CITY OF CHESAPEAKE, VIRGINIA **NUMBER: 2.62**

ADMINISTRATIVE REGULATION **EFFECTIVE DATE: 03/01/2017**

SUBJECT: DEPARTMENT OF HUMAN RESOURCES CITY OF CHESAPEAKE EMPLOYEE/ RETIREE GROUP HEALTH PLAN: HIPAA AND HITECH ACT COMPLIANCE **SUPERCEDES: 01/01/2016**

I. PURPOSE

Effective January 1, 2016, the City of Chesapeake established a self-insured group health plan for eligible employees, retirees and their dependents ("the Plan"). The Plan is a health care component of the City of Chesapeake obligated to comply with applicable portions of the Health Insurance Portability and Accountability Act (HIPAA) of 1996, the Health Information Technology for Economic and Clinical Health (HITECH) Act, and regulations promulgated thereunder by the U. S. Department of Health and Human Services ("HIPAA regulations").

It is the purpose of this administrative regulation to establish appropriate safety and security practices to ensure the protection of individually identifiable health information in connection with the administration of the Plan; to notify covered members of the City's privacy practices; to establish regular HIPAA training for employees involved in the operation and administration of the group health plan; and delineate a formal process for investigating and documenting all written HIPAA complaints and suspected HIPAA violations including breaches. This policy also articulates the steps to be taken to notify affected individuals if a breach occurs.

II. NOTICE OF PRIVACY PRACTICES

The Plan shall publish and maintain an Employee/Retiree Privacy Notice ("the Notice"), with which all affected staff members shall comply. The current Notice shall be provided to each covered employee and retiree in the manner described in the Notice. In addition, the current Notice will also be posted on the Human Resources Department's page on the City's website.

If the Plan makes any material changes in the Notice, a revised Notice shall be provided to each covered employee or retiree prior to any material changes taking effect.

III. DEFINITIONS

For purposes of this regulation, the following definitions apply:

A. **Breach:** The acquisition, access, use, or disclosure of protected health information in a manner not permitted under the HIPAA regulations that compromises the security or privacy of the protected health information. Breach excludes the following:

- Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of the Plan or a business associate of the Plan, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the HIPAA regulations.

- Any inadvertent disclosure by a person who is authorized to access protected health information for Plan administration (including the Plan's business associates) to another person authorized to access protected health information for the Plan (including its business associates) and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA regulations.

- A disclosure of protected health information when the Plan or business associate of the Plan has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

B. **Business Associate:** An individual or entity who is not employed by the City of Chesapeake but who performs certain functions or activities that involve the use or disclosure of protected health information on behalf of the Plan.

C. **Business Associate Agreement:** A contract between a health care component of the City of Chesapeake and a business associate that identifies permitted and required uses and disclosures of protected health information.

D. **Complaint:** An allegation made by an individual that his/her rights under HIPAA have been violated.

E. **Privacy Officer:** An individual designated by the Plan to be responsible for developing, monitoring and implementing privacy policies and procedures applicable to the administration of the Plan. The Privacy Officer is also responsible for the enforcement of this regulation and is responsible for receiving privacy related complaints.

F. **Protected Health Information (PHI):** Individually identifiable health information that is transmitted or maintained in any format. This information is protected under HIPAA.

G. **Unsecured PHI:** protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary of Health and Human Services.

IV. RESPONSIBILITIES

The Privacy Officer is responsible for the following:

A. Receiving, investigating, and documenting all reported written complaints and suspected HIPAA violations.

B. Making recommendations for resolution of violations and prevention of future violations of the same nature.

C. Ensuring training of new staff members within a reasonable amount of time after joining the organization.

D. Ensuring training of existing staff as procedures, polices or job duties change.

E. Reviewing/updating policies, procedures and reporting processes no less frequently than every two years.

V. PROCEDURES

A. HIPAA Complaints

Any individual may file a written complaint if they believe HIPAA regulations have been violated in connection with Plan operation or administration. Complaints must be filed with the Privacy Officer or their designee. All written complaints will be investigated in accordance with this regulation. The final disposition of the complaint will be documented by the Privacy Officer.

B. Investigation Procedures

1. If a complaint alleges a breach of unsecured PHI, the Privacy Officer must inform the City Manager, or designee, within one (1) business day after learning of the potential violation.

2. Upon receipt of a written complaint or report of a suspected or actual violation of any HIPAA regulation or the Plan's HIPAA policy or procedures, the Privacy Officer will initiate an investigation. In the event of a suspected or actual violation of the HIPAA Security Rules (45 CFR Parts 162 and 45 CFR Part 164, Subpart C), the Privacy Officer and Security Officer will work together to investigate the incident.

3. All investigations will be completed within 30 business days of receipt. If unable to complete the investigation within 30 days, the Privacy Officer may have one 30 day extension granted by the City Manager or designee.

4. The investigation will be documented. As appropriate, the complainant or individual reporting the violation will be interviewed as well as employees and other witnesses.

5. Any related documentation, such as correspondence or existing policies, will be reviewed. The Privacy Officer may request the assistance from other City offices as appropriate (e.g., City Attorney's Office).

C. Violation Determination

1. The Privacy Officer, in consultation with appropriate City staff, will make a determination as to whether the complaint or alleged violation constituted a violation of HIPAA regulations.

2. Except for situations excluded from the definition of "breach" in Section III.A of the regulation, any acquisition, access, use or disclosure of PHI in a manner not permitted under the HIPAA regulations is presumed to be a breach unless the City demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

   a. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

   b. The unauthorized person who used the PHI or to whom the disclosure was made;

   c. Whether the PHI was actually acquired or viewed; and

   d. The extent to which the risk to the PHI has been mitigated.

D. Breach Notification

In the event that a breach of unsecured PHI is discovered, the Privacy Officer, in consultation with appropriate City staff, shall oversee the breach notification process as required by the HIPAA regulations.

1. Breach Notification to Individuals

   a. If it is determined that there was a breach of unsecured PHI, the Privacy Officer and appropriate City staff shall work together to notify each individual whose unsecured protected health information has been, or reasonably believed to have been, accessed, acquired, used, or disclosed as a result of such breach. This notification shall occur without unreasonable delay and in no case later than 60 calendar days after the discovery of the

breach. If a breach is deemed by the Privacy Officer to require immediate notice because of possible imminent misuse of unsecured PHI, notice may be provided to individuals by telephone or other means, as appropriate, in addition to written notice.

b. Written notification must be made to individuals as follows:

i. Written notification must be provided to an individual by first-class mail to the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail.

ii. If the Plan has knowledge that an individual is deceased and has the address of the next of kin or personal representative of the individual (e.g., executor or other person with legal authority to act on behalf of the deceased person or the person's estate), written notification must be provided by first class mail to either the next of kin or personal representative.

iii. The notification may be provided in one or more mailings as information is available.

iv. The notification to affected individuals must include, to the extent possible, the following items:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.

- A description of the types of unsecured PHI that was involved in the breach (such as full name, social security number, date of birth, home address, account number, or diagnosis).

- Any steps individuals should take to protect themselves from potential harm resulting from the breach.

c. Depending on the nature of the breach the following steps may be suggested to individuals:

i. Alert financial institution;

ii. Place fraud alerts on credit files;

iii. Monitor credit files and account statements closely;

iv. Purchase identity theft protection;

v. A brief description of what the Plan is doing to investigate the breach, to mitigate harm to affected individuals, and to protect against further breaches; and

vi. Contact information for individuals to ask questions or request additional information.

d. Substitute Notice: In certain situations the Privacy Officer may determine that a substitute form of notice is required. The standards for providing a substitute notice are as follows:

i. In the case where there is insufficient or out-of-date contact information that precludes written notification to an individual, a substitute form of notice reasonably calculated to reach the individual must be provided.

ii. In the case in which there is insufficient or out-of-date contact information for fewer than ten individuals, then such substitute notice may be provided by an alternative form of written notice, telephone, or other means.

e. In the case in which there is insufficient or out-of-date contact information for ten or more individuals, the substitute notice must be as follows:

i. Be in the form of either a conspicuous posting for a period of 90 days on the home page of the City's website, or conspicuous notice in a major print or broadcast media in geographic areas where individuals affected by the breach reside. The Privacy Officer will work with the City's Public Communications Department to provide the required notification; and

ii. Include a toll-free phone number that remains active for at least 90 days where an individual may call for additional information and to determine if their unsecured PHI may be included in the breach.

2. Media Notification for Breaches of 500 or More Individuals

For a breach of unsecured PHI involving more than 500 individuals the following must occur:

a. The Privacy Officer must provide notification to prominent media outlets serving the City of Chesapeake without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach. The Privacy Officer shall work with the Public Communications Department in order to provide the required notification.

b. The media notification must meet all the requirements set forth in the *Breach Notification to Individuals* section of this policy.

c. Media notification is to supplement, not replace, written notice to affected individuals.

3. Notification to the Department of Health and Human Services

The Privacy Officer, following the discovery of a breach of unsecured PHI, must notify the Department of Health and Human Services (HHS) as follows:

For breaches involving less than 500 individuals, the Privacy Officer must maintain a log or other documentation of such breaches and, not later than 60 days after the end of the calendar year, provide notification to HHS in the manner specified on the HHS website. For breaches involving 500 or more individuals, the Privacy Officer, under the direction of the City Manager or designee, must provide notification to HHS in the manner specified on the HHS website. This notification must be made contemporaneously with the notice provided to individuals affected by the breach.

4. Business Associate Breach Notification

As set forth in its Business Associate Agreement, a Business Associate of the Plan must, following the discovery of a breach of unsecured PHI, notify the Plan of the breach. The Privacy Officer will work with the Business Associate in order to ensure the Plan's compliance with HIPAA regulations.

5. Law Enforcement Delay of Notification

If a law enforcement official notifies the Plan that a notification, notice, or posting required under this policy would impede a criminal investigation or cause damage to national security, the Plan must do the following:

a. Delay such notification, notice, or posting for the time period specified by the law enforcement official, if the official provides a statement in writing that specifies the time for which a delay is required; or

b. Delay such notification, notice, or posting for no longer than 30 days if the official makes the statement orally and the statement is documented by the City employee to whom the statement was directed.

c. Maintain documentation of a law enforcement delay in notification.

E. Documentation

The Privacy Officer is responsible for completing an investigation report which provides a summary of the investigation as well as any recommended policy or procedural changes.

1. The Privacy Officer will provide the appropriate department head a copy of the investigation report if necessary for the department head to take disciplinary action against an employee who committed a violation.

2. In the case of a HIPAA breach, the investigation report will also be submitted to the City Manager or designee.

3. In the case of a HIPAA complaint, the complainant will be informed in writing of the determination and final disposition. However, a complainant will not be informed of any disciplinary action taken against an employee.

4. The Privacy Officer will be responsible for maintaining all documentation related to the investigation for six years from either the date of the investigation's conclusion or the date of last activity regarding the investigation, whichever is later.

F. Refraining from Intimidating or Retaliatory Acts

1. All City employees shall cooperate with any HIPAA investigation conducted by HHS or the Plan.

2. The City and its employees may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise of their rights or for participating in any investigation or

process provided for in this policy, including filing a complaint or reporting a violation.

G. Disciplinary Action

1. Appropriate disciplinary action may be applied against any employee who fails to comply with the HIPAA regulations or any HIPAA policy or procedure.

2. Disciplinary Action will be in accordance with the City of Chesapeake Human Resources Administrative Regulation 2.11 – Disciplinary Policy

VI. RESOURCES

Employees who have questions or concerns should contact the Privacy Officer at HIPAAPrivacyOfficer@cityofchesapeake.net.

APPROVED AS TO FORM AND CONTENT:

Dana E. Sanford, Deputy City Attorney — Date: 2·13·2017

APPROVED AND ADOPTED:

James E. Baker, City Manager — Date: 2/14/17