POLICY

The District is committed to protecting the privacy of people and organizations it protects, particularly those who receive direct services from the District.

PURPOSE

To ensure that all District personnel who have access to private, confidential, or sensitive information of employees or recipients of services, hereinafter as "recipients", understand the organization's concern for the respect of the privacy of the employees and recipients and are educated on District policies and practices regarding privacy.

RESPONSIBILITIES

It is the responsibility of the **Board of Directors** and **all personnel** to respect the confidentiality and privacy rights of employees and recipients.

It is the responsibility of the **Board of Directors** to appoint a Privacy Officer.

It is the responsibility of the **Privacy Officer** to ensure employee and recipients' legal confidentiality and privacy rights, monitor compliance with the District's confidentiality and privacy program, receive and investigate reports of unauthorized disclosures and confidentiality or privacy complaints, and report incidents and breaches as required.

It is the responsibility of the **Privacy Officer**, working with the **Personnel Officer** and **Training Officer**, to ensure each member of the Board of Directors and all personnel receive education regarding District policies and practices regarding confidentiality and privacy.

It is the responsibility of the **Privacy Officer**, working with the **Personnel Officer**, to ensure that every individual with the District signs a confidentiality and privacy agreement.

BROAD DEFINITIONS FOR THIS POLICY

Personal information (PI): Also known as personal data. Information that can be used to identify, locate, or contact an individual, alone or when combined with other personal or identifying information; however, for federal and state privacy and data security laws, the precise definition of personal information varies depending on the law and may be more narrowly defined.

PI examples include information frequently contained in incident reports and Patient Care Reports PCRs), including preparation thereof, but are not limited to:

- Name;
- Home or other physical address;
- Email address;
- Telephone number;
- Social Security number;
- Passport number;
- Driver's license number;
- Bank account number;
- Credit or debit card number; and
- Personal characteristics, including photographic image, fingerprints, handwriting or other unique biometric data.

Personally Identifiable information (PII): Information frequently contained in incident reports and Patient Care Reports PCRs), including preparation thereof, that can be used to infer an individual's identity, and includes:

- Information that can identify someone alone, e.g., name, Social Security number, driver's license number; and
- Information that can be used in combination to identify someone, e.g., mother's maiden name and an individual's birthday.

Protected Health Information (PHI): Information frequently contained in incident reports and Patient Care Reports (PCRs), including preparation thereof, that was obtained or used to provide healthcare.

PHI examples include, but are not limited to:

- Identity information such as:
    - Name;
    - Birthday; and
    - Location;
- Identifying images such as pictures that show a patient's face;
- Identity numbers and codes, such as:
    - Email and physical addresses;
    - Social Security numbers;
    - Health insurance account numbers; and
    - License plate numbers;
- Medical records, including:
    - Prescriptions;
    - Health histories; and
    - Laboratory results;
- Biometric data, including:
    - Heartbeat monitoring;
    - Blood sugar monitoring; and
    - Voice recognition.

RECIPIENT AND EMPLOYEE RIGHTS

1. Recipients and employees may exercise their rights to access, amend, restrict, and request an accounting of their PI, PII, and PHI possessed by the District.

2. Recipients and employees may lodge complaints regarding the District's access to and security, collection, disclosure, use of their PI, PII, or PHI with the District's Privacy Officer.

3. Recipients and employees may lodge complaints regarding the access to and security, collection, disclosure, use of their PHI with the Secretary of the Department of Health and Human Services.

PRACTICES

Education Practices

1. The Board of Directors and all personnel are required to be educated on District policies and practices regarding confidentiality and privacy within a reasonable time of being elected, appointed, or hired.

2. The Board of Directors and all personnel are required to be educated on significant changes to District policies and practices regarding confidentiality and privacy.

3. The Board of Directors and all personnel shall be provided access to District policies and practices regarding confidentiality and privacy.

4. Educational topics on employee and recipient confidentiality and privacy shall include:

    a. A complete review of District policies and practices regarding privacy;

    b. Overview of federal and state laws concerning privacy, including the Health Insurance Portability and Accountability Act (HIPAA);

    c. Definition of PI, PII, and PHI;

    d. Recipient and employee rights under HIPAA and District policies and practices regarding confidentiality and privacy;

e. Individual responsibilities under HIPAA and District policies and practices regarding confidentiality and privacy;

f. Importance and benefits of compliance to HIPAA and District policies and practices regarding confidentiality and privacy; and

g. Consequences for failure to comply with HIPAA and District policies and practices regarding confidentiality and privacy.

5. After being educated on District policies and practices regarding confidentiality and privacy, all personnel must provide the Personnel Officer with an executed ***Employee Confidentiality and Privacy Agreement Form 730-1***.

6. After being educated on District policies and practices regarding confidentiality and privacy, each member of the Board of Directors must provide the Personnel Officer with an executed ***Director Confidentiality and Privacy Agreement Form 730-2***.

7. An employee that fails to provide the Personnel Officer with an executed ***Employee Confidentiality and Privacy Agreement Form 730-1*** within a reasonable time of being educated on the District's confidentiality and privacy policies and practices shall not have access to or collect, secure, disclose, use, or retain any private, confidential, and sensitive information, including PI, PII, or PHI.

8. A member of the Board of Directors that fails to provide the Personnel Officer with an executed ***Director Confidentiality and Privacy Agreement Form 730-2*** within a reasonable time of being time of being educated on the District's confidentiality and privacy policies and practices shall not have access to or collect, secure, disclose, use, or retain any private, confidential, and sensitive information, including PI, PII, or PHI and shall be subject to termination.

<u>Access, Collection, Security, Disclosure, Use, and Retention Practices</u>

1. Access to and collection, security, disclosure, and use of PI, PII, and PHI shall be based on the role or position an individual with the District has and shall only be to the extent necessary for that individual to fulfill the responsibilities of that individual's role or position.

2. When PI, PII, and PHI is collected, accessed, disclosed, or used, an individual with the District shall make every effort to only collect, access, disclose, and use the PI, PII, and PHI to the minimum extent necessary to accomplish the intended purpose of accessing, disclosing, or using the PI, PII, and PHI.

3. Individuals with the District should only discuss PI, PII, and PHI with those who are involved in the incident or care of the patient, regardless of a physical location.

4. Individuals with the District must be sensitive to their level of voice and to the fact that others may be in the area when they are speaking; however, this sensitivity must not stop anyone's ability to speak effectively with other individuals at the incident or engaged in the care of a patient.

5. All preliminary documentation used by personnel to assist in the creation or modification of an incident or PCR is the sole property of the District.

6. All scratch paper or other articles used by personnel in the preparation of an incident report or PCR must be properly disposed as soon as the incident report or PCR has been completed.

7. Individuals with the District will be given a unique username to use District's human resources and incident management systems.

8. Individuals with the District shall protect their username and/or password to the District's human resources and incident management systems and no one shall disclose his or her human resources or incident management systems usernames and/or passwords to anyone.

9. Individuals with the District shall only access employee information or incidents and PCRs in the District's human resources or incident management systems necessary for an individual to fulfill the responsibilities of that individual's role or position.

10. No one shall log into the District's human resources or incident management systems with someone else's username.

11. An incident report or PCR may only be amended by an individual with approval of the Fire Chief or Assistant Fire Chief.

12. Printing of incident reports and PCRs shall be minimized and should be limited to open records requests or the quality improvement/quality assurance (QI/QA) process.

13. Inappropriate access to or collection, security, disclosure, use, or retention of PI, PII, or PHI by an employee may result in disciplinary action, up to and including performance improvement counseling, verbal and written warnings, suspension, demotion and/or termination from the District.

14. Inappropriate access to or collection, security, disclosure, use, or retention of PI, PII, or PHI by a member of the Board of Directors may result in a vote of censure by the Board of Directors or even a requested resignation from office by the rest of the Board of Directors, and that the Board of Directors reserves the right to request a quo warranto proceeding to be filed by the County Prosecutor's Office or the Attorney General's Office if necessary for removal from office to enforce the District's legitimate confidentiality and privacy policies and needs.

<u>Incidental Disclosure Practices</u>

1. Incidental disclosures are inevitable in the context of operational and administrative functions, over the radio or face-to-face conversation between personnel, or when PI, PII, and PHI in written or computer form and is inadvertently left out in the open for others to access or view; however, all individuals with the District must be:

    - Sensitive about the importance of maintaining the confidence and security of all information created or used that contains PI, PII, and PHI;

    - Sensitive to avoiding incidental disclosures to anyone who does not have a need to know the information; and

    - Pay attention to who is within earshot when verbal statements are made about a recipient's PI, PII, and PHI; and

    - Follow commonsense procedures to avoid inadvertent incidental disclosures:

2. Individuals with the District shall not have access to information that is not necessary for an individual to fulfill the individual's role or position.

Unauthorized Disclosure and Confidentiality or Privacy Complaint Practices

1. Individuals with the District shall report unauthorized disclosure of PI, PII, or PHI to the District's Privacy Officer.

2. Privacy complaints from recipients and reports of unauthorized disclosure of PI, PII, or PHI reported to the District's Privacy Officer shall be logged and investigated to determine substantiation of the confidentiality or privacy complaint or report of unauthorized disclosure of PI, PII, or PHI.

3. If a confidentiality or privacy complaint or report unauthorized disclosure of PI, PII, or PHI is substantiated, the Privacy Officer shall further determine:

    - Root cause of any unauthorized disclosure of PI, PII, or PHI;
    - Corrective actions;
    - Mitigation or elimination of such future unauthorized disclosure;
    - Recommendation of any disciplinary action to the Personnel Officer and the District Manager or Fire Chief as appropriate; and
    - Report on confidentiality or privacy complaints, incidents, and breaches as required.

RELATED POLICIES

Performance Improvement Counseling 618
Disciplinary Actions 621

STATUTORY REFERENCES

RSMo §32.091
RSMo §161.096
RSMo §167.183
RSMo §188
RSMo §§191.656-191.703
RSMo §194.600
RSMo §§210 and 211
RSMo §302.170
RSMo §362.422
RSMo §§375.1300-375.1312
RSMo §§407.430-407.436
RSMo §407.1355
RSMo §§408.675-408.700
RSMo §§565.252 and 565.253
RSMo §§569.095-569.099
RSMo §§570-223 and 570.224
RSMo §595.232
RSMo §610.021
RSMo §610.035
RSMo §§610.100 to 610.150

Gramm-Leach-Bliley Financial Modernization Act of 1999 (GLBA)
Health Information Technology for Economic and Clinical Health (HITECH) Act
Health Insurance Portability and Accountability Act of 1996 (HIPAA)

REVISION HISTORY

Revision Date	Author	Revision Details
March 12, 2022	Monte Olsen	Initial version