No. 441

Palmyra Area School District

SECTION: PROFESSIONAL EMPLOYEES

TITLE: MANAGEMENT OF PROTECTED HEALTH INFORMATION (HIPAA)

ADOPTED: April 15, 2004

REVISED:

	441. MANAGEMENT OF PROTECTED HEALTH INFORMATION
1. Statement	The Palmyra Area School District ("District") has established a plan for providing dental and medical benefits ("Health Plan") and a plan for providing a comprehensive range of professional employee assistance and development services, including consulting, training, personnel services, diagnosis, treatment, referral, case management and education seminars in a variety of areas including psychotherapy, performance, psychology, behavioral health, psychological assessment, substance abuse, career services, organizational systems, team building and performance improvement ("Employee Assistance Plan") (each, a "Plan", and together, the "Plans"). It shall be the policy of the Plans to collect, retain, maintain, use and disclose the Plans' "protected health information" pursuant to appropriate information management policies and actions that meet applicable legal and regulatory requirements as set forth in the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and the standards adopted by the Department of Health and Human Services pursuant thereto.
2. Purpose	The purpose of this Policy is to identify and disseminate the framework and principles for information management that guide the actions and operations of the Plans in protecting, generating, and sharing protected health information collected, maintained, used and disclosed by the Plans.
3. Definitions	Words and phrases used in this Policy unless otherwise defined have the same meanings herein as in the Standards for Privacy of Individually Identifiable Health Information (the "Privacy Standards" or the "Privacy Rule") found at 45 CFR Parts 160 and 164, as amended from time to time.
4. Standards for Privacy & Security	A <u>General Standards</u> i) In order to protect the individually identifiable health information entrusted to the Plans, no protected health information shall be disclosed by the Plans except as permitted or required by Sections

164.502(a), 164.502(b), and Section 164.504(f) of the Privacy Rule, and as otherwise permitted by the Privacy Rule.

ii) All protected health information of the Plans in any medium shall be maintained in a central depository for the Plans under the control of the Privacy Officer and Security Officer.

iii) Only District employees involved in the professional functions of the Plans shall have access to protected health information.

iv) Those District employees with access to protected health information of the Plans shall be restricted to the minimum number reasonably necessary to perform professional functions of the Plans. Persons with access to protected health information of the Plans may only have such access on a need to know basis and must be approved as an "authorized data user" prior to access thereto by the Privacy Officer.

v) It is the responsibility of every authorized data user to maintain confidentiality of protected health information of the Plans even if technical security mechanisms fail or are absent. A lack of security measures to protect the confidentiality of information does not imply that such information is public.

vi) Protected health information is the property of the individual to whom the information pertains and the Plans are the steward of that information and the owner of the storage medium.

vii) Protected health information of the Plans may not be disclosed for purposes of employment related actions, nor for any other purpose prohibited by the Privacy Rule (see, for example, Section 164.504(f)(3) of the Privacy Rule).

B. <u>Personnel Designations</u>

i) The Assistant Director Of Business Affairs shall act as the Privacy Officer and Security Officer.

ii) The Privacy Officer is responsible for the coordination and implementation of this Policy; the development from time to time of any appropriate amendments or additions to the Policy and its procedures; cataloging protected health information of the Plans; receiving complaints; assisting the beneficiaries of the Plans on the interpretation of this Policy; preparing and providing information regarding the Plans' Notice of Privacy Practices; monitoring and tracking violations and appeals; identifying areas of risk with the Security Officer; defining with the Security Officer security controls; training and education; and supervising maintenance of records of authorized data users. The Privacy Officer shall have any additional

duties as are from time to time delegated by the School District executive administrators in furtherance of matters related to this Policy.

iii) The Security Officer is responsible for the design, development and implementation of security policies, procedures, and requirements for the gathering, storing, transmission and security of the Plans' protected health information and data processing and computer information technologies. Without limiting the generality of the foregoing, the Security Officer is responsible for determining appropriate security measures and, if necessary, creating policies and procedures that monitor and control access to system resources and data of the Plans. The Security Officer will update security standards as necessary and is responsible for the prevention, detection, containment and correction of security breaches.

C. Complaints; Correction of Data

i) The Privacy Officer is responsible for all complaints. Individuals have the right to correct inaccurate individually identifiable health information under the Plans' control. The appropriate process for validating and processing such corrections is determined individually by the Privacy Officer.

ii) The Privacy Officer is responsible for ensuring that validated correction requests relevant to individually identifiable health information of the Plans is implemented.

iii) To the extent that an audit trail shows access to a Plan beneficiary's protected health information, it shall be made accessible to that individual at the individual's request in the event that questions arise about improper access to his or he records.

iv) The Privacy Officer shall document all complaints received and their disposition.

D. Safeguards and Security

i) The Plans' security shall be the responsibility of the Security Officer, under the general supervision of the Privacy Officer, and may include, to the extent deemed necessary by the Security Officer:

a) Policies to ensure the prevention, detection, containment, and correction of breaches of security, integrity, and confidentiality;

b) Risk analysis;

c) Risk management, including formal, documented procedures for monitoring, detection, auditing, reporting, and responding to breaches of security, integrity, and confidentiality; and

d) A disciplinary process including procedures for the potential discipline, up to and including dismissal, for misuse, misappropriation of data, or acts of omission or commission which result in breaches of security, integrity, or confidentiality of protected health information of the Plans.

ii) The prevention of access to protected health information of the Plans by unauthorized or untrained personnel shall be addressed by taking measures aimed at:

a) Ensuring that all personnel with access or potential access to protected health information of the Plans are specifically authorized for that access, are trained in relevant confidentiality policies, and have attested knowledge of and compliance with those policies;

b) Ensuring that operating and maintenance personnel are given the access necessary for them to perform system maintenance responsibilities without compromising protected health information;

c) Ensuring that personnel performing maintenance activities related to protected health information of the Plans are supervised by authorized, knowledgeable persons;

d) Requiring maintenance of records of those granted physical access to protected health information of the Plans;

e) Implementing other appropriate personnel security policy/procedures; and

f) Ensuring that system users, including technical maintenance personnel, are trained in system security.

iii) Certain protected health information, such as information regarding HIV, substance abuse, sexual abuse, mental health, and psychotherapy notes, are subject to additional specific legal restrictions. Disclosure to anyone other than the individual in question or for treatment, payment for health care operations of such information shall only be made as permitted by this Policy and appropriate law.

E. Training

i) All applicable employees performing functions for the Plans shall receive education and training on the expectations, knowledge, and skills related to information security and the requirements of this Policy and the Privacy Rule prior to April 14, 2004,and upon any material change in this Policy or the Privacy Rule, and in addition, as to new employees performing functions for the Plans, prior to being given access to protected health information of the Plans. The Privacy Officer shall verify and document the training and that employees performing functions for the Plans have received required education and training and attested to this Policy.

ii) The employees performing functions for the Plans shall receive training with respect to any material change to the Policy within a reasonable time after its implementation.

F. Sanctions and Mitigation

i) Should evidence of data access or disclosure of protected health information outside that granted and permitted under this Policy be discovered, it may result in disciplinary action, up to and including termination of employment.

ii) Failure to follow the requirements of this Policy are subject to appropriate disciplinary action up to and including termination of employment.

iii) All sanctions will be documented in accordance with District employee policy.

iv) The Plans shall mitigate, to the extent practicable, any harmful effect that is known of a use or disclosure of protected health information in violation of this Policy.

G. Notice of Privacy Practices

i) The Plans' Notice of Privacy Practices is attached to this Policy and is incorporated into this Policy.

ii) The Privacy Officer is responsible for maintenance of the Notice of Privacy Practices.

iii) a) The Notice of Privacy Practices shall be distributed to all participants of the Plans on or before April 14, 2004. Thereafter, the Notice of Privacy Practices shall be distributed to each new enrollee at the time of enrollment and to individuals covered by the Plans within sixty (60) days of a material revision to the Notice.

b) Not less frequently than once every three (3) years, the Plans will notify Plan beneficiaries of the availability of the Notice and how to obtain the Notice.
