HIPAA PRIVACY POLICY

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) grants individuals the right to receive notice of the uses and disclosures of their protected health information that may be made by the district, and sets forth the individual's rights and the district's legal obligations with respect to protected health information. The purpose of this policy is to assist the district in complying with the HIPAA privacy standards, to ensure that individuals receive adequate notice of the district's practices with regard to the dissemination and use of protected health information, and to protect the confidentiality and integrity of protected health information.

Definitions

For the purposes of this policy, the following definitions shall apply:

Individually Identifiable Health Information is a subset of health information, including demographic information collected from an individual and is created or received by a health care provider, health plan, employer, or health care clearinghouse; relates to past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual; and identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Protected Health Information is individually identifiable health information that is transmitted by electronic means; maintained in any electronic medium, such as magnetic tape, disc, or optical file; or transmitted or maintained in any other form or medium, such as paper, verbal, email, or fax.

Covered Functions means those functions of the district the performance of which makes the school district a health plan, health care provider, or health care clearinghouse.

Designated Record Set is a group of records maintained by or for the district that is medical records and billing records about individuals; the enrollment, payment, claims adjudication, and case or medical management systems; or used in whole or in part by the district to make decisions about individuals.

Business Associate is a person or entity that provides certain functions, activities, or services for or on behalf of the district involving the use and/or disclosure of protected health information.

Confidentiality of Individually Identifiable Health Information

All officers, employees, and agents of the district shall preserve the confidentiality and integrity of individually identifiable health information pertaining to any individual. Individually identifiable health information is protected health information and shall be safeguarded to the extent possible in compliance with the requirements of the security and privacy rules and standards established by the HIPAA.

The district and its officers, employees, and agents will not use or disclose an individual's protected health information for any purpose without the properly documented consent or authorization of the individual or his/her authorized representative unless required or authorized to do so under state or federal law or this policy, unless an emergency exists, or unless the information has been sufficiently de-identified that the recipient of the information would be unable to link the information to a specific individual.

All officers, employees, and agents of the district are expected to comply with and cooperate fully with the administration of this policy. The district will not tolerate any violation of the HIPAA privacy or security standards or this policy. Any such violation shall constitute grounds for disciplinary action up to and including termination of employment.

Any officer, employee, or agent of the district who believes that there has been a breach of these privacy and security policies and procedures or a breach of the integrity or confidentiality of any person's protected health information shall immediately report such breach to his or her immediate supervisor or the formally appointed Privacy Officer. The Privacy Officer shall conduct a thorough and confidential investigation of any reported breach and notify the complainant of the results of the investigation and any corrective action taken.

The district will not retaliate or permit reprisals against any employee who reports a breach to the integrity or confidentiality of protected health information. Any employee involved in retaliatory behavior or reprisals against another individual for reporting an infraction of this policy shall be subject to disciplinary action up to and including termination of employment.

Security Provisions

The district shall take reasonable steps to limit the use and/or disclosure of and requests for protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure or request and to determine the extent to which various classifications of employees need access to such information. The district shall also implement reasonable administrative, technical, and physical safeguards to protect individually identifiable health information from any intentional or unintentional use or disclosure and that mitigate, to the extent practicable, any harmful effect that is known to the district as a result of a use or disclosure of protected health information in violation of this policy or the HIPAA privacy and security standards. The district's security measures shall include the following:

A. Administrative procedures to guard data integrity, confidentiality, and availability, including documented, formal practices to manage the selection and execution of security measures to protect data and to manage the conduct of personnel in relation to the protection of data;

B. Physical safeguards to protect data integrity, confidentiality, and availability including the protection of physical computer systems and related buildings and equipment from fire and other natural and environmental hazards and from intrusion and the use of locks, keys, and other administrative measures to control access to computer systems and facilities;

C. Technical security services to protect data integrity, confidentiality, and availability including processes put in place to protect information and to control individual access to information;

D. Technical security mechanisms including processes put in place to protect against unauthorized access to data that is transmitted over a communications network; and

E. The optional use of an electronic digital signature.

Mitigating the Effects of Unauthorized Use or Disclosure

If the Privacy Officer determines that there has been a breach of this privacy policy or the procedures of the district, he/she shall make a determination of the potential harmful effects of the unauthorized use or disclosure and decide upon a course of action to minimize the harm. Any individual responsible for the unauthorized use or disclosure shall be referred to the Superintendent or designee for appropriate disciplinary action.

Use or Disclosure of Personal Health Information

The district may use and disclose personal health information, without the written consent of the individual or his/her authorized representative, both within and outside of the district, for the following purposes:

A. Treatment: The provision, coordination, or management of health care, health care services or supplies related to an individual and related services by or among providers, providers and third parties, and referrals from one provider to another.

B. Payment: Activities undertaken by a health plan to obtain premiums or determine responsibility for coverage, or activities of a health care provider or health plan to obtain reimbursement for the provision of health care. Payment activities include, but are not limited to, billing, claims management, collection activities, eligibility determination, and utilization review.

C. Health Care Operations: Activities of the district to the extent such activities are related to covered functions including quality assessment and improvement activities; credentialing health care professionals; insurance rating and other insurance activities related to the creation or renewal of a contract for insurance; conducting or arranging for medical review, legal services and auditing functions, including compliance programs; business planning such as conducting cost-management and planning analyses to managing and operating the district including formulary development and administration, development, improvements for methods of payment or coverage policies; business management and general administration activities; due diligence in connection with the sale or transfer of assets to a potential successor in interest if the potential successor is a covered entity or will become a covered entity; consistent with privacy requirements, creating de-identified health information, fundraising for the benefits of the covered entity and marketing for which an individual authorization is not required.

D. As required by law.

E. For public health activities.

F. About victims of abuse, neglect, or domestic violence.

G. To health oversight agencies in connection with health oversight activities.

H. For judicial and administrative proceedings.

I. For law enforcement purposes.

J. Regarding decedents to coroners, medical examiners, and funeral directors.

K. For research if a waiver of authorization has been obtained.

L. To prevent serious and imminent harm to the health or safety of a person or the public.

M. For specialized governmental functions.

N. Military and veterans activities.

O. National security and intelligence.

P. Protective services for the President and others.

Q. To the Department of the State to make medical suitability determinations.

R. To correctional institutions and law enforcement officials regarding an inmate.

S. Workers' compensation if necessary to comply with the laws relating to workers' compensation and other similar programs.

Prior to releasing any protected health information for the purposes set forth above, the district representative disclosing the information shall verify the identity and authority of the individual to whom disclosure is made. This verification may include the examination of official documents, badges, driver's licenses, workplace identity cards, credentials, or other relevant forms of identification or verification.

Authorization

The district shall not disclose protected health information for purpose other than those set forth above without a valid authorization. A valid authorization is a document signed by the individual that gives the district permission to use specified health information for a specified purpose and time frame. The district shall not condition the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits on an individual's provision of authorization except:

A. The district may condition the provision of research-related treatment on the provision of authorization.

B. A health plan may condition enrollment or eligibility for benefits on the provision of an authorization requested by the plan prior to enrollment.

C. The authorization is sought for the plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations.

D. The district may condition provision of health care that is solely for the purpose of creating protected health information for disclosure to a third party on the provision of authorization for the disclosure of the protected health information to the third party.

To be valid, an authorization shall contain at least the following elements:

A. A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;

B. The name or other specific identification of the person(s) or class of person(s) authorized to make the requested use or disclosure;

C. The name or other specific identification of the person(s) or class of person(s) to whom the district may make the requested use or disclosure;

D. An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure;

E. A statement of the individual's right to revoke the authorization in writing and the exceptions to the right to revoke together with a description of how the individual may revoke the authorization;

F. A statement that information used or disclosed pursuant to the authorization may be subject to redisclosure by the recipient and no longer be protected by this rule; and

G. Signature of the individual and date and, if the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual.

In addition to the requirements set forth above, authorization requested by the district for its own use of protected health information that it maintains, must comply with the following additional requirements:

A. A statement that the district will not condition treatment, payment, enrollment in the health plan, or eligibility for benefits upon the individual's provision of authorization for the requested use;

B. A description of each purpose of the requested use or disclosure;

C. A statement that the individual may inspect or copy the protected health information to be used or disclosed and refuse to sign the authorization; and

D. If the disclosure of the requested information will result in direct or indirect remuneration to the district from a third party, a statement that remuneration will result.

The district shall provide the individual with a copy of the signed authorization.

An authorization for the use or disclosure of protected health information may not be combined with any other document to create a compound authorization.

An authorization is not valid if the document submitted has any of the following defects:

A. The expiration date has passed or the expiration event is known to have occurred;

B. Any required element is missing or has not been filled out;

C. The authorization is known to have been revoked;

D. The authorization has been improperly combined with another document;

E. The district has violated the rules on making the authorization a condition; or

F. Any material information in the authorization is known to be false.

An individual may revoke an authorization at any time, provided the revocation is in writing.

Rights Related to Protected Health Information

Individuals shall have the following rights with regard to their protected health information:

A. Access. Individuals shall have the right to access their own protected health information that is maintained in record sets of the district and its business associates.

B. Restrictions. Individuals shall have the right to request restrictions on how the district will use or disclose their own protected health information for treatment, payment or health care operations and how their information will be disclosed or not disclosed to family members or others involved in their care. The district shall comply with the individual's reasonable request to receive communications of protected health information by alternative means or at alternative locations.

C. Amendment. Individuals shall have the right to amend erroneous or incomplete protected health information unless the information:

1. Was not created by the district;

2. Is not in a designated record set or is not otherwise available for inspection;

3. Is accurate and complete; or

4. Would not be subject to the right of access.

A request to amend protected health information must be submitted to the Privacy Officer in writing. The Privacy Officer shall review the request and respond in writing within thirty calendar days. If a request to amend is denied, the individual may appeal the denial using the complaint procedure set forth in this policy. The denial must be written in plain language and contain:

- The basis for the denial;

- A statement of the individual's right to submit a written statement disagreeing with the denial and how it may be filed;

- A statement that, if the individual does not submit a statement of disagreement, his/her right to request that the request for amendment and its denial be provided with any future disclosure of the protected health information that is the subject of the request for amendment;

- A description of how the individual may appeal the denial; and

- The right of the district to reasonably limit the length of the statement of disagreement.

The district may also choose to prepare a written rebuttal to the statement of disagreement and provide a copy to the individual. All of the statements related to the amendment denial shall become part of the individual's designated record set and shall be linked to the individual's protected health information.

D. Accounting. Individuals shall have the right to an accounting of disclosures of their own protected health information that is maintained in record sets of the district and its business associates. Such accounting shall include a period of six years prior to the request.

Business Associates

The district, its officers, employees, and agents shall not disclose protected health information to any business associate in the absence of a written contract with the business associate that assures that the business associate will use the information only for the purposes for which it was engaged by the district; will safeguard the information from misuse; and will assist the district in complying with its duties to provide individuals with access to health information about them and a history of certain disclosures. The district shall disclose protected health information to a business associate for the sole purpose of assisting the district in completing healthcare functions, not for the independent use by the business associate.

The district shall enter into a contract with each business associate, which shall be a document separate from the service agreement. The Privacy Officer shall be responsible for managing all business associate contracts and ensuring that they are current and in compliance with the requirements of this policy and the HIPAA privacy rule. Under the contract, the business associate shall be obligated to notify the Privacy Officer when unauthorized uses and/or disclosures of protected health information have occurred in the business associate's organization. The Privacy Officer will take appropriate steps to address the violation up to and including termination of the business associate contract.

However, the district shall not be liable for privacy violations of a business associate, and the district is not required to actively monitor or oversee the means by which a business associate carries out safeguards or the extent to which a business associate abides by the requirements of the contract.

Privacy Officer

Unless otherwise appointed in writing, the Treasurer shall be the Privacy Officer for the district. The Privacy Officer will be responsible for overseeing all ongoing activities related to the development, implementation, maintenance, and adherence to the district's policies and procedures concerning the security and privacy of protected health information.

Complaint Procedure

The following procedure shall be used for the processing of complaints regarding the collection, use, management, disclosure, or amendment of protected health information:

Step 1 – A written complaint must be submitted to the Privacy Officer. A complaint can also be made directly to the Secretary of Health and Human Services. Upon receipt of a complaint, the Privacy Officer will review the complaint, conduct any necessary investigation, and provide the complainant with a written disposition within ten working days.

Step 2 – The disposition of the Privacy Officer may be appealed by the complainant to the Superintendent or designee within ten working days of receipt of the disposition of the Privacy Officer. The Superintendent or designee shall meet within ten school days with the complainant, the Privacy Officer, and any other necessary individuals. The Superintendent or designee will respond in writing to the complainant within ten working days following the meeting.

Step 3 – If the complaint is not satisfactorily resolved, a written appeal may be made to the Board of Education within ten school days of receipt of the Superintendent's decision. The Board of Education will meet with the complainant at its next regular meeting, and provide a written response to the complaint no later than the following regular meeting.

Notice

The district shall distribute a Notice of Privacy Practices to individuals at the time of their enrollment in the health plan and within sixty days of any material revision. The notice shall also be posted in a clear and prominent location in each facility in the district and be printed in staff handbooks and the health plan booklet. The district will also notify individuals covered by the health plan of the availability of and how to obtain the notice at least once every three years. The notice shall adequately inform individuals of their rights to:

A. Request restrictions on certain uses and disclosures of protected health information;

B. Request the communication of confidential information by some reasonable alternative means or at an alternative location;

C. Inspect and copy records or receive a summary of specific information;

D. Request that protected health information be amended;

E. Request an accounting of certain disclosures of protected health information; and

F. Receive a paper copy of the notice upon request.

Training

All employees and business associates shall receive training regarding the district's privacy policies and procedures as necessary and appropriate to carry out their job duties. Training shall also be provided when there is a material change in the district's privacy practices or procedures.

Documentation

Documentation shall be required in support of the policies and procedures of the district and all other parts of the HIPAA privacy regulations that directly require documentation, including, but not limited to, all authorizations and revocations of authorizations and complaints and disposition of complaints. All documentation shall be kept in written or electronic form for a period of six years from the date of creation or from the date when it was last in effect, whichever is later.

LEGAL REF: 29 U.S.C. §1181 *et seq.*

Adopted: October 18, 2011

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

NOTICE OF PRIVACY PRACTICES

Effective Date: April 14, 2003

THIS PRIVACY NOTICE IS PROVIDED BY FAIRVIEW PARK CITY SCHOOLS AND ITS THIRD PARTY ADMINISTRATOR, ANTHEM BENEFIT ADMINISTRATORS referred to as "the Plan"). This notice covers functions of the Plan to the extent the performance of those functions are in connection with providing medical care, including items and services paid for as medical care, directly or through insurance, reimbursement or otherwise.

The Health Insurance Portability and Accountability Act (HIPAA) is a federal law. The Plan is required by HIPAA to provide you with this notice. This notice describes the Plan's privacy practices, legal duties, and your rights concerning your protected information. The Plan must follow the privacy practices described in this notice while it is in effect. This notice takes effect April 14, 2003. It will remain in effect until the Plan publishes and issues a new notice.

1. THE PLAN'S COMMITMENT TO YOUR PRIVACY

The Plan is committed to protecting the confidential nature of your medical information to the fullest extent of the law. In addition to various laws governing your privacy, the Plan has its own privacy policies and procedures in place. These are designed to protect your information. The Plan will continue to make protecting your privacy a priority.

2. THE PLAN'S LEGAL DUTIES

The Plan is required by applicable federal and state laws to keep certain information about you private. An example of this is your medical information. The Plan treats your medical and demographic information that it collects as part of providing your coverage, as "Protected Information." It is the Plan's policy to maintain the privacy of Protected Information in

accordance with HIPAA, except to the extent that applicable state law provides greater privacy protections. This Notice of Privacy Practices was drafted to be consistent with the HIPAA privacy regulation. Any terms not defined in this Notice will have the same meaning as they have in the HIPAA privacy regulation.

The HIPAA Privacy Regulations generally do not "preempt" (or take precedence over) state privacy or other applicable laws that provide individuals greater privacy protections. As a result, to the extent state law applies, the privacy laws of a state, or other federal laws, rather than the HIPAA Privacy Regulation, might impose a privacy standard that the Plan is required to follow.

The Plan reserves the right to change the terms of this notice. The Plan may make the new notice provisions effective for all the Protected Information that it maintains. This includes information that the Plan created or received before it made the changes. Any revised notice will be provided to you by one of the following means: (1) by mail to the participant under the terms of your coverage; or (2) by delivery of the notice to the participant at his or her work location if the participant is an active employee of the plan sponsor. A copy of any revised notice will also be available on the Plan's website.

Anyone may request a copy of the Plan's notice at any time. For more information about the Plan's privacy practices, or for additional copies of this notice, please contact the Plan's Privacy Officer. Contact information is provided at the end of this notice.

---

3. THE PLAN'S PRIMARY USES AND DISCLOSURES OF YOUR PROTECTED INFORMATION

The Plan may use and disclose your Protected Information without your specific authorization for purposes of treatment, payment, and health care operations. To illustrate:

- **Treatment activities.** Activities performed by a health care provider related to the provision, coordination or management of health care provided to you. The Plan does not provide treatment, which is the role of a health care provider (your physician, a hospital or the like). However, the Plan may disclose Protected Information to your health care provider in order for that provider to treat you.

- **Payment activities.** Activities undertaken to obtain premiums or to determine or fulfill the Plan's responsibilities for coverage and provision of plan benefits. These include activities such as determining eligibility or coverage, utilization review activities, billing, claims management, and collection activities. For example, the Plan may use Protected Information to determine whether a particular medical service given or to be given to you is covered under the terms of your coverage. The Plan may also disclose Protected

Information to health care providers or other health plans for their payment activities, such as to coordinate benefits.

- **Health care operation activities.** Activities such as credentialing, business planning and development, quality assessment and improvement, premium rating, enrollment, underwriting, claims processing, customer service, medical management, fraud and abuse detection, obtaining legal and auditing services, and business management. For example, the plan may use your Protected Information for underwriting, premium rating, or other activities associated with the creation, renewal or replacement of a contract of health insurance or health benefits. The Plan may also disclose Protected Information to other health plans or health care providers for certain health care operation activities of their own as described in the HIPAA privacy regulation.

  The Plan may also use your Protected Information to give you information about one of its disease/care management programs. The Plan may also give you information about treatment alternatives or other health-related benefits and services that may interest you. The Plan may disclose Protected Information to the sponsor of the Plan, provided that the Plan adopts certain protections required by federal law.

When using and disclosing your Protected Information in the Plan's payment and healthcare operation activities, the Plan may only request, use, and disclose the minimum amount of your Protected Information necessary to complete the activity.

The Plan may contract with others to assist it with treatment, payment or health care operation activities that involve the use of your Protected Information. Such third parties are referred to as the Plan's business associates. The Plan requires business associates to agree, in writing, to contract terms. These terms are specifically designed to safeguard Protected Information before it is shared with them. The Plan may also have business associates assist in the activities described in the following section that involve permitted uses and disclosures.

4. OTHER USES AND DISCLOSURES OF YOUR PROTECTED INFORMATION

You and on Your Authorization. The Plan must disclose your Protected Information to you. This is described in the Individual Rights section of this notice, below. You may also give the Plan written authorization to use or disclose your Protected Information to anyone for any purpose. If you give the Plan an authorization, you may revoke it in writing at any time. Your revocation will not affect any use or disclosures permitted by your authorization while it was in effect. Without your written authorization, the Plan may not use or disclose your Protected Information for any reason except as described in this notice.

The following is a description of other possible ways the Plan may (and are permitted by law to) use and/or disclose your Protected Information without your specific authorization.

- **Family and Friends.** If you are unavailable to agree, the Plan may disclose your Protected Information to a family member, friend or other person when the situation indicates that disclosure would be in your best interest. This includes a medical emergency or disaster relief. If you are available and agree, the plan may disclose your Protected Information to a family member, friend or other person to the extent necessary to help with your health care or with payment for your health care.

- **Research. Death. Organ Donation.** The Plan may use or disclose your Protected Information for research purposes in limited circumstances specified in the HIPAA privacy regulation. The Plan may disclose the Protected Information of a deceased person to a coroner, medical examiner, funeral director, or organ procurement organization for certain purposes.

- **Public Health and Safety.** The Plan may disclose some of your Protected Information permitted by state law to the extent necessary to avert a serious and imminent threat to your health or safety or the health and safety of others. The Plan may disclose your Protected Information to a government agency that oversees the health care system or government programs or its contractors, and to public health authorities for public health purposes. The Plan may disclose your Protected Information to appropriate authorities if it reasonably believes that you are a possible victim of abuse, neglect, domestic violence or other crimes.

- **Required by Law.** The Plan may use or disclose your Protected Information when it is required to do so by law. For example, the Plan must disclose your Protected Information to the U.S. Department of Health and Human Services upon request in order to determine if it is in compliance with federal privacy laws. The Plan may disclose your Protected Information to comply with workers' compensation or similar laws.

- **Legal Process and Proceedings.** The Plan may disclose your Protected Information in response to a court or administrative order, subpoena, discovery request, or other lawful process. These disclosures are subject to certain administrative requirements imposed by the HIPAA privacy regulation and permitted by state law.

- **Law Enforcement.** The Plan may disclose limited information to a law enforcement official concerning the Protected Information of a suspect, fugitive, material witness, crime victim or missing person subject to certain administrative requirements approved by the HIPAA regulation and permitted by state law. The Plan may disclose the Protected Information of an inmate or other person in lawful custody to a law enforcement official or correctional institution under certain circumstances specified by the HIPAA privacy regulation. The Plan may also disclose Protected Information where

necessary to assist law enforcement officials to capture an individual who has admitted to participation in a crime or has escaped from lawful custody.

- **Military and National Security.** The Plan may disclose to the military authorities the Protected Information of Armed Forces personnel under certain circumstances specified by the HIPAA privacy regulation. The Plan may also disclose to authorized federal officials Protected Information required for lawful intelligence, counterintelligence, and other national security activities.

---

5. INDIVIDUAL RIGHTS

- **Access.** You have the right to inspect and obtain copies of your Protected Information for as long as your information is maintained in the Plan's designated record set. The Plan's designated record set includes records from its claims administrator's enrollment, billing, claims, and medical management systems, as well as any other records the Plan maintains in order to make decisions about your health care benefits. Your right of access to Protected Information does not extend to certain information. This includes information contained in psychotherapy notes or information compiled in reasonable anticipation of, or for use in a civil, criminal or administrative proceeding.

  You may request that the plan provide copies in a format other than photocopies. It will use the format you request unless it is not practical for it to do so. The Plan reserves the right to charge a reasonable fee for copies of Protected Information that it provides.

  Any request to exercise your individual right of access to your Protected Information must be in writing. You may obtain a form to request access by using the contact information listed at the end of this notice. The Plan will respond to your request for access within 30 days of receiving the request. If all or any part of your request is denied, the Plan's response will detail any appeal rights you may have with respect to that decision.

  Notwithstanding the formal process for your right of access, certain information related to enrollment and claims processing may be available to you by contacting the Plan's claims administrator as part of its normal customer service function. You should contact the claims administrator first to see if your request can be satisfied as a customer service request.

- **Amendment.** You have the right to request that the Plan amend your Protected Information that it keeps in its designated record set if you believe it is inaccurate. A request that your Protected Information be amended must be done in writing. You may

obtain a form to request amendment by using the contact information listed at the end of this notice. The Plan will respond to your request for amendment within 60 days of receiving the request.

If the Plan accepts your request to amend the information, it will notify you. The Plan will make reasonable efforts to inform other persons, including those identified by you as having received your Protected Information and needing the amendment. The Plan will also include the changes in any future disclosure of that information. If the Plan denies your request for reasons permitted by the HIPAA privacy regulations, its notice to you will explain any appeal rights you may have with respect to that decision.

Notwithstanding the formal process for your right of amendment, certain information related to enrollment and claims processing may be corrected by contacting the Plan's claims administrator. This is part of its normal customer service function. You should contact the claims administrator first to see if your request can be satisfied as a customer service request.

- **Disclosure Accounting.** You have the right to request and receive an accounting of disclosures of your Protected Information made by the Plan. It is not required under the HIPAA privacy regulation to provide you with an accounting of certain types of disclosures. The most significant types include:

  - Any disclosures made prior to April 14, 2004.
  - Disclosures for treatment, payment or health care operations activities.
  - Disclosures to you or pursuant to your authorization.
  - Disclosures to persons involved in your care.
  - Disclosures for disaster relief, national security or intelligence purposes.
  - Disclosures that are incidental to a permitted use or disclosure.

  To request an accounting of disclosures, you must send a written request to the contact office listed at the end of this notice. You may request one such accounting at no charge every 12 months. You may request that the accounting cover up to a 6 year period of reportable disclosures from the date of your request. The Plan will respond within 60 days of your request. It reserves the right to impose a reasonable charge for requests made more than once per year.

- **Confidential Communications.** You may believe that you will be in danger if the Plan communicates Protected Information to you to your address of record. If so, you have the right to request that the Plan communicate with you about your Protected Information at an alternative location or by alternate means. The Plan will make reasonable efforts to accommodate your request if you specify an alternate address. To request a confidential communication, you must direct your request to the contact office listed at the end of this notice.

- **Restriction Request.** You have the right to request that the Plan restrict the use or disclosure of your Protected information for treatment, payment or health care operation activities. You also have the right to request that the Plan restricts disclosures to relatives, friends, or other individuals that may be involved in your care or payment for your health care. The Plan is not required to agree to such a request for restriction. To request a restriction, you must direct your request to the contact office listed at the end of this notice.

---

6. CONTACTING THE PLAN

Please contact the Plan at the address below.

- If you want a printed copy of the Plan's current notice
- If you want to access your Protected Information
- If you want to request an amendment to your Protected Information
- If you want to request an accounting of the Plan's disclosures of your Protected Information
- If you want to request a restriction on the Plan's use and disclosure of your Protected Information
- If you want the Plan to communicate with you at an alternative address or by alternate means because you believe that you are endangered
- If you have questions, concerns, or complaints about this notice or the Plan's privacy practices

Group Privacy Officer

FAIRVIEW PARK CITY BOARD OF EDUCATION
ATTN: RYAN GHIZZONI
21620 MASTICK ROAD
FAIRVIEW PARK CITY, OHIO 44126
1-440-331-5500

As described in section 5 of this notice, you may also be able to access or amend certain information in enrollment, billing, or claims systems by contacting the claims administrator using the contact information on your ID card.

7. CONTACTING THE DEPARTMENT OF HEALTH AND HUMAN SERVICES

You may also submit a written complaint to the Department of Health and Human Services if you believe your privacy rights have been violated.

THE PLAN MAINTAINS AND ENFORCES A POLICY OF NON-RETALIATION AGAINST THE PLAN'S MEMBERS, MEMBERS OF THE PLAN'S WORKFORCE, OR MEMBERS OF THE PUBLIC WHO BRING BREACHES (OR POTENTIAL BREACHES) OF THIS NOTICE TO THE ATTENTION OF THE PLAN'S PRIVACY OFFICER OR THE DEPARTMENT OF HEALTH AND HUMAN SERVICES.