HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY (HIPAA)

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.

Confidentiality of Individually Identifiable Health Information

All officers, employees and agents of the District must 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 HIPAA.

The District and its employees 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.

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.

All employees 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 constitutes grounds for disciplinary action, up to and including termination of employment.

Any employee 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/her immediate supervisor or the Board-appointed privacy/security officer. The privacy/security 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 is subject to disciplinary action up to and including termination of employment.

Following the discovery of a breach of unsecured health information, the privacy/security officer will notify each individual whose unsecured protected health information has been, or is reasonably believed to have been, accessed, acquired, used or disclosed as a result of a breach. Any individual responsible for the unauthorized use or disclosure is referred to the Superintendent or his/her designee for appropriate disciplinary measures.

Privacy/Security Officer

The Treasurer shall be the privacy/security officer for the District. The privacy/security officer is 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.

Notice

The District shall distribute a Notice of Privacy Practices to individuals at the time of their enrollment in the health plan and within 60 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.

Training

All employees 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, complaints and disposition of complaints. All documentation is 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.

[Adoption date: August 22, 2005]
[Re-adoption date: April 19, 2011]
[Re-adoption date: July 27, 2017]

LEGAL REFS.: Health Insurance Portability and Accountability Act; 29 USC 1181 et seq.
45 C.F.R.
ORC 9.01; 9.35
149.41; 149.43
1347.01 et seq.
4113.23

CROSS REF.: KBA, Public's Right to Know