PERSONNEL POLICY 20-3

SUBJECT: Health Insurance Portability and Accountability Act (HIPAA) Privacy Policy

PURPOSE: To establish policy, and guidance, for HIPAA compliance within the City of Clarksville workforce.

APPLICABILITY: All Departments

REFERENCES: Federal HIPAA Privacy Rule and Law

POLICY STATEMENT: To give the City of Clarksville workforce standard information so that Federal HIPAA laws can be implemented.

RIGHT TO AN ACCOUNTING OF DISCLOSURES:

Under HIPAA, individuals have the right to request an accounting of certain Protected Health Information. (PHI) disclosures. This allows individuals to determine where their PHI has been used and disclosed outside of the normal treatment, payment, and health care operations. As a business associate, in order to respond to individuals' requests for an accounting of PHI disclosures, the City will have to track disclosures made of individual's PHI every time it is used outside of treatment, payment, and health care operations.

1. Individuals have the right to request an "accounting of disclosures." This is a list of the disclosures made of PHI about the individual, that were not made to the individual, pursuant to an authorization by the individual, was not an incidental disclosure or part of a limited data set (data that does not include directly identifiable information), used for research, used for public health purposes, to persons involved in the individual's care, for national security or intelligence purposes, to correctional institutions or law enforcement, for a health care provider or plan's treatment, payment or health care operations, or for disclosures made prior to the date of compliance with privacy standards.

2. Disclosures and requests for an accounting of disclosures will be tracked in the Log of PHI Disclosures form (Appendix A) that will be maintained in the master HIPAA file.

3. To request an Accounting of Disclosures (Appendix B), the individual, or a health care provider on behalf of the individual, must submit a request in writing to the HIPAA Privacy Officer. The request must state a time period that can be no longer than six years.

4. The request will indicate in what form the information is to be delivered (written, electronic, etc).

5. Responses for requests for accounting disclosures will be made within thirty (30) calendar days.

6. If additional time is needed, the individual or covered entity will be informed, within the thirty (30) days, in writing of the delay, the reason for the delay, and the date the accounting will be provided that will be no later than 60 days from the original request.

IMPROPER USES/DISCLOSURES OF PHI:

When any type of improper use/disclosure of PHI is discovered:

1. The City of Clarksville will immediately notify the affected covered entity both by phone call and in writing.

2. The City of Clarksville will immediately provide the Notice of Incident Involving Disclosure of PHI (Appendix C), and the Risk Assessment for Breach of Unsecured Protected Health Information (Appendix D) to the covered entity including:

    a. the details of the improper use/disclosure of PHI
    b. the date the improper use/disclosure of PHI occurred
    c. the date the improper use/disclosure was discovered
    d. a list of names and associated contact information for those individuals whose PHI was affected
    e. what steps those individuals whose PHI was affected should take
    f. what steps The City of Clarksville is taking to mitigate the improper use/disclosure of PHI
    g. Privacy Officer's contact information for further information.

If the improper use/disclosure of PHI involves "unsecured PHI" it has special significance and may constitute a breach under the HIPAA regulations which carries more stringent mitigation/reporting requirements potentially causing the covered entity (and us) to notify the affected individuals, the HHS (Department of Health and Human Services), and the media of the breach. More information about breaches of unsecured PHI is provided below.

DETERMINING IF A BREACH HAS OCCURED

For an acquisition, access, use, or disclosure of PHI to constitute a breach, it must constitute a violation of the HIPAA Privacy Rule. For example, if information is de-identified in accordance with 45 CFR 164.514(b), it is not PHI and any inadvertent or unauthorized use or disclosure of such information will not be considered a breach under the notification requirements of the Act and the Rule.

UNSECURED PHI

The Department of Health and Human Services (HHS) has defined unsecured to mean PHI that has not been:

1. Encrypted consistent with standards set by the National Institute for Standards and Technology; or
2. Destroyed in a manner that renders the information irrecoverable, such as shredding for paper records. Thus, while HIPAA does not require the use of encryption, encrypting PHI can reduce the risk that a covered entity will be required to provide notice of a security breach.

The City of Clarksville will deploy the proper technologies and methodologies that will make PHI unusable, unreadable, or indecipherable to unauthorized individuals. Proper use of such technologies and methodologies will help prevent PHI from becoming Unsecured PHI.

There are two methods for making PHI unusable, unreadable, or indecipherable to unauthorized individuals: encryption and destruction. Below are the guidelines for how these methods apply to the following data states:

1. **Data at Rest** - An encryption process for "data at rest" (i.e., data that resides in databases, file systems, and other structured storage methods) will be valid if it is consistent with National Institute of Standards and Technology ("NIST") Special Publication 800-111, Guide To Storage Encryption Technologies for End User Devices.

2. **Data in Motion** - An encryption process for "data in motion" (i.e., data that is moving through a network, including wireless transmission) will be valid if it complies with the requirements of Federal Information Processing Standards ("FIPS") 140-2.

3. **Data Disposed** - "Data disposed" (e.g., discarded paper records or recycled electronic media) will be properly destroyed if (1) paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed, and (2) electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved

EXCEPTION TO THE BREACH DEFINITION

The following three situations are excluded from the definition of "breach" under the Act:

1. The unintentional acquisition, access, or use of PHI by any workforce member or person acting under the authority of a covered entity or business associate, 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 by the Privacy Rule.

2. The inadvertent disclosure of PHI by an individual otherwise authorized to access PHI at a facility operated by The City of Clarksville to another person at The City of Clarksville, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule.

3. An unauthorized disclosure where a person at The City of Clarksville has a good faith belief that an unauthorized person to whom PHI is disclosed would not reasonably have been able to retain the information.

BREACH NOTIFICATION REQUIREMENTS

If it is determined that a breach has occurred the following steps will apply:

1. A Risk Assessment (RA) will be conducted. If The City of Clarksville can demonstrate through the RA that there is a low probability that the Protected Health Information has been compromised then Breach Notification is not required:

    a. The RA will consider:

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

        ii. The unauthorized person who used PHI or to whom the PHI was disclosed.

        iii. Whether the PHI was actually acquired or viewed.

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

2. If the RA determines that the PHI has been compromised the following steps will be implemented:

    a. The affected covered entity will be immediately notified both by phone call and in writing.

    b. Written documentation to the covered entity will be provided, and will include:

        i. the details of the breach
        ii. whether the breach involved secured or unsecured PHI

iii. the date the breach occurred
iv. the date the breach was discovered
v. a list of names and associated contact information for those individuals whose PHI was breached
vi. what steps those individuals whose PHI was breached should take
vii. what steps we are taking to mitigate the breach
viii. Privacy Officer's contact information for further information.

COMPUTER SYSTEMS:

PASSWORDS

1. All systems will require a valid user ID and password.

2. It is recommended that all users change their passwords at least every 90 days.

3. In the event of a suspected or actual password breach those passwords are to be changed immediately.

4. After three unsuccessful attempts to enter a password, the involved user ID will be suspended until reset by the system administrator.

5. The display or printing of passwords will be masked so that unauthorized parties will not be able to observe or recover them.

6. Passwords will not be stored in written or readable form.

7. Upon termination all passwords for the employee will be immediately changed or deactivated.

ACCESS

1. Computer screens will be positioned in such a manner that only authorized users may see the information contained on the screen.

2. All terminals will have a password protected screen saver that will be activated after no more than fifteen minutes of inactivity.

3. If computer equipment will be permanently taken out of service, the hard drive will be totally erased.

4. Install Antivirus software.

5. Update Antivirus software every six months.

6. Automatic logoff of systems after no more than 30 minutes of inactivity.

7. A notice, at system start-up, warning that only those with proper authority should access the system will be displayed initially before signing onto the system OR a written notice with a warning that only those with proper authority should access the system will be displayed near the computer terminal.

8. Individuals who are not employees, contractors, consultants, or business partners will not be granted access to any systems.

9. Employees will logoff the system before going to lunch or taking breaks.

10. Employees will logoff the system before they end their shift for the day.

11. The room where the workstation is contained will be locked when not in use.

12. All removable media (e.g. CD-ROMs. backup tapes, diskettes, and etc.) will be stored in a locked cabinet to prevent unauthorized use.

13. All removable media (e.g. CD-ROMs backup tapes, diskettes, etc.) no longer in use will be reformatted or destroyed preventing any protected health information from being seen by unauthorized individuals.

14. Printed versions (hardcopy) of protected health information will be shredded before it is discarded.

15. System access will be reviewed annually to remove identification codes and passwords of users who no longer require access.

REMOTE ACCESS

1. Remote access via modem should be through an approved security mechanism such as a dial back system, or only allowing modem connectivity from specific phone numbers.

2. After three unsuccessful attempts to enter a password, the involved user ID will be suspended until reset by the system administrator.

INTERNET

1. Use of the Internet via our network will be primarily for business or professional development.

2. Use of the Internet via our network is not permitted for personal use.

3. A firewall will be installed to protect against unauthorized intrusion.

E-MAIL (ELECTRONIC MAIL)

1. Prohibited use of the electronic mail system includes, but is not limited to:
    a. Disclosure of an individual's personal health information without appropriate authorization.
    b. Transmission of information inside or outside of the organization without a legitimate business need for the information.
    c. Use for marketing purposes without explicit permission of the employee.

2. Employee will be informed about privacy issues such as:
    a. Who besides addressee processes messages.
        i. During addressee's usual business hours.
        ii. During addressee's vacation or illness.
    b. That messages are to be included as part of the medical record.

3. The following types of transactions (prescription refill, appointment scheduling, etc.) and sensitive subject matter (HIV, mental health, etc.) should not be sent over e-mail.

4. Employees will be instructed to put the category of transaction in the subject line of message for filtering: "prescription," "appointment," "medical advice," "billing question."

5. Employees will be instructed to put their name and employee identification number in the body of the message.

6. The sharing of company e-mail accounts with family members is strictly prohibited.

7. Confirm all "To:" fields prior to sending messages.

8. No less than weekly backups of mail onto long-term storage.

9. The use of distribution lists for distributing confidential information is strictly prohibited.

10. The subject line will contain a notation referring to the confidential or sensitive nature of the information.

11. Document employee consent to guidelines for e-mail use:
    a. E-mail will not be used for emergencies or time-sensitive issues.
    b. Privacy and security of e-mail messages is not guaranteed.
    c. Staff other than the intended recipient may read and process e-mail.
    d. Indemnify the City for information loss due to technical failures.

12. Member authorization should be obtained before forwarding protected health information to a third party such as a consultant or health plan.

13. Member e-mail addresses will not be supplied to third parties for advertising.

14. When an e-mail account will not be monitored during a vacation or office closure, an auto reply should be sent notifying the sender that the intended recipient is away.

15. Upon termination of employment the e-mail account will be deactivated.

BACKUP AND RECOVERY

1. A full system backup will be performed every Friday.

2. An incremental backup will be performed Monday, Tuesday, Wednesday, and Thursday.

3. Backup and recovery procedures will be tested at least once a year.

HIPAA Covered Entities:

- **Health Care Providers**: physicians, clinics, hospitals, etc.
- **Health Plans**: employer group health plans, health insurance carriers, etc.
- **Health Care Clearinghouses**: processes/ facilitates processing of health information from a nonstandard format to a standard format.

The City of Clarksville is considered a Business Associate, which is a person or organization that performs a function or activity involving the use or disclosure of PHI (Protected Health Information) on behalf of a covered entity, but is not part of the covered entity's workforce. Business Associates can be but are not limited to the following:

- Claims processors or administrators
- Billing Agencies
- Benefit managers
- Consultants
- Clearing houses
- Storage Facilities
- Lawyers
- Accountants
- Collection Agencies
- Medical Answering Services
- Temporary Staffing Agencies

When business associates are involved in the use or disclosure of PHI while performing a function on behalf of a covered entity, they are expected to adhere to the same standards for safeguarding PHI as the covered entity. Under the recent ARRA/HITECH updates to HIPAA, the Department of Health and Human Services now has direct jurisdiction over business associates. Covered entities and business associates are expected to assure that PHI is used and disclosed appropriately by entering into a Business Associate Contract.

Business associates are required to assure covered entities that PHI will be used and disclosed appropriately by entering into a Business Associate Contract to protect the privacy and security

of PHI.

1. The City of Clarksville will sign a Business Associate Contract with all covered entities from which it receives or will receive PHI.

2. The City of Clarksville will appropriately safeguard any PHI entrusted to our organization.

3. The City of Clarksville will sign an agreement stating that it will not use or disclose PHI in any manner which would not be permissible for the covered entity under the HIPAA privacy regulations.

4. The City of Clarksville will:

    a. Not use or further disclose PHI other than as permitted under the contract or as required by law.
    b. Use appropriate safeguards to prevent use or disclosure of PHI other than provided by the contract.
    c. Report to The City of Clarksville's and covered entity's Privacy Officer any violation of use or disclosure as stated in the contract.
    d. Notify covered entity of any unauthorized acquisition, access, use, or disclosure of unsecured PHI held on covered entity's behalf, including the identity of each individual who is the subject of the unsecured PHI breach.
    e. Ensure that any agents to whom it provides PHI agree to the same restrictions
    f. Provide a list of agents with their contact information that have been granted access to PHI to covered entity's Privacy Officer upon request
    g. Provide proof that our employees and agents have been trained in protecting health information upon request to covered entity's Privacy Officer
    h. Maintain a list of uses and disclosures of individual's PHI outside of treatment, payment, and healthcare operations (for electronic health records, a log of all disclosures including those for treatment, payment, and healthcare operations must be kept) and provide them upon request to help satisfy HIPAA's right for individuals to request an accounting of PHI uses and disclosures.

5. All reported and/or discovered violations of the Business Associate contract will be reported to the City of Clarksville's Privacy Officer as well as the covered entity's Privacy Officer.

EMPLOYEE SANCTIONS:

The purpose of this section is to address non-compliance with the HIPAA policy requirements governing the confidentiality of protected health information (PHI) which includes electronic protected health information (ePHI).

It is the policy of The City of Clarksville to take appropriate steps to promote compliance with the requirements for maintaining the confidentiality of PHI. The City of Clarksville takes

seriously its requirements under HIPAA to protect the confidentiality of PHI and will respond appropriately to violations of HIPAA policies.

The appropriate response to such violations will depend on the severity of the violation, and the record of the employee.

The response will be decided after investigating the specific facts of the situation and may include, but is not limited to, such actions as: system changes, additional education, a written reprimand, a suspension, and termination of employment.

Employees and others who are working on behalf of The City of Clarksville, who report, in good faith, violations of HIPAA policy requirements shall not be retaliated against. They may report any retaliation to their direct supervisor, or the HIPAA Compliance Officer. If reported to anyone other than the HIPAA Compliance Officer, it shall be referred to the HIPAA Compliance Officer. The HIPAA Compliance Officer shall determine who will investigate the matter.

1. It is the responsibility of the HIPAA Compliance Officer to determine the appropriate process to follow when aware of allegations of HIPAA policy violations by an employee. If it is determined that a violation which could result in disciplinary action has occurred, the HIPAA Compliance Officer will work with the appropriate supervisor, and Department Head, to determine the appropriate response.

2. One of the factors to consider when determining the appropriate response for HIPAA policy violations is the severity of the violation. The City of Clarksville has determined that there are four categories of violations.

   Type I – these violations are inadvertent or accidental breaches of confidentiality that may or may not result in the actual disclosure of protected health information (for example, sending an email to an incorrect address).

   Type II – these violations result from failure to follow existing policies/procedures governing security (for example, failure to obtain appropriate authorization to release information, failure to fulfill training requirements).

   Type III – these violations include inappropriately accessing a patient/individual/plan participant's record without a job-related need to know (for example, accessing the record of a friend or co-worker out of curiosity without a legitimate need to know the information).

   Type IV – these violations include accessing and using protected health information for personal gain or to harm another person.

3. In addition to the severity of the violation, factors such as the past record of the employee must be considered. As a result, the appropriate response must be determined on a case-by-case basis. For example, while an inadvertent violation might normally result in

additional education, it could result in more serious action if it was part of a pattern of violations or other performance problems.

All violations must immediately be reported to The City of Clarksville's HIPAA Compliance Officer.

DOCUMENTATION REQUIREMENTS

Each instance of workforce disciplinary action regarding security of PHI is to be documented in a written or electronic record by the HIPAA Compliance Officer. The HIPAA Sanctions Log (Appendix E) will contain the following information:

- Name of employee
- Description of violation
- Level of breach or violation
- Location of breach or violation
- Date and time of breach or violation
- Disciplinary action taken

This documentation must be retained for six years from the date of its creation or the date when it was last in effect whichever is later.

FACSIMILE MACHINES:

Facsimile machines will be kept in secure areas where members of the workforce that do not require routine access to PHI do not have easy access.

SENDING FACSIMILES

Prior to sending the initial facsimile to an entity, the user will verify the facsimile phone number and will call the recipient before sending the facsimile to let them know it is about to be transmitted.

1. A cover letter should precede each facsimile transmission with the following information:

    a. Date and time of transmission.
    b. Sending facility's name, address, telephone number and facsimile number.
    c. Name of person sending the facsimile.
    d. Authorized receivers name.
    e. Number of pages transmitted.
    f. Confidentiality statement, with directions on disclosure and destruction.

2. If a facsimile does not reach its intended destination:

    a. Note in a log.

b. Send a facsimile to that number explaining that the transmission information was misdirected and ask that the documents be returned by US mail.
c. Call intended recipient and verify facsimile information.
d. Notify HIPAA compliance officer.

3. Any facsimile containing protected health information (PHI) will be stored in a secured area where members of the workforce that do not require routine access to PHI will not have easy access.

4. Any facsimile document containing PHI will be shredded before it is discarded.

RECEIVING FACSIMILES

1. When receiving a facsimile transmission:

    a. Remove documents promptly and deliver to intended recipient.
    b. Follow instructions on cover page.
    c. Notify sender of any transmission problems.
    d. Notify the sender of any misdirected documents and either return by mail or destroy depending on the request of the sender.

2. Any facsimile document containing PHI will be shredded before it is discarded.

PHI USE AND DISCLOSURES:

PHI refers to all information (oral, paper-based documents, and electronic documents) that relates to an individual including but not limited to:

- Medical information
- Billing information
- Financial information
- Names and other identifying information such as:
    - Telephone numbers
    - Fax numbers
    - Electronic Mail addresses
    - Social security numbers
    - Medical record numbers
    - Birth date
    - Date of death
    - Health plan beneficiary numbers
    - Account numbers
    - Certificate/license numbers
    - Vehicle identifiers and serial number, including license plate numbers
    - Device identifiers and serial numbers
    - Full face photographic images and any comparable images

- Any other unique identifying number characteristic, or code

MINIMUM NECESSARY

1. When using or disclosing protected health information, employees will take reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

2. The following are situations in which the Minimum Necessary provisions would **not** apply:

   - Uses or Disclosures that are required by law.
   - Uses or Disclosures made to the individual.
   - Uses or Disclosures made pursuant to an authorization.
   - Disclosures to a health care provider for treatment purposes.
   - Disclosures to the Secretary of Health and Human Services for enforcement purposes.
   - Uses or Disclosures that are required for compliance with HIPAA requirements.

3. Before using or disclosing information consider two basic questions:

   a. How much information is needed to fulfill the purpose of this request?
   b. Are we about to provide information that is not necessary to fulfill the purpose of this request?

   For example: When an insurance company requests documentation that the patient was treated for a broken arm, it is not necessary to provide information about the patient's treatment for high blood pressure.

SPECIFIED USE IN BUSINESS ASSOCIATE CONTRACT

Employees will only use PHI given by a covered entity (healthcare provider, health plan, or healthcare clearinghouse) in accordance with the specific use and purpose specified in the Business Associate Contract with the covered entity. The use and purpose should further be confined to purposes of treatment, payment, or healthcare operations for the covered entity or for uses and disclosures for which the covered entity has specific authorization from the individuals (to whom the PHI belongs) to do so.

DISCLOSURE FOR DECEASED INDIVIDUAL

Employees may use and disclose a deceased individual's PHI to family members and others who were involved in an individual's care, unless doing so is inconsistent with any prior expressed wishes or preferences of the deceased individual.

TO AVERT A SERIOUS THREAT TO HEALTH OR SAFETY

Employees may use and disclose PHI about individuals when necessary to prevent a serious threat to the individual's health and safety or the health and safety of the public or another person. Any disclosure, however, would only be to someone able to help prevent the threat.

LAWSUITS AND DISPUTES

PHI may be disclosed in response to a subpoena, discovery request, or other lawful order from a court.

AS REQUIRED BY LAW

Employees will disclose PHI about individuals when required to do so by federal, state or local law.

AS PERMITTED BY LAW

To the extent that the law permits employees to release information, employees may disclose PHI if asked to do so by a law enforcement official as part of law enforcement activities; in investigations of criminal conduct or of victims of crime; in response to court orders; in emergency circumstances.

SUBCONTRACTORS AND AGENTS:

A subcontractor or agent is considered to be a person or organization that creates, receives, maintains, or transmits PHI on behalf of the City of Clarksville. Subcontractors or agents can be but are not limited to the following:

- Claims processors
- Temp/Staffing Agencies
- Billing Companies
- Consultants
- Clearinghouses
- Lawyers
- Accountants
- Collection Agencies
- Record Storage Facilities
- E-Prescribing Gateways

Subcontractors or agents who are involved in the use or disclosure of PHI while performing a function on behalf of the City of Clarksville are expected to adhere to the same standards for safeguarding PHI as the City of Clarksville. The City of Clarksville will assure that PHI is used and disclosed appropriately by:

1. Entering into Business Associate Contracts to protect the security, integrity and confidentiality of PHI.
2. Investigating when complaints or other credible evidence of violations by a subcontractor or agent are received.

3. Taking reasonable steps to correct a breach, notify the Covered Entity of the breach, and if necessary terminate the contract with a business associate after becoming aware of a material breach by a subcontractor or agent.
4. Subcontractors or agents are required to get written assurances from their subcontractors that the subcontractor will adhere to the same standards for safeguarding PHI as we do.
5. The City of Clarksville will obtain satisfactory assurances that the subcontractor or agent will appropriately safeguard any PHI entrusted to it.
6. The subcontractor or agent will sign an agreement stating that it will not use or disclose PHI in any manner that would not be permissible under the HIPAA Security Regulations.
7. The subcontractor or agent will get written assurances from its subcontractors that the subcontractor will not use or disclose protected health information in any manner which would not be permissible for the City of Clarksville under the HIPAA privacy regulations.
8. Existing business associate contracts must be updated to reflect the Omnibus changes in HIPAA law and signed by September 23, 2013, however, the City of Clarksville and our subcontractor or agents must continue to comply with the breach notification interim rules.
9. Subcontractor or agent will:
    a. Not use or further disclose PHI other than as permitted under the contract or as required by law.
    b. Use appropriate safeguards to prevent use or disclosure of PHI other than provided by the contract.
    c. Report to the City of Clarksville's HIPAA Compliance Officer any violation of use or disclosure as stated in the contract.
    d. Notify the City of Clarksville of any unauthorized acquisition, access, use, or disclosure of unsecured PHI they hold on our behalf, including the identity of each individual who is the subject of the unsecured PHI breach.
    e. Ensure that any agents to whom the subcontractor or agent provides PHI agree to the same restrictions.
    f. Provide a list of agents (along with their contact information) that have been granted access to PHI to the City of Clarksville's Security Officer.
    g. Provide proof that its employees and agents have been trained in protecting health information.
10. All reported and/or discovered violations of the subcontractor and agent contract will be recorded and maintained in a file with the signed contract.

If the City of Clarksville becomes aware of a pattern or practice of the subcontractor or agent that constitutes a material breach or violation of the subcontractor's or agent's obligations under its contract, the City of Clarksville will take action (discussions with the subcontractor or agent, sanctions, etc.) to cure the breach or to end the violation. If such steps are not successful the City of Clarksville will terminate the contract if feasible. If it is not feasible to terminate the contract the City of Clarksville will report the problem to the Covered Entity for which the PHI belongs.

WORKFORCE TERMINATIONS:

1. When an individual separates service from the City, both physical and electronic access to information will be denied.

2. New combinations to combination locks will be issued; if a new combination cannot be issued then the combination lock will be changed.

3. Security system access codes will be changed immediately.

4. Security will be notified that the individual separating service is no longer granted access under any conditions.

5. All office staff will be notified that the individual separating service is no longer granted access (keys, combinations, passwords, and etc.) under any conditions.

6. The individual separating service will be removed from all access lists.

7. The individual separating service will turn in their keys, tokens, or cards that allow access to their supervisor or the security officer as part of terms of receiving their final paycheck.

8. All user accounts of the individual separating service will be terminated.

9. Any partners or entities that have access to protected health information will be notified to deny the terminated individual access.

WORKFORCE TRAINING:

1. All current members of the workforce, who are likely to come into contact with protected health information, will be given a HIPAA awareness training and be trained in the policies and procedures with respect to protected health information.

2. New members of the workforce will receive HIPAA awareness training and training in the HIPAA policies and procedures within sixty (60) days of their hire date.

3. If there is a material change in the HIPAA privacy policies and procedures, all members of the workforce, whose duties are directly affected by the change, will be retrained within sixty (60) days.

4. Upon completion of training, members of the workforce will be required to sign the confidentiality agreement (Appendix F) certifying that he or she received the privacy training and will honor the HIPAA privacy policies and procedures.

5. All employees will do a refresher HIPAA Awareness training every year.

Future revisions to this policy can be made, and approved, by the Mayor, Human Resources Director, HIPAA Security Officer, and HIPAA Privacy Officer.

HIPAA Privacy Policy
Official Document
Approved by City Council: November 5, 2020

Will Wyatt, Human Resources Director

RESOLUTION 29-2020-21

A RESOLUTION ADOPTING PERSONNEL POLICY 20-3 PERTAINING TO HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) PRIVACY POLICY

BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY OF CLARKSVILLE TENNESSEE:

That Personnel Policy 20-3 pertaining to Health Insurance Portability and Accountability Act (HIPAA) Privacy Policy, is hereby adopted.

Mayor

ATTEST:

City Clerk

ADOPTED: November 5, 2020