information, whether in paper or electronic media, shall be limited to Authorized Employees.

E. Mitigation of Inadvertent Disclosures

HIPAA requires that the OHCA mitigate, to the extent possible, any harmful effects that become known to it of a use or disclosure of an individual's protected health information in violation of this Privacy Policy. As a result, if an Authorized Employee becomes aware of a disclosure of protected health information, either by an Authorized Employee or a business associate of the OHCA or a group health plan that is part of the OHCA, that is not in compliance with the policies and procedures of the OHCA, such Authorized Employee shall immediately contact the Privacy Officer so that the appropriate steps to mitigate any potential harm to the individual can be taken.

F. Employee Training

HIPAA requires that protected health information is protected against unauthorized use or disclosure. To that end, the Company, in its capacity as the plan sponsor, is responsible for training all members of its workforce with respect to its privacy policies and procedures. Specifically, the OHCA must:

- provide training to each member of the workforce who is authorized to have access to protected health information prior to the compliance date;

- provide training to all new employees who will be authorized to have access to protected health information within a reasonable time after they join the workforce;

- provide training to all new employees who may be authorized to have access to protected health information upon the occurrence of an unanticipated or unusual event. Access under these circumstances shall be limited in time and scope. Basic training may be provided within a reasonable time after such employee joins the workforce. Such training shall be followed by any additional training that may be necessary at the time of the unanticipated or unusual event;

- retrain each member of the workforce who is authorized to have access to protected health information when and to the extent that material changes in policies and procedures are made; and

- document the training on the OHCA's "Employee Training Log," a copy of which is attached hereto as Exhibit 14.

(1) *Existing Employee Training*. All existing employees of the Company with access to protected health information will receive a privacy orientation. The employee's supervisor or other trainer will explain the HIPAA privacy regulations as they relate to the employee's job, their importance, and how the Company has responded to these regulations. Each employee with access to protected health information will receive a copy of this Privacy Policy and will be asked to sign a statement indicating that they have read, understand and agree to abide by all policies and procedures set forth in the Privacy Policy, and further understand that the penalties for not following the Privacy Policy could include severe disciplinary action, up to and including termination. The written statement which is entitled "Employee Acknowledgment" and is attached hereto as Exhibit 15, shall be retained by the OHCA.

(2) *New Employee Training*. All new employees of the Company with access to protected health information will receive a privacy orientation. The employee's supervisor or other trainer will explain the HIPAA privacy regulations as they relate to the employee's job, their importance, and how the Company has responded to these regulations. Each new employee with access to protected health information will receive a copy of this Privacy Policy and will be asked to sign the "Employee Acknowledgment" form, which is attached hereto as Exhibit 15, indicating that they have read, understand and agree to abide by all policies and procedures set forth in the Privacy Policy, and further understand that the penalties for not following the Privacy Policy could include severe disciplinary action, up to and including termination.

The Privacy Officer is responsible for ensuring that appropriate education and procedures are in place and enforced to assure senior management that new employees are trained properly regarding privacy and confidentiality and in accordance with our policies and the relevant statutes.

G. Sanctions for Violations of Policies and Procedures

The Company will apply appropriate sanctions against any employee who violates the policies and procedures set forth herein. Authorized Employees are provided training (and retraining as necessary) to ensure they understand all of the policies and procedures that apply to protected health information. Appropriate sanctions for violations of the OHCA's policies and procedures will be determined with reference to the nature of the violation, the severity of the violation and whether the violation was intentional or unintentional. Sanctions may include verbal warnings, written warnings, imposition of probationary periods or termination.

H. Complaints

HIPAA requires that a group health plan create a process for individuals to submit complaints regarding the OHCA's policies and procedures and create a system for handling such complaints. The OHCA's Notice of Privacy Practice and related forms state that if the individual is dissatisfied with the OHCA in regard to the individual's protected health information request, the individual may file a complaint with the Contact Person (who will deliver the complaint to the Privacy Officer) or the Department of Health and Human Services. If an individual exercised his or her right to file a written complaint with the Contact Person, the Privacy Officer, upon receipt of the complaint, shall log the complaint in a separate file maintained exclusively for this purpose. In addition, in response to any such complaint, the Privacy Officer shall:

(1) investigate the complaint and document his or her findings;

(2) document the decision regarding whether a violation actually occurred, and any resolution regarding the alleged violation, regardless of determination;

(3) if a procedure change in policy or procedure is warranted, the Privacy Officer shall implement the necessary changes or modifications, amend the Policy to be consistent with those changes or modifications, and communicate the changes to all Authorized Employees; and

(4) correspond, in writing, with the individual filing the complaint and indicate what, if any, action the OHCA will take with respect to the complaint (such action may include an apology and/or a description of the change in policies or procedures to prevent similar complaints in the future).

If the Privacy Officer is unable to resolve the complaint, the individual should be advised to file a complaint with the Office for Civil Rights of the United States Department of Health and Human Services. The address of the Department varies depending on the location of the individual who wishes to file the complaint. To file a complaint with the OHCA, contact the Assistant Superintendent for Business/Finance at 1745 West Grand Ave., Haysville, KS 67060. All complaints must be submitted in writing. You will not be penalized, or in any other way retaliated against, for filing a complaint with the Office for Civil Rights or with the OHCA.

V. Electronic Security

A. Risk Analysis

The OHCA has developed a "Risk Analysis Worksheet," a copy of which is attached hereto as Exhibit 16. The Worksheet documents the OHCA's electronic security analysis.

The OHCA has no employees. All of the OHCA's functions, including creation and maintenance of its records, are carried out by Authorized Employees of the Company, by business associates of the OHCA, by business associates of a group health plan that is part of the OHCA, or by the insurer. The OHCA does not own or control any of the equipment or media used to create, maintain, receive, and transmit electronic PHI relating to the OHCA, or any of the facilities in which such equipment and media are located. Such equipment, media and facilities are owned or controlled by the Company, its business associates, and the insurer. Accordingly, the Company, its business associates, and the insurer create and maintain all of the electronic PHI relating to the OHCA, own or control all of the equipment, media and facilities used to create, maintain, receive, or transmit electronic PHI relating to the OHCA, and control their employees, agents, and subcontractors who have access to electronic PHI relating to the OHCA. The OHCA has no ability to assess or in any way modify any potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI relating to the OHCA. That ability lies solely with the Company, its business associates, and the insurer.

Because the OHCA has no access to or control over the employees, equipment, media, facilities, policies, procedures, or documentation of the Company and its business associates affecting the security of electronic PHI relating to the OHCA, and the Company and its business associates have undertaken certain obligations relating to the security of electronic PHI that they handle in relation to the performance of administration functions for the OHCA, the OHCA's policies and procedures, including this Policy, do not address the following standards (including the implementation specifications associated with them) established under HIPAA and are set out in Subpart C of 45 CFR Part 164:

- security management process;
- workforce security;
- information access management;
- security awareness and training;
- security incident procedures;
- contingency plan;
- evaluation;
- facility access controls;

- workstation use;
- workstation security;
- device and media controls;
- access control;
- audit controls;
- integrity;
- person or entity authentication; and
- transmission security.

B. Plan Document

The plan document shall include provisions requiring the Company to:

(1) implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that the Company creates, receives, maintains, or transmits on behalf of the group health plans that are part of the OHCA (the OHCA's electronic PHI);

(2) ensure that reasonable and appropriate security measures support the plan document provisions providing for adequate separation between the OHCA and the Company;

(3) ensure that any agents or subcontractors to whom the Company provides electronic PHI agree to implement reasonable and appropriate security measures to protect the OHCA's electronic PHI; and

(4) report to the Security Officer any security incident of which the Company becomes aware.

C. Disclosures of Electronic PHI to Business Associates

In the future, the OHCA may permit one or more business associates to create, receive, maintain, or transmit electronic PHI on its behalf only if the OHCA or the group health plan that is part of the OHCA first obtains satisfactory assurances from the business associate that it will appropriately safeguard the information, pursuant to 45 C.F.R. Parts 160 and 164. Such satisfactory assurances shall be documented through a written contract providing that the business associate will:

(1) implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that the business associate creates, receives, maintains, or transmits on behalf of the OHCA or the group health plan that is part of the OHCA;

(2) ensure that any agents or subcontractors to whom the business associate provides electronic PHI enter into a contractual arrangement with the business associate in which they agree to implement reasonable and appropriate security measures to protect the electronic PHI;

(3) immediately report to the OHCA or the group health plan that is part of the OHCA any security incident of which the business associate becomes aware; and

(4) authorize termination of the contract by the OHCA or the group health plan that is part of the OHCA if the OHCA or the group health plan that is part of the OHCA determines that the business associate has violated a material term of the contract.

D. Documentation

The OHCA's security policies and procedures shall be documented, reviewed periodically, and updated as necessary in response to environmental or operational changes affecting the security of the OHCA's electronic PHI, and any changes to policies or procedures will be documented promptly.

Except to the extent that they are carried out by the Company, business associates, or the insurer, the OHCA shall document certain actions, activities, and assessments with respect to electronic PHI required by HIPAA to be documented (including amendment of the plan document in accordance with this policy, for example).

Policies, procedures, and other documentation controlled by the OHCA may be maintained in either written or electronic form. The OHCA will maintain such documentation for at least six years from the date of creation or the date last in effect, whichever is later.

The OHCA will make its policies, procedures, and other documentation available to the Security Officer and the Company, as well as business associates or other persons responsible for implementing the procedures to which the documentation pertains.

VI. Breach Notifications

The OHCA will comply with the requirements of the Health Information Technology for Economic and Clinical Health ("HITECH") Act and its implementing regulations to provide notification to affected individuals, HHS and the media (when required) if the OHCA or one of its business associates discovers a Breach of Unsecured PHI.

A. Definitions of Breach / Unsecured PHI

(1) *"Breach"* means the unauthorized acquisition, access, use, or disclosure of Protected Health Information which compromises the security or privacy of such Protected Health Information. The following three types of unauthorized acquisition, access, use, or disclosure are excluded from the definition of a Breach:

(a) Any unintentional acquisition, access, or use of PHI by an employee or individual acting under the authority of the OHCA if such acquisition, access, or use was made in good faith and within the course and scope of employment or other professional relationship of such employee or individual with the OHCA, and the information is not further acquired, accessed, used, or disclosed by any person in a manner not permitted by the Privacy and/or Security Rules;

(b) Any inadvertent disclosure from an individual who is otherwise authorized to access PHI at a facility operated by the OHCA to another similarly situated individual at the same facility so long as the information received is not further used or disclosed in a manner not permitted by the Privacy and/or Security Rules; and

(c) Any disclosure to an unauthorized person where the PHI that was disclosed would not reasonably have been retained by such person.

(2) *"Unsecured Protected Health Information"* means Protected Health Information that is not secured through the use of a technology or methodology specified by the Secretary of Health and Human Services ("HHS") through guidance issued by the Secretary.

B. Breach Determination and Risk Analysis

(1) *Breaches by a Business Associate.* Under the HITECH Act, a business associate must timely notify the OHCA or the group health plan that is part of the OHCA if it discovers or should have discovered (using reasonable diligence) a Breach of Unsecured PHI. If a business associate informs the OHCA or the group health plan that is part of the OHCA that it has discovered a Breach of Unsecured PHI, the OHCA or the group health plan that is part of the OHCA will consult the business associate agreement which is in place with the business associate in question in order to determine if the business associate agreed to make any of the notifications on behalf of the OHCA or the group health plan that is part of the OHCA to individuals, HHS or, if applicable, the media. To the extent that the business associate did *not* agree to make the necessary notifications to affected individuals, the OHCA or the group health plan that is part of the OHCA will make such notification(s) in accordance with VI.C.(1), (2) and/or (3) below.

(2) *Breaches by the OHCA.* The OHCA will perform a risk assessment to determine if a Breach of Unsecured PHI has occurred. The acquisition, access, use, or disclosure of PHI in an impermissible manner is presumed to be a Breach unless the OHCA can demonstrate that there is a low probability that the PHI has been compromised based on a risk assessment as set forth in 45 C.F.R. 164.402(2). The "Breach Determination – Risk Assessment: (Exhibit 17) shall be used to perform this analysis. If it is determined that there is a Breach of Unsecured PHI, certain notifications need to be made to individuals, HHS, and potentially, the media. These notifications shall be made in accordance with VI.C.(1), (2) and/or (3) below.

C. Breach Notifications

If, after performing a risk assessment, it is determined that a Breach of Unsecured PHI has occurred, the OHCA will notify the following parties, as applicable:

(1) *Individuals.* All individuals whose Unsecured PHI has been or is reasonably believed by the OHCA to have been accessed, acquired, used, or disclosed as a result of a Breach of Unsecured PHI shall be notified of the Breach without unreasonable delay and in no case later than 60 calendar days after the Breach is discovered (or should have been discovered through exercising reasonable diligence).

The notification shall include, to the extent possible, the following:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
- A description of the types of Unsecured PHI involved in the Breach (such as whether the full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
- Any steps individuals should take to protect themselves from potential harm resulting from the Breach;
- A brief description of what the OHCA is doing to investigate the Breach, to mitigate harm to individuals, and to protect against further Breaches; and
- Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, email address, website, or postal address.

The notification shall be written in plain, easy-to-understand language. The written notification shall be sent by 1st class mail to the individual at his/her last known address. If the individual agrees to electronic notice and has not withdrawn such agreement, the notification may be sent via electronic mail. One or more mailings may be made as additional information becomes available.

If the OHCA knows that the individual is deceased and has the address of the next of kin or personal representative, written notification by 1st class mail to either the next of kin or personal representative of the individual.

If there is insufficient or out-of-date contact information which would prevent the OHCA from making the proper notification, a substitute form of notice which is reasonably calculated to reach the individual shall be provided. A substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative. If there is insufficient or out-of-date contact information for fewer than 10 individuals, then such substitute notice may be provided by an alternative form of written notice, telephone or other means.

(2) *Media.* The media need only be notified if the Breach of Unsecured PHI involved more than 500 residents of a State or jurisdiction. If more than 500 residents of a State or jurisdiction are involved, the OHCA will notify prominent media outlets serving that State or jurisdiction of the Breach. This notification will be provided without unreasonable delay and in no case later than 60 calendar days after discovery of the Breach.

(3) *HHS.* If there is a Breach of Unsecured PHI the Secretary of HHS will be notified. The timing of this notification and the type of notification depend on whether or not the Breach involved 500 or more individuals, as follows:

(a) *Breaches Involving 500 or More Individuals.* If a Breach of Unsecured PHI involves 500 or more individuals, the OHCA will notify the Secretary of HHS at the same time the individual notice is given. The manner for notifying the Secretary is set forth on the HHS website.

(b) *Breaches Involving Less than 500 Individuals.* If a Breach of Unsecured PHI involves less than 500 individuals, the OHCA will maintain a log or other documentation of the Breaches and notify the Secretary of HHS of these Breaches within 60 days after the end of the calendar year in which the Breaches were discovered. The OHCA will consult the HHS website for instructions for submitting the notification. A log for keeping track of Breaches is found behind Exhibit 18 to these Policies and Procedures.

D. Law Enforcement Delay

The OHCA must temporarily delay any notification if it is instructed by a law enforcement official to delay notification. The law enforcement official must provide a written statement justifying the delay and indicating a time period for the delay. For example, a delay may be necessary if the required notification would impede a criminal investigation. If only an oral statement is provided by the law enforcement official, the OHCA must document the statement and the identity of the official. The maximum period of delay where only an oral statement has been given is 30 days.