Geneseo CUSD #228 **Health Care Plan**

PLAN SPONSOR POLICIES AND PROCEDURES

FOR SEPARATION OF THE PLAN AND THE PLAN SPONSOR, FOR FIREWALLS AND EMPLOYEE ACCESS AND FOR NOTIFICATION OF BREACH OF UNSECURED PHI

The Plan Sponsor and the Plan Administrator hereby adopt the following Policies and Procedures which shall be instituted and followed by the Plan Sponsor, both in its capacity as an employer and as the Plan Sponsor of the Plan, and by the Plan:

1. **Defined Terms.** The following terms shall have the meanings set forth below when used in this document:

"Breach" shall mean the acquisition, access, use, or disclosure of protected health information in a manner not permitted under the privacy standards which compromise the security or privacy of the protected health information of HIPAA.

"HIPAA" shall mean the Health Insurance Portability and Accountability Act of 1996, as amended.

"Individual" shall mean the person who is the subject of PHI.

"Plan Sponsor" shall mean the Plan Sponsor designated by the Plan.

"Plan Administrator" shall mean the Plan Sponsor of the Plan.

"Plan" shall mean the plan referenced above.

"Privacy Official" shall mean the individual appointed as such by the Plan Administrator.

"Privacy Standards" shall mean the Standards for Privacy of Individually Identifiable Health Information enacted pursuant to HIPAA.

"Protected Health Information" or "PHI" shall mean individually identifiable health information, as more specifically defined in the Privacy Standards.

"TPO" shall mean treatment, payment and health care operations, as more specifically defined in the Privacy Standards.

"Unsecured PHI" shall mean PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5 on the HHS Web site.

2. **Compliance Policy.** The Plan and the Plan Sponsor at all times shall comply with the Privacy Standards, and specifically, shall ensure that there exists adequate separation between the Plan and the Plan Sponsor, as required in §164.504(f)(2)(iii) of the Privacy Standards. In addition, the Plan shall make reasonable efforts to limit access to PHI to those individuals in the Plan Administrator's workforce who require access to PHI to carry out their duties and job responsibilities and, further, to limit their access to only the category or categories of PHI to which access is needed, upon any conditions appropriate to such access. In the event the Privacy Standards are amended, these Policies and Procedures shall be deemed to be amended in accordance therewith.

3. **Persons with Access to PHI.** Individuals, including their clerical support staff, who are involved with Plan administration, supervision or management, shall be given access to the PHI.

4. **Restrictions on Use.** The above persons must be advised that (a) PHI may not be used or disclosed for any purpose other than those related to treatment, payment and health care operations (each, as defined in the Privacy Standards) activities under the Plan; (b) PHI may not be used or disclosed in connection with any

employee benefit or employee benefit plan other than the Plan, unless proper authorization is first obtained; (c) PHI must not be used or disclosed for any employment-related decisions, such as hiring, promotions or terminations; and (d) PHI may not be used or disclosed for any employment-related decisions, such as leaves of absence, drug testing and compliance with the Americans with Disabilities Act, unless proper authorization is first obtained.

5. Firewalls. The Plan Sponsor and Plan Administrator shall review the following checklist and establish and maintain firewalls and restrictions on employee access to PHI, as set forth below:

- Review and limit access to PHI to those employees not described above.
- Locate PHI in a place and manner which eliminates unauthorized access.
- Mark PHI as PHI to the extent possible to lessen the likelihood of inadvertent review by unauthorized personnel.
- Prohibit computers containing PHI from being left unattended and accessible to individuals not authorized to access PHI.
- Destroy or discard unneeded PHI in a manner that prohibits its review by unauthorized personnel.
- Take precautions to limit PHI information received by fax to authorized individuals.
- Train employees with employment related functions and Plan related functions of their duty to not use PHI for employment related decisions.

The Plan Sponsor and Plan Administrator shall take steps to ensure that it meets all of the requirements set forth in the above checklist, and the Privacy Official shall monitor this compliance on an on-going basis.

6. Unauthorized Use. Plan PHI may not be used for employment related functions or in connection with any other benefit or benefit plans of the Plan Sponsor.

7. Notification to individuals. (a)(1) *General rule*. The Plan shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the Plan to have been, accessed, acquired, used, or disclosed as a result of such breach. (2) *Breaches treated as discovered.* For purposes of paragraph (a)(1), a breach shall be treated as discovered by the Plan as of the first day on which such breach is known to the Plan, or, by exercising reasonable diligence would have been known to the Plan. The Plan shall be deemed to have knowledge of a breach if such breach is known, or be exercising reasonable due diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the Plan Administrator (determined in accordance with the federal common law of agency).

(b) *Timeliness of notification.* The Plan shall provide the notification required by paragraph (a) without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

(c) *Content of notification.* The notification required by paragraph (a) shall include, to the extent possible: (1) a brief description of what happened, including the date of the breach and the date of the discovery of the breach , if known; (2) a description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved); (3) any steps individuals should take to protect themselves from potential harm resulting from the breach; (4) a brief description of what the Plan involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and (5) contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, website, or postal address.

(d) *Methods of Individual Notification.* The notification required by paragraph (a) shall be provided in the following form: (1) *Written notice.* (i) Written notification by first-class mail to the individual at the last known

address of the individual, or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as information is available. (ii) If the Plan knows the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by first-class mail to either the next of kin or personal representative of the individual. The notification may be provided in one or more mailings as information is available. (2) *Substitute notice.* In the case in which there is insufficient or out-of-date contact information that precludes written notification to the individual under paragraph (d)(1)(i), a substitute form of notice reasonably calculated to reach the individual shall be provided. 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 of the individual. (i) in the case in which 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. (ii) in the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall: (A) be in the form of either a conspicuous posting for a period of 90 days on the home page of the website of the Plan or Plan Administrator, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and (B) Include a toll-free number that remains active for at least 90 days where an individual can learn whether the individual's unsecured protected health information may be included in the breach. (3) *Additional notice in urgent situations.* In any case deemed by the Plan to require urgency because of possible imminent misuse of unsecured protected health information, the Plan may provide information to individuals by telephone or other means, as appropriate, in addition to notice provided under this section.

8. Notification to the Media. (a) *Notification.* For a breach of unsecured protected health information involving more than 500 residents of a State or jurisdiction, the Plan shall, following the discovery of the breach, notify prominent media outlets serving the State or jurisdiction. (b) *Timeliness of notification.* Except as provided in the regulations, the Plan shall provide the notification required by paragraph (a) of section 7 without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

9. Notification to the Secretary. (a) *Notification.* The Plan shall, following the discovery of a breach of unsecured protected health information, notify the Secretary of Health and Human Services. (b) *Breaches involving 500 or more individuals.* For breaches of unsecured protected health information involving 500 or more individuals, the Plan shall, provide the notification required by paragraph (a) contemporaneously with the notice required by Section 7(a) and in the manner specified on the HHS Web site. (c) *Breaches involving less than 500 individuals.* For breaches of unsecured protected health information involving less than 500 individuals, the Plan shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification required by paragraph (a) for breaches occurring during the preceding calendar year, in the manner specified on the HHS Web site.

10. Notification by a Business Associate. (a) *Standard.* (1) A business associate shall, following the discovery of a breach of unsecured protected health information, notify the Plan of such breach. (2) *Breaches treated as discovered.* For purposes of paragraph (1), a breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the federal common law of agency). (b) *Timeliness of notification.* A business associate shall provide the notification required by paragraph (a) without reasonable delay and in no case later than 60 calendar days after discovery of a breach. (c) *Content of notification.* (1) The notification required by paragraph (a) shall include, to the extent possible, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach. (2) A business associate shall

provide the Plan with any other available information that the Plan is required to include in notification to the individual at the time of the notification required by paragraph (a) or promptly thereafter as information becomes available.

11. Law Enforcement Delay. If a law enforcement official states to the Plan or business associate that a notification, notice, or posting required under this policy would impede a criminal investigation or cause damage to national security, the Plan or business associate shall: (a) if the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or (b) if the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in paragraph (a) is submitted during that time.

12. Training. The Plan Administrator must train all members of its workforce on these policies and procedures, as necessary and appropriate for the members of the workforce to carry out their functions with the Plan.

13. Specific Procedures for Compliance – Internal Complaints; Mitigation. Any complaints by Individuals regarding non-compliance with the Plan's privacy policies and procedures provided herein shall be directed to the contact person specified in the Notice of Privacy Practices provided to all individuals covered by the Plan. The Plan shall keep a written record of all written and oral complaints received and a brief explanation of their disposition. The Plan shall be responsible for (a) investigating any complaints (for example, by interviews or review of relevant documents); (b) mitigating, to the extent practicable, any harmful effect that is known to the Plan Administrator of a use or disclosure of PHI in violation of these Policies and Procedures or the Privacy Standards; and (c) resolving any complaints, including, if necessary, by making changes to the Plan's privacy policies and procedures. A written explanation of the disposition of each complaint shall be furnished to the Individual who made the complaint within thirty (30) days of receipt of the complaint. The Plan will not retaliate against any Individual for filing a complaint.

14. Specific Procedures for Compliance – Sanctions. The following sanctions shall be imposed against any employee of the Plan Administrator who breaches the foregoing privacy policies and procedures:

1st offense:	Oral warning
2nd offense:	Written warning
3rd offense:	Three (3) days' suspension without pay
4th offense:	Termination of employment

Notwithstanding the above, the Privacy Official shall have the authority, after consultation with senior management of the Plan Administrator, to impose a greater sanction if the Privacy Official believes that it is called for by the severity of the violation. All sanctions imposed shall be documented in the employee's personnel file. Further, documentation of any sanctions imposed shall be maintained as required by the Privacy Standards.

Approved and Adopted By:

_____

Effective Date: February 17, 2010