HIPAA PRIVACY POLICY

Introduction

The Illinois Educators Risk Management Program Association (the "Association") sponsors the Illinois Educators Risk Management Program Group Health Plan (the "Plan").

Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) the Plan is considered to be a “covered entity.” Members of the Association or its participating Employers workforce may have access to the individually identifiable health information of Plan participants (1) on behalf of the Plan; or (2) on behalf of the Association or Employer, for administrative functions of the Plan.

HIPAA as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act and its implementing regulations restrict the Association's and Employer’s ability to use and disclose protected health information (PHI).

Protected Health Information. Protected health information means information that is created or received by the Plan and relates to the past, present, or future physical or mental health or condition of a participant; the provision of health care to a participant; or the past, present, or future payment for the provision of health care to a participant; and that identifies the participant or for which there is a reasonable basis to believe the information can be used to identify the participant. Protected health information includes information of persons living or deceased.

It is the Association's and Employers' policy to comply fully with HIPAA’s requirements for the privacy of PHI. To that end, all members of the workforce of these entities who have access to PHI must comply with this Privacy Policy. For purposes of this Policy and the Association's and Employers' more detailed use and disclosure procedures, the Association's and Employers' workforce includes individuals who would be considered part of the workforce under HIPAA such as employees, volunteers, trainees, and other persons whose work performance is under the direct control of the Association or an Employer, whether or not they are paid by the Association or an Employer. The term “employee” includes all of these types of workers. Additionally, any subcontractors that provide services to the Association or an Employer, which involve the creation, receipt, maintenance, or transmission of private health information on behalf of the Association or an Employer to fulfill its contractual duties, must comply fully with HIPAA’s requirements.

No third party rights (including but not limited to rights of Plan participants, beneficiaries, covered dependents, or business associates) are intended to be created by this Policy. The Association reserves the right to amend or change this Policy at any time (and even retroactively) without notice. To the extent this Policy establishes requirements and obligations above and beyond those required by HIPAA, the Policy shall be aspirational and shall not be binding upon the Plan, the Association, or an Employer. This Policy

does not address requirements under other federal laws or under state laws. To the extent that this policy is in conflict with the HIPAA privacy rules, the HIPAA privacy rules shall govern.

This policy shall apply to all business associates of the Plan, including Health Alliance. However, Health Alliance may use its own forms and security policies and procedures, provided such forms, policies, and procedures comply with the HIPAA privacy and security requirements.

Plan's Responsibilities as Covered Entity

I. Privacy Officer and Contact Person

The Association designates Lori Eisenmenger as the initial Privacy Officer.

The Privacy Officer will be responsible for the development and implementation of policies and procedures relating to privacy, including but not limited to this Privacy Policy and the Employer's more detailed use and disclosure procedures. The Privacy Officer will also appoint those employees who will serve as the contact persons for participants who have questions, concerns, or complaints about the privacy of their PHI.

The Privacy Officer is responsible for ensuring that the Plan complies with the provisions of the HIPAA privacy rules regarding business associates, including the requirement that the Plan have a HIPAA-compliant Business Associate Agreement in place with all business associates. The Privacy Officer shall also be responsible for monitoring compliance by all business associates with the HIPAA privacy rules and this Privacy Policy.

II. Workforce Training

It is the Association's policy to train all members of its workforce on its privacy policies and procedures. The Privacy Officer is charged with developing training schedules and programs so that all workforce members receive the training necessary and appropriate to permit them to carry out their functions within the Plan in compliance with HIPAA.

III. Administrative, Technical and Physical Safeguards and Firewall

The Association will establish on behalf of the Plan appropriate administrative, technical and physical safeguards to prevent PHI from intentionally or unintentionally being used or disclosed in violation of HIPAA's requirements. Administrative safeguards include implementing procedures for use and disclosure of PHI. See the Plan's Privacy Use and Disclosure Procedures. Technical safeguards include limiting access to information by creating computer firewalls. Physical safeguards include locking doors or filing cabinets.

Firewalls will ensure that only authorized employees will have access to PHI, that they will have access to only the minimum amount of PHI necessary for plan administrative

functions, and that they will not further use or disclose PHI in violation of HIPAA's privacy rules.

IV. Privacy Notice

The Privacy Officer is responsible for developing and maintaining a notice of the Plan's privacy practices that describes:

- the uses and disclosures of PHI that may be made by the Plan;
- the individual's rights under the HIPAA privacy rules;
- the Plan's legal duties with respect to the PHI; and
- other information as required by the HIPAA privacy rules.

The privacy notice will inform participants that the Association and Employers will have access to PHI in connection with its plan administrative functions. The privacy notice will also provide a description of the Plan's complaint procedures, the name and telephone number of the contact person for further information, and the date of the notice.

The notice of privacy practices will be individually delivered:

- at the time of an individual's enrollment in the Plan;
- to a person requesting the notice; and
- within 60 days after a material change to the notice.

The Plan will also provide notice of availability of the privacy notice (or a copy of the privacy notice) at least once every three years in compliance with the HIPAA privacy regulations.

V. Complaints

The Privacy Officer will be the Plan's contact person for receiving complaints.

The Privacy Officer is responsible for creating a process for individuals to lodge complaints about the Plan's privacy procedures and for creating a system for handling such complaints. A copy of the complaint procedure shall be provided to any participant upon request.

VI. Sanctions for Violations of Privacy Policy

Sanctions for using or disclosing PHI in violation of HIPAA or this HIPAA Privacy Policy will be imposed in accordance with the Association's and applicable Employer's discipline policy, up to and including termination.

VII. Mitigation of Inadvertent Disclosures of Protected Health Information

The Plan shall mitigate, to the extent possible, any harmful effects that become known to it of a use or disclosure of an individual's PHI in violation of HIPAA or the policies and

procedures set forth in this Policy. As a result, if an employee or a Plan representative becomes aware of a disclosure of protected health information, either by an employee, representative, or a business associate the employee or the business associate, that is not in compliance with this policy or HIPAA, the employee or representative, should immediately contact the Privacy Officer so that the appropriate steps to mitigate the harm to the participant can be taken.

VIII. No Intimidating or Retaliatory Acts; No Waiver of HIPAA Privacy

No employee or representative 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 under the Plan.

IX. Plan Documents

Plan documents shall include provisions to describe the permitted and required uses and disclosures of PHI by the Association or an Employer for plan administrative purposes or other permitted purposes. Specifically, Plan documents shall require the Employer to:

- not use or further disclose PHI other than as permitted by the Plan documents or as required by law;
- ensure that any agents or subcontractors to whom it provides PHI received from the Plan agree to the same restrictions and conditions that apply to the Employer;
- not use or disclose PHI for employment-related actions or in connection with any other employee benefit plan;
- report to the Privacy Officer any use or disclosure of the information that is inconsistent with the permitted use or disclosure and, if necessary, report such use or disclosure to the Department of Health and Human Services (HHS),as required by HITECH and subsequent regulations;
- make PHI available to Plan participants, consider their amendments and, upon request, provide them with an accounting of PHI disclosures in accordance with HIPAA privacy rules;
- make the Employer's internal practices and records relating to the use and disclosure of PHI received from the Plan available to HHS upon request;
- if feasible, return or destroy all PHI received from the Plan that the Employer still maintains in any form and retain no copies of such information when no longer

needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible: and

- provide access to electronic PHI to an individual or his/her designee.

The Plan documents must also require the Employer to (1) certify to the Privacy Officer that the Plan documents have been amended to include the above restrictions and that the Employer agree to those restrictions; and (2) provide adequate firewalls in compliance with the HIPAA privacy rules.

X. Documentation

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

The Plan shall document certain events and actions (including authorizations, requests for information, sanctions, and complaints) relating to an individual's privacy rights.

If a change in law impacts the privacy notice, the privacy policy must promptly be revised and made available. Such change is effective only with respect to PHI created or received after the effective date of the notice.

The documentation of any policies and procedures, actions, activities and designations may be maintained in either written or electronic form. The Plan must maintain such documentation for at least six years.

Policies on Use and Disclosure of PHI

I. Use and Disclosure Defined

The Association, applicable Employer and the Plan will use and disclose PHI only as permitted under HIPAA. The terms "use" and "disclosure" are defined as follows:

- *Use.* The sharing, employment, application, utilization, examination, or analysis of individually identifiable health information by any person representing the Association, working for or within the benefits department of the Employer, or by a Business Associate (defined below) of the Plan.

- *Disclosure.* For information that is PHI, disclosure means any release, transfer, provision of access to, or divulging in any other manner of individually identifiable health information to persons not representing the Association, employed by or working within the Human Resources Department of the Employer, or not a Business Associate (defined below) of the Plan.

II. Workforce Must Comply With Plan's Policy and Procedures

All representatives of the Association and members of the Employer's workforce (described at the beginning of this Policy and referred to herein as "employees") who has access to Plan PHI must comply with this Policy and with the Plan's more detailed use and disclosure procedures, which are set forth in a separate document.

III. Access to PHI Is Limited to Certain Employees

The following employees ("employees with access") have access to PHI:

- Any employee who performs functions directly on behalf of the Plan; and

- Any employee of a Business Associate who has access to PHI on behalf of the Business Associate for its use in "plan administrative functions" of the covered entities.

The same employees may be named or described in both of these two categories. These employees with access may use and disclose PHI for plan administrative functions, and they may disclose PHI to other employees with access for plan administrative functions (but the PHI disclosed must be limited to the minimum amount necessary to perform the plan administrative function). Employees with access may not disclose PHI to employees (other than employees with access) unless an authorization is in place or the disclosure otherwise is in compliance with this Policy and any associated procedures.

IV. Permitted Uses and Disclosures for Plan Administration Purposes

The Plan may disclose to the Association or an Employer for its use the following: (a) de-identified health information relating to plan participants; (b) Plan enrollment information; (c) summary health information for the purposes of obtaining premium bids for providing health insurance coverage under the Plan or for modifying, amending, or terminating the Plan; or (d) PHI pursuant to an authorization from the individual whose PHI is disclosed.

The Plan may disclose PHI to the following employees who have access to use and disclose PHI to perform functions on behalf of the Plan or to perform plan administrative functions ("employees with access"):

- Any employee who performs functions directly on behalf of the Plan; and

- Any other Association representative or employee who has access to PHI on behalf of the Association or Employer for its use in "plan administrative functions."

The same employees may be named or described in both of these two categories. These employees with access may use and disclose PHI for plan administrative functions, and they may disclose PHI to other employees with access for plan administrative functions (but the PHI disclosed must be limited to the minimum amount necessary to perform the plan administrative function). Employees with access may not disclose PHI to employees (other than employees with access) unless an authorization is in place or the disclosure otherwise is in compliance with this Policy and the more detailed use and disclosure procedures. For purposes of this Policy, "plan administrative functions" include the payment and health care operation activities described in this section of this Policy.

V. Permitted Uses and Disclosures: Payment and Health Care Operations

The Plan may disclose to the Association or Employer for the Plan's own payment purposes, and PHI may be disclosed to another covered entity for the payment purposes of that covered entity.

Payment. Payment includes activities undertaken to obtain Plan contributions or to determine or fulfill the Plan's responsibility for provision of benefits under the Plan, or to obtain or provide reimbursement for health care. Payment also includes:

- eligibility and coverage determinations including coordination of benefits and adjudication or subrogation of health benefit claims;

- risk adjusting based on enrollee status and demographic characteristics;

- 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; and

- any other payment activity permitted by the HIPAA privacy regulations.

PHI may be disclosed for purposes of the Plan's own health care operations. PHI may be disclosed 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, if the other covered entity has (or had) a relationship with the participant and the PHI requested pertains to that relationship.

Health Care Operations. Health care operations means any of the following activities to the extent that they are related to Plan administration:

- conducting quality assessment and improvement activities;

- reviewing health plan performance;

- underwriting and premium rating;

- conducting or arranging for medical review, legal services and auditing functions;
- business planning and development;
- business management and general administrative activities;
- to de-identify the information in accordance with HIPAA Rules as necessary; and
- any other payment activity permitted by the HIPAA privacy regulations.

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

PHI may not be used or disclosed for the payment or operations of the Association's or Employers' "non-health" benefits (e.g., disability, workers' compensation, life insurance, etc.), unless the participant has provided an authorization for such use or disclosure (as discussed in "Disclosures Pursuant to an Authorization") or such use or disclosure is required by applicable state law and particular requirements under HIPAA are met.

VII. Mandatory Disclosures of PHI: to Individual and HHS

A participant's PHI must be disclosed as required by HIPAA in three situations:

- The disclosure is to the individual who is the subject of the information (see the policy for "Access to Protected Information and Request for Amendment" that follows);
- The disclosure is required by law, or
- The disclosure is made to HHS for purposes of enforcing of HIPAA.

VIII. Other Permitted Disclosures of PHI

PHI may be disclosed in the following situations without a participant's authorization, when specific requirements are satisfied. The requirements include prior approval of the Privacy Officer. Permitted are disclosures—

- about victims of abuse, neglect or domestic violence;
- for treatment purposes;
- for judicial and administrative proceedings;
- for law enforcement purposes;
- for public health activities;

- for health oversight activities;
- about decedents;
- for cadaveric organ, eye or tissue donation purposes;
- for certain limited research purposes;
- to avert a serious threat to health or safety;
- for specialized government functions; and
- that relate to workers' compensation programs.

IX. Disclosures of PHI Pursuant to an Authorization

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

X. Complying With the "Minimum-Necessary" Standard

HIPAA requires that when PHI is used or disclosed, the amount disclosed generally must be limited to the "minimum necessary" to accomplish the purpose of the use or disclosure.

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 HHS;
- uses or disclosures required by law; and
- uses or disclosures required to comply with HIPAA.

Minimum Necessary When Disclosing PHI. The Plan, when disclosing PHI subject to the minimum necessary standard, shall take reasonable and appropriate steps to ensure that only the minimum amount of PHI that is necessary for the requestor is disclosed. More details on the requirements are found in the Plan's Privacy Use and Disclosure Procedures. All disclosures not discussed in the Plan's Privacy Use and Disclosure Procedures must be reviewed on an individual basis with the Privacy Officer

to ensure that the amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure.

Minimum Necessary When Requesting PHI. The Plan, when requesting PHI subject to the minimum-necessary standard, shall take reasonable and appropriate steps to ensure that only the minimum amount of PHI necessary for the Plan is requested. More details on the requirements are found in the Plan's Privacy Use and Disclosure Procedures. All requests not discussed in the Plan's Privacy Use and Disclosure Procedures must be reviewed on an individual basis with the Privacy Officer to ensure that the amount of information requested is the minimum necessary to accomplish the purpose of the disclosure.

XI. Disclosures of PHI to Business Associates

Employees may disclose PHI to the Plan's business associates and allow the Plan's business associates to create or receive PHI on its behalf. However, prior to doing so, the Plan must first obtain assurances from the business associate that it will appropriately safeguard the information. Before sharing PHI with outside consultants or contractors who meet the definition of a "business associate," employees must contact the Privacy Officer and verify that a business associate contract is in place.

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.);

- 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 PHI;

- health information organizations;

- e-prescribing gateways;

- other entities that provide data transmission services with respect to PHI and require routine access to PHI;

- entities that offer a personal health record to one or more individuals on behalf of a covered entity; or

- entities that maintain PHI, whether or not the entities actually review the PHI.

XII. Disclosures of De-Identified Information

The Plan may freely use and disclose de-identified information in accordance with HIPAA privacy regulations. De-identified information is health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. There are two ways a business associate can determine that information is de-identified: either by professional statistical analysis, or by removing specific identifiers.

XIII. Physical Access Controls/Guidelines to Guard PHI

The Association and Employers will maintain strict physical access controls to its information systems at all times and under all conditions. This includes the physical security of electronic and paper data.

The Association and Employers will terminate access to information systems and other sources of PHI, including access to rooms or buildings where PHI is located, when an employee, agent or contractor ends his/her employment or engagement. The Association and Employers will terminate access to specific types of PHI when the status of any member of the workforce no longer requires access to those types of information.

Cleaning personnel:

Cleaning personnel do not need PHI to accomplish their work. Whenever reasonably possible, PHI will be placed in locked containers, cabinets or rooms before cleaning personnel enter an area. When it is not reasonably possible to lock up PHI, it must be removed from sight before cleaning personnel enter an area and a supervisor must be present.

Computer Screens:

Computer screens at each workstation must be positioned so that only authorized users at that workstation can read the display. When screens cannot be relocated, filters, hoods, or other devices may be employed. Computer displays will be configured to go blank, or to display a screen saver, when left unattended for more than a brief period of time. The period of time will be determined by the Compliance Official. Wherever practicable, reverting from the screen saver to the display of data will require a password. Computer screens left unattended for longer periods of time will log off the user. The period of time will be determined by the Privacy Officer.

Conversations:

Conversations concerning individual care or other PHI must be conducted in a way that reduces the likelihood of being overheard by others. Wherever reasonably possible, barriers will be used to reduce the opportunity for conversations to be overheard.

Copying medical records and other PHI:

When PHI is copied, only the information that is necessary to accomplish the purpose for which the copy is being made, may be copied. This may require that part of a page be masked.

Desks and countertops:

Provider reports and other documents which may display identifiers and other "keys" to information should be placed face down on counters, desks, and other places where individuals or visitors can see them. Wherever it is reasonably possible to do so, medical reports and other documents containing PHI will not be left on desks and countertops after business hours. Supervisors will take reasonable steps to provide all work areas where PHI is used in paper form with lockable storage bins, lockable desk drawers or other means to secure PHI during periods when the area is left unattended. In areas where locked storage after hours cannot reasonably be accomplished, PHI must be kept out of sight. A supervisor must be present whenever someone who is not authorized to have access to that data is in the area.

Disposal of paper with PHI:

Paper documents containing PHI must be shredded when no longer needed. If retained for a commercial shredder, they must be kept in a locked bin.

Home office:

Any member of the workforce who is authorized to work from a home office must assure that the home office complies with all applicable policies and procedures regarding the security and privacy of PHI, including these guidelines.

Key policy:

The Privacy Officer will develop a list of which personnel, by job title, may have access to which keys. This includes keys to storage cabinets, storage rooms and buildings. All keys must be signed out. Keys must be surrendered upon termination of employment. The Privacy Officer will ensure that locks are changed whenever there is evidence that a key is no longer under the control of an authorized member of the workforce, and its loss presents a security threat that justifies the expense.

Phones or Laptops:

The privacy and security policies apply to any PHI that is stored on a phones or laptop. Users of PDAs and laptops are responsible for assuring that the PHI on their devices is kept secure and private. Any loss or theft of a phone or laptop thought to contain PHI must be reported to the Privacy Officer immediately. Users of phones who store PHI on their devices will receive special training in the risks of this practice, and measures that they can take to reduce the risks (such as use of passwords).

Printers and Fax Machines:

Printers and fax machines must be located in secure areas, where only authorized members of the workforce can have access to documents being printed.

Records carried from one building to another:

When PHI is carried from one building to another, it must be signed out and signed in. When a member of the workforce is transporting PHI from one building to another, it may not be left unattended unless it is in a locked vehicle, in an opaque, locked container. Locking the vehicle alone is not sufficient.

Record Storage:

Areas where records and other documents that contain PHI are stored must be secure. Wherever reasonably possible, the PHI will be stored in locking cabinets. Where locking cabinets are not available, the storage area must be locked when no member of the workforce is present to observe who enters and leaves and no unauthorized personnel may be left alone in such areas without supervision.

Workforce Vigilance:

All members of the workforce are responsible for watching for unauthorized use or disclosure of PHI, to act to prevent the action, and to report suspected breaches of privacy and security policies to their supervisor, or to the Privacy Officer (example of a breach: individual or visitor looking through PHI left on a counter).

Visitors:

Visitors to areas where PHI is being used must be accompanied by a representative of the Association or a member of the Employer's workforce.

XIV. Breach Notification Requirements

The Plan will comply with the requirements of the HITECH Act and its implementing regulations to provide notification to affected individuals, HHS, and the media (when

required) if the Plan or one of its business associates discovers a breach of unsecured PHI.

Policies on Individual Rights

I. Access to PHI and Requests for Amendment

HIPAA gives participants the right to access and obtain copies of their PHI (or electronic copies of PHI) that the Plan (or its business associates) maintains in designated record sets. HIPAA also provides that participants may request to have their PHI amended. The Plan will provide access to PHI and it will consider requests for amendment that are submitted in writing by participants.

Designated Record Set is a group of records maintained by or for the Plan that includes:

- the enrollment, payment, and claims adjudication record of an individual maintained by or for the Plan; or
- other PHI used, in whole or in part, by or for the Plan to make coverage decisions about an individual.

II. Accounting

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

- to carry out treatment, payment or health care operations;
- to individuals about their own PHI;
- incident to an otherwise permitted use or disclosure;
- pursuant to an authorization;
- to persons involved in the patient's care or other notification purposes;
- to correctional institutions or law enforcement when the disclosure was permitted without authorization;
- as part of a limited data set;
- for specific national security or law enforcement purposes; or
- disclosures that occurred prior to the compliance date.

The Plan shall respond to an accounting request within 60 days. If the Plan is unable to provide the accounting within 60 days, it may extend the period by 30 days, provided that it gives the participant notice (including the reason for the delay and the date the information will be provided) within the original 60-day period.

The accounting must include the date of the disclosure, the name of the receiving party, a brief description of the information disclosed, and a brief statement of the purpose of the disclosure (or a copy of the written request for disclosure, if any). If a brief purpose statement is included in the accounting, it must be sufficient to reasonably inform the individual of the basis of the disclosure.

The first accounting in any 12-month period shall be provided free of charge. The Privacy Officer may impose reasonable production and mailing costs for subsequent accountings.

III. Requests for Alternative Communication Means or Locations

Participants may request to receive communications regarding their PHI by alternative means or at alternative locations. For example, participants may ask to be called only at work rather than at home. Such requests may be honored if, in the sole discretion of the Employer, the requests are reasonable.

However, the Plan shall accommodate such a request if the participant clearly provides information that the disclosure of all or part of that information could endanger the participant. The Privacy Officer has responsibility for administering requests for confidential communications.

IV. Requests for Restrictions on Uses and Disclosures of Protected Health Information

A participant may request restrictions on the use and disclosure of the participant's PHI. It is the Plan's' policy to attempt to honor such requests if, in the sole discretion of the Employer, the requests are reasonable. The Plan is charged with responsibility for administering requests for restrictions and shall communicate any restrictions to the Privacy Officer.

515-217