**HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF
1996 (HIPAA) PRIVACY POLICY**

IN GENERAL

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) authorized the Secretary of Health and Human Services (HHS) to establish standards for protecting the privacy of personal health information. The district is covered in two ways. This policy is intended to comply with those HHS regulations. However, because the regulations are fairly complex and subject to differing interpretations, the Superintendent is directed to recommend updates to this policy as new information becomes available.

HIPAA COVERAGE

The District has determined that certain functions of the District are covered functions, making the District a covered entity under HIPAA. The District is a "health plan" as defined by HIPAA, and/or the District is a "health care provider" as defined by HIPAA. The District declares itself to be a "hybrid entity," which means that only the covered functions of the District's operations (i.e., student health services) are subject to HIPAA.

IMPLEMENTATION PROCEDURES FOR HEALTH PLAN RECORDS

In order to comply with HIPAA's privacy standards, the District has taken the following steps:

1.   Contact Person. The District has designated the Business Manager as the contact person responsible for receiving complaints about HIPAA compliance and providing additional information about the District's HIPAA practices and procedures.

2.   Privacy Officer. The District has designated Business Manager as the Privacy Officer for HIPAA purposes. The Privacy Officer is responsible for developing and implementing privacy policies and procedures for the District, training District staff, and monitoring compliance. The Privacy Officer shall also be responsible for receiving complaints about HIPAA violations and for providing information about matters covered by privacy notices.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA) PRIVACY POLICY continued

3.   <u>Security of PHI Records</u>. District officials must ensure that records containing individually identifiable personal health information (PHI) are secure so that these records are readily available only to the minimum number of individuals who need them to carry out Treatment, Payment or health care Operations (TPO). The Privacy Officer shall develop reasonable administrative, technical and physical safeguards to protect the privacy of PHI. The Superintendent or designee should review these practices on a periodic basis.

4.   <u>Authorization of Disclosure of PHI</u>. HIPAA does not require participant authorization for health care providers to use or disclose PHI for purposes of treatment, payment or health care operations. With some exceptions, disclosure of PHI by health care providers (except for purposes of treatment, payment or Health Care operations) requires written authorization signed by the individual in question. The Privacy Officer shall determine activities and transactions that require an authorization and will develop an authorization form that complies with the HIPAA Privacy Rule.

5.   <u>Notice of Privacy Practices</u>. District officials will provide a notice to health care participants about their privacy rights and how their PHI will be used. Such information is known as a Notice of Privacy Practices. The notice must not only be provided by the date of disclosure, except in an emergency, but the District must make a good faith attempt to obtain the individual's acknowledgment of receipt of such notice.

6.   <u>Business Associates</u>. A "business associate" is an outside business that provides various administrative services or assists with the District's health plan. The District shall identify its business associates and shall enter into a written contract to safeguard PHI before the District can share PHI with the Business Associate. The deadline for having agreements in place is April 14, 2004.

7.   <u>Training</u>. The District shall train those District employees who work in areas covered by the HIPAA Privacy Rule and who have access to PHI to follow the appropriate procedures to ensure PHI is not disclosed except as allowed by law.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA) PRIVACY POLICY continued

8. <u>Complaints</u>. There shall be a complaint procedure in place whereby written complaints related to PHI and HIPAA standards may be lodged. Any complainant is entitled to a hearing before the privacy officer, who has 10 school days to rule on such complaint. If the complainant is not satisfied with the disposition of the complaint, he/she may appeal to the Superintendent or his or her designee, who shall review the matter and make a final decision within 15 school days of receiving written notice of the appeal. The District shall not intimidate, threaten, coerce, discriminate against, or take any other retaliatory action against any individual exercising his or her HIPAA rights.

STUDENT RECORDS

Although the District is a "health care provider" under HIPAA because of the health care services it provides to students, student records are not subject to HIPAA. The HIPAA Privacy Rules expressly exempt from coverage student records covered by the federal law known as the Family Educational Rights and Privacy Act (FERPA). Such records are not governed by HIPAA even if they contain individually identifiable health information.

EMPLOYEE RECORDS

The HIPAA Privacy Rule does not govern a school district's obligations as an "employer" to maintain, use or disclose medical records of its "employees." Those obligations flow from the Americans with Disabilities Act and should be dealt with in accordance with those laws. Similarly, the HIPAA Privacy Rule prohibits the District from using PHI created or received by the group health plan for employment-related functions.

Legal Reference:

Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, and applicable regulations 45 C.F.R. Part 160 and 164

Added 1/04

KETCHIKAN GATEWAY BOROUGH SCHOOL DISTRICT
Adoption Date: 7/23/08