PERSONNEL POLICY 20-4

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

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

APPLICABILITY: All Departments

REFERENCES: Federal HIPAA Security Rule and Law

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

UNIQUE USER IDENTIFICATION AND PASSWORD:

1. Any user or workforce member that requires access to any network, system, or application that accesses, transmits, receives, or stores ePHI, must be provided with a unique user identification string.

2. When requesting access to any network, system, or application that accesses, transmits, receives, or stores ePHI, a user or workforce member must supply his or her previously assigned unique user identification in conjunction with a secure password to gain access.

3. Each user's or workforce member's password must meet the following:

    - Passwords must be a minimum of eight characters in length.
    - Passwords must incorporate at least three of the following four: uppercase, lowercase, number or special character.
    - Passwords must not be words found in a dictionary.
    - Passwords must not include easily guessed information such as personal information, names, pets, birth dates, etc.
    - If a system does not support the minimum structure and complexity as detailed in the aforementioned guidelines, one of the following procedures must be implemented:
        i. The password assigned must be adequately complex to ensure that it is not easily guessed and the complexity of the chosen alternative must be defined and documented.
        ii. The legacy system must be upgraded to support the requirements as soon as administratively possible.
        iii. All ePHI must be removed and relocated to a system that supports the foregoing security password structure.
    - Users or workforce members must not allow another user or workforce member to use their unique user identification or password.

- Users or workforce members must ensure that their user password is not documented, written, or otherwise exposed in an insecure manner.

4. Each user and workforce member must ensure that their assigned user identification is appropriately protected and only used for legitimate access to networks, systems, or applications. If a user or workforce member believes their user identification has been compromised, they must report that security incident to the Security Officer or their immediate supervisor.

EMERGENCY ACCESS

1. Retrieve critical system and data backups from offsite location.

2. Retrieve hardware stored off-site.

3. Restore system and data to hardware.

AUTOMATIC LOGOFF

1. Servers, workstations, or other computer systems containing ePHI repositories must employ inactivity timers or automatic logoff mechanisms. The aforementioned systems must terminate a user session after a maximum of 15 minutes of inactivity.

2. Servers, workstations, or other computer systems located in open, common, or otherwise unsecure areas that access, transmit, receive, or store ePHI must employ inactivity timers or automatic logoff mechanisms. (i.e., password protected screensaver that blacks out screen activity.) The aforementioned systems must terminate a user session after a maximum of 15 minutes of inactivity.

3. Applications and databases using ePHI must employ inactivity timers or automatic session logoff mechanisms. The aforementioned application sessions must automatically terminate after a maximum of 30 minutes of inactivity.

4. Servers, workstations, or other computer systems that access, transmit, receive, or store ePHI and are located in locked or secure environments need not implement inactivity timers or automatic logoff mechanisms.

5. If a system that otherwise would require the use of an inactivity timer or automatic logoff mechanism does not support an inactivity timer or automatic logoff mechanism, one of the following procedures must be implemented:
   - The system must be upgraded to support the required inactivity timer or automatic logoff mechanism.
   - The system must be moved into a secure environment.

- All ePHI must be removed and relocated to a system that supports the required inactivity timer or automatic logoff mechanism.

6. When leaving a server, workstation, or other computer system unattended, workforce members must lock or activate the systems automatic logoff mechanism (e.g. CTRL, ALT, DELETE and Lock Computer) or logout of all applications and database systems containing ePHI.

ENCRYPTION AND DECRYPTION OF EPHI MAINTAINED ON INTERNAL DATABASES

Encryption of ePHI as an access control mechanism is not required unless the custodian of said ePHI deems the data to be highly critical or sensitive. Encryption of ePHI may be required in some instances as a transmission control and integrity mechanism.

FIREWALL USE

1. Networks containing ePHI-based systems and applications must implement perimeter security and access control with a firewall.

2. Firewalls must be configured to support the following minimum requirements:

   - Limit network access to only authorized workforce members and entities.
   - Limit network access to only legitimate or established connections. An established connection is return traffic in response to an application request submitted from within the secure network.
   - Console and other management ports must be appropriately secured or disabled.
   - Implement mechanism to log failed access attempts.
   - Must be located in a physically secure environment.

3. The City must document its configuration of firewalls used to protect networks containing ePHI-based systems and applications. This documentation should include a configuration plan that outlines and explains the firewall rules.

REMOTE ACCESS

1. Dialup connections directly into secure networks are considered to be secure connections and do not require a VPN connection. This implementation of secure remote access extends the secure network to the remote user using a secure PSTN (Public Switched Telephone Network) connection.

2. Authentication and encryption mechanisms are required for all remote access sessions to networks containing ePHI via an ISP (internet service provider) or dialup connection. Examples of such mechanisms include VPN clients, authenticated SSL web sessions, and secured Citrix client access.

3. The following security measures must be implemented for any remote access connection into a secure network containing EPHI:

    - Mechanisms to bypass authorized remote access mechanisms are strictly prohibited. For example, remote control software and applications such as PC Anywhere or GoToMyPC.com are not permitted.
    - Remote access systems must employ a mechanism to "clear out" cache and other session information upon termination of session.
    - Remote access workstations must employ a virus detection and protection mechanism.
    - Users of remote workstations must comply with HIPAA Security Policy - Workstation Use.

4. VPN split-tunneling is not permitted for connections originating from outside the City's network.

5. All encryption mechanisms implemented to comply with this policy must support a minimum of, but not limited to, 128-bit encryption.

WIRELESS ACCESS

1. Wireless access to networks containing ePHI-based systems and applications is permitted so long as the following security measures have been implemented:

    - Encryption must be enabled. (See HIPAA Security Policy – Transmission Security)
    - MAC-based or User ID/Password authentication must be enabled. MAC-based (Media Access Control) authentication is based on a permitted list of hardware addresses that can access the wireless network. MAC addresses are hard coded on each network interface card and typically cannot be changed.
    - All console and other management interfaces have been appropriately secured or disabled.

2. Unmanaged, ad-hoc, or rogue wireless access points are not permitted on any secure network containing ePHI-based systems and applications.

3. All encryption mechanisms implemented to comply with this policy must support a minimum of, but not limited to, 128-bit encryption.

AUDIT CONTROL MECHANISMS:

1. The City must utilize a mechanism to log and store system activity for each system that contains or accesses ePHI.

2. Each system's audit log **must** include, but is not limited to, user ID, login date/time, and activity time. Audit logs **may** include system and application log-in reports, activity reports, exception reports or other mechanisms to document and manage system and

application activity.

3. System audit logs must be reviewed at least once every 180 days.

AUDIT CONTROL AND REVIEW PLAN

1. The audit logs must be reviewed at least once every 180 days.

2. Any potential threats or incidents must be reported to the Security Officer

3. The Security Officer must investigate all reports of threats or incidents.

APPLICATIONS AND DATA CRITICALITY ANALYSIS:

1. The relative criticality of specific applications and data must be assessed for purposes of developing a Data Backup Plan, Disaster Recovery Plan and Emergency Mode Operation Plan.

2. The assessment of data and application criticality should be conducted periodically and at least annually to ensure that appropriate procedures are in place for data and applications at each level of risk.

DATA BACKUP PLAN

1. The City must create and maintain retrievable exact copies of all ePHI.

2. All files, records, images, voice or video files that may contain ePHI, must be backed up.

3. All media used for backing up ePHI must be stored in a physically secure environment, such as a secure, off-site storage facility or, if backup media remains on site, in a physically secure location, different from the location of the computer systems it backed up.

4. If an off-site storage facility or backup service is used, a written contract or Business Associate Agreement must be used to ensure that the Business Associate will safeguard the ePHI in an appropriate manner.

5. Data backup procedures must be tested on a periodic basis to ensure exact copies of ePHI can be retrieved and made available.

DISASTER RECOVERY PLAN

1. The City must restore or recover any loss of ePHI and the systems needed to make that ePHI available in a timely manner, to ensure that the City can recover from the loss of data due to an emergency or disaster such as fire, vandalism, terrorism, system failure, or natural disaster

effecting systems containing ePHI.

2. The City must restore ePHI from data backups in the case of a disaster causing data loss, as follows:

    a. Retrieve critical system and data backups from offsite location.
    b. Retrieve hardware stored offsite.
    c. Restore system data and critical application data to hardware.

3. The City will log system outages, failures, and data loss to critical systems.

4. The disaster recovery procedures outlined above must be tested on a periodic basis to ensure that ePHI and the systems needed to make ePHI available can be restored or recovered.

EMERGENCY MODE OPERATION PLAN

1. The City must establish and implement procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.

2. Emergency mode operation procedures outlined in the Emergency Mode Operation Plan must be tested on a periodic basis to ensure that critical business processes can continue in a satisfactory manner while operating in emergency mode.

INITIAL EVALUATION:

The City's security policies and procedures initially should be evaluated to determine their compliance with the HIPAA Security Regulations. Once compliance with the HIPAA Security Regulations is established, the City's security policies and procedures should be evaluated on a periodic basis to assure continued viability in light of technological, environmental or operational changes that could affect the security of ePHI.

PERIODIC EVALUATION BY HIPAA SECURITY OFFICER

1. The HIPAA Security Officer will review on an on-going basis the viability of the City's security policies and procedures.

2. The HIPAA Security Officer will develop and implement any necessary security policy or procedure changes.

EVALUATION UPON OCCURRENCE OF CERTAIN EVENTS

In the event that one or more of the following events occur, the policy and procedure evaluation process will be immediately triggered:

- Changes in the HIPAA Security Regulations or Privacy Regulations

- New federal, state, or local laws or regulations affecting the privacy or security of protected health information (PHI)
- Changes in technology, environmental processes or business processes that may affect HIPAA security policies or procedures
- A serious security violation, breach, or other security incident occurs

FACILITY SECURITY PLAN:

To safeguard all facilities, systems, and equipment used to store electronic protected health information (ePHI) against unauthorized physical access, tampering, or theft; the City will implement the following:

1. Contingency Operations – allow physical facility access during emergencies to support restoration of data under the Disaster Recovery Plan.

    a. A list containing the names and job titles that will have access to facilities during emergencies will be maintained by the Security Officer.
    b. During emergencies only workforce members and business associates whose names appear on the list will be granted access to systems containing ePHI.

2. Access Control and Validation – Control and validate workforce members' access to facilities based on their role or function.

    a. The Security Officer in conjunction with department supervisors will develop a list based on job function to determine who should have what level of access to systems containing ePHI.
    b. This list will reside with the Security Officer and the department supervisors.
    c. When a workforce member joins a department their physical access to ePHI will be granted based on their job function, as detailed on the access list.
    d. When a workforce member leaves a department all access rights for that workforce member will be revoked.

3. Physical Access Records – log physical access to any facility containing ePHI-based systems. Examples of facilities requiring physical access records are computer and system rooms.

    a. A log to track who entered facilities that house ePHI based systems will be maintained at each facility. The log will track the workforce member's name, identification number (if any) and the time and date they entered the facility.

Maintenance Records – document maintenance, repairs and modifications to the physical security components of the facility including locks, doors, and other physical access control hardware.

b. The log to document repairs to physical security components will be maintained by the Physical Plant Operations Manager (or equivalent) and the Security Officer.
c. The log will document the date and time of the repair, type of repair, and, who performed the repair.

WORKFORCE ACCESS CONTROLS

1. The City must control and validate workforce member access to all facilities used to house ePHI based systems.

    a. Before entering facilities used to house ePHI based systems employees must sign into the access log or show proper organization or plan sponsor issued identification.

2. If the City utilizes employee identification badges the workforce members must wear their identification badges at all times while in facilities that contain systems that house ePHI.

3. Each facility must adopt appropriate access control mechanisms to control physical access to all facilities containing ePHI-based systems. Code locks, badge readers, and key locks are examples of physical access control mechanisms.

4. Workforce members seeking access to any network, system, or application that contains ePHI must satisfy a user authentication mechanism such as unique user identification and password, biometric input, or a user identification smart card to verify their authenticity.

5. Workforce members seeking access to any network, system, or application must not misrepresent themselves by using another person's user ID and password, smart card, or other authentication information.

6. Workforce members are not permitted to allow other persons or entities to use their unique user ID and password, smart card, or other authentication information.

7. A reasonable effort must be made to verify the identity of the receiving person or entity prior to transmitting ePHI.

VISITOR ACCESS CONTROLS

1. The City will control, validate, and document visitor access to any facility used to house ePHI based systems. Visitors include vendors, repair personnel, and other non-workforce members.

2. All visitors who require access to facilities containing ePHI based systems must sign in and provide information regarding their identity and the purpose of their visit.

3. All visitors must be provided a temporary identification badge or be escorted to and from their destination.

ADEQUATE SEPARATION: FIREWALLS:

Included within the City are various support services including, without limitation, legal, accounting, audit, finance, tax, risk management, information systems management, maintenance, facilities, environmental health and safety. Individuals who perform such support services for both HIPAA health care components and non-covered functions shall not use protected health information that they obtain in the course of furnishing services for the HIPAA covered health care components to provide services to the non-covered functions. In addition, when using or disclosing Protected Health Information, the HIPAA covered health care components shall treat the non-covered functions as if they were legally separate entities.

The non-covered entity must:

1. Describe those employees or classes of employees or other persons under the control of the non-HIPAA covered entity to be given access to protected health information; all employees who receive information in the ordinary course of business must be included in the description.

2. Restrict the access to and use by such employees to administration functions that the non-HIPAA covered entity performs.

3. Provide an effective mechanism for resolving any issues of noncompliance by such employees, including disciplinary sanctions.

REPORTING AND RESPONDING TO HIPAA SECURITY INCIDENTS:

All incidents, threats, or violations that affect or may affect the confidentiality, integrity, or availability of electronic protected health information (ePHI) must be reported to your immediate supervisor and/or the Security Officer.

The IT department or IT vendor will investigate and propagate recommended updates or fixes to threatened or actual security incidents. The IT department or IT vendor must also notify the HIPAA Security Officer if a threat to ePHI exists.

Each supervisor must report security incidents to the HIPAA Security Officer. Incidents that should be reported include, but are not limited to:

- Virus, worm, or other malicious code attacks

- Network or system intrusions
- Persistent intrusion attempts from a particular entity
- Unauthorized access to ePHI, an ePHI based system, or an ePHI based network
- ePHI data loss due to disaster, failure, or error

The HIPAA Security and Privacy Officers must notify each other of security or privacy issues.

All correspondence with outside authorities such as local police, FBI, media, etc. must go through the Security Officer.

DOCUMENTATION OF SECURITY INCIDENTS

All HIPAA Security related incidents and their outcomes must be logged and documented by the Security Officer.

MITIGATION OF HARMFUL EFFECTS OF KNOWN SECURITY INCIDENTS

The harmful effects of known security incidents will be mitigated by notifying the Security Officer of a known incident so that appropriate action may be taken.

EPHI TRANSMISSIONS TO NON-ORGANIZATIONS:

To appropriately guard against unauthorized access to or modification of ePHI that is being transmitted from the City to an outside network, the following procedures outlined must be implemented.

1. All transmissions of ePHI from the City's network to an outside network must utilize an encryption mechanism between the sending and receiving entities or the file, document, or folder containing said ePHI must be encrypted before transmission.

2. Prior to transmitting ePHI from the City's network to an outside network the receiving person or entity must be authenticated. (see HIPAA Security Policy - Person or Identity Authentication)

3. All transmissions of ePHI from the City's network to an outside network should include only the minimum amount of ePHI.

EPHI TRANSMISSIONS USING ELECTRONIC REMOVABLE MEDIA

1. When transmitting ePHI via removable media, including but not limited to, floppy disks, CD ROM, memory cards, magnetic tape and removable hard drives, the sending party must:

    - Use an encryption mechanism to protect against unauthorized access or modification.

- Authenticate the person or entity requesting said ePHI in accordance with HIPAA Security Policy - Person or Entity Authentication.
- Send the minimum amount of said ePHI required by the receiving person or entity.

2. If using removable media for the purpose of system backups and disaster recovery and the aforementioned removable media is stored and transported in a secured environment, no additional security mechanisms are required.

EPHI TRANSMISSIONS USING EMAIL OR MESSAGING SYSTEMS

1. The transmission of ePHI from the City via an email or messaging system is permitted if the sender has ensured that the following conditions are met:

    - The recipient has been made fully aware of the risks associated with transmitting ePHI via email or messaging systems.
    - The recipient has formally authorized the City to utilize an email or messaging system to transmit ePHI to them.
    - The recipient's identity has been authenticated.
    - The email or message contains no excessive history or attachments.

2. The transmission of ePHI from the City to an outside entity via an email or messaging system is permitted if the sender has ensured that the following conditions are met:

    - The receiving entity has been authenticated.
    - The receiving entity is aware of the transmission and is ready to receive said transmission.
    - The sender and receiver are able to implement a compatible encryption mechanism.
    - All attachments containing ePHI are encrypted.

3. The transmission of ePHI within the City's network via an email or messaging system is permitted without additional security measures or safeguards so long as only a minimal amount of ePHI is being transmitted and the ePHI is not high risk, sensitive or critical. ePHI that is high risk, sensitive or critical should not be sent through clear text email; such ePHI should be sent via encrypted attachment or other secure measure. If an email or message includes an attachment that contains ePHI, the attachment must be encrypted or password protected before transmission.

4. Email accounts that are used to send or receive ePHI must not be forwarded to non-organization accounts.

EPHI TRANSMISSIONS USING WIRELESS LANS AND DEVICES

1. The transmission of ePHI over a wireless network within the City's network is permitted if the following conditions are met:

- The local wireless network is utilizing an authentication mechanism to ensure that wireless devices connecting to the wireless network are authorized.
- The local wireless network is utilizing an encryption mechanism for all transmissions over the aforementioned wireless network.

2. If transmitting ePHI over a wireless network that is not utilizing an authentication and encryption mechanism, the ePHI must be encrypted before transmission.

INITIAL GRANT OF EPHI ACCESS AND ONGOING SUPERVISION OF EPHI ACCESS:

1. Only workforce members with a need to access ePHI will be granted access to ePHI.

2. The workforce member's supervisor and/or the Security Officer will determine who will require access to ePHI to perform their job functions.

3. The workforce member's supervisor and/or the Security Officer will maintain documentation detailing each workforce member's role and responsibilities, why such workforce members require access to ePHI and the specific levels of ePHI access required by such workforce member.

4. All workforce members who work with ePHI must be supervised so that unauthorized access to EPHI is avoided

ACCESS UPON TRANSFER OF EMPLOYMENT WITHIN THE ORGANIZATION

If a workforce member transfers to another department or workgroup within the organization:

1. The workforce member's access to ePHI within his/her current unit must be terminated as of the date of transfer.

2. The workforce member's new supervisor or manager is responsible for requesting access to ePHI commensurate with the workforce member's new role and responsibilities.

ACCESS UPON TERMINATION OF EMPLOYMENT

The City must implement procedures to ensure that when a workforce member's employment terminates:

1. The workforce member's supervisor or manager ensures that all such workforce member's accounts to access ePHI are terminated.

2. The workforce member's supervisor or manager ensures that such workforce member's access to all facilities housing ePHI is terminated, including but not limited to card access, keys, codes, and other facility access control mechanisms. Codes for key punch

systems, equipment access passwords (routers and switches), administrator passwords, and other common access control information should be changed when appropriate.

3. Access to ePHI is not extended to a workforce member beyond the termination date of such workforce member's employment unless one of the following two conditions have been met:

    - A Business Associate Contract is entered into with such workforce member.
    - The workforce member will be accessing ePHI as in accordance with a HIPAA compliant authorization.

SERVER SECURITY REQUIREMENTS:

1. All servers used to access, transmit, receive or store ePHI must be located in a physically secure environment.

2. The system administrator or root account must be password protected.

3. A user identification and password authentication mechanism must be implemented to control user access to the system.

4. A security patch and update procedure must be established and implemented to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected.

5. Servers must be located on a secure network with firewall protection. If for any reason the server must be maintained on a network that is not secure, an intrusion detection system must be implemented on the server to detect changes in operating and file system integrity.

6. All unused or unnecessary services shall be disabled.

DESKTOP SYSTEM SECURITY REQUIREMENTS

1. Each desktop system used to access, transmit, receive or store ePHI must be located in a physically secure environment.

2. The system administrator or root account must be password protected.

3. A user identification and password authentication mechanism must be implemented to control user access to the system.

4. A security patch and update procedure must be established and implemented to ensure that all relevant security patches and updates are promptly applied based on the severity

of the vulnerability corrected.

5. A virus detection system must be implemented including a procedure to ensure that the virus detection software is maintained and up to date.

6. All unused or unnecessary services must be disabled.

7. Desktop systems that are located in open, common, or otherwise unsecure areas must also implement the following measures:

    - An inactivity timer or automatic logoff mechanisms must be implemented.
    - The workstation screen or display must be situated in a manner that prohibits unauthorized viewing. The use of a screen guard or privacy screen is recommended.

MOBILE SYSTEMS SECURITY POLICY

1. All mobile systems used by workforce members to access, transmit, receive or store ePHI must be appropriately secured.

2. The system administrator or root account must be password protected.

3. A user identification and password authentication mechanism must be implemented to control user access to the system. All mobile devices and laptops must use a boot password to ensure that the system is only accessible to authorized users.

4. A security patch and update procedure must be established and implemented to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected.

5. A virus detection system must be implemented including a procedure to ensure that the virus detection software is maintained and up-to-date.

6. All unused or unnecessary services must be disabled.

7. Mobile stations that are located or used in open, common, or otherwise unsecure areas must also implement the following measures:

    - A theft deterrent device (such as a laptop locking cable) must be utilized when the device is unattended.
    - An inactivity timer or automatic logoff mechanism must be implemented.
    - Reasonable safeguards must be in place to prohibit unauthorized entities from viewing confidential information such as logins, passwords, or PHI.

8. Personal Digital Assistants (PDAs) and other handheld mobile devices must not be used for long-term storage of ePHI. ePHI stored on hand held mobile devices must be purged as soon as it is no longer needed on that device, with a storage time not to exceed 30 days.

9. Each mobile system that is used to access, transmit, receive, or store ePHI must comply with as many of the aforementioned measures as is allowed by the system and operating system architecture.

PASSWORDS:

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

2. Passwords will have the following characteristics:

    a. Passwords will be at least eight characters long
    b. All user-chosen passwords should have at least three of the following four: uppercase, lowercase, number or special character.
    c. The use of control characters and non-printing characters is prohibited

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

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

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

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

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

8. 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. 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.

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

4. Do not access or intercept files or data of others without permission. Do not use the password of others or access files under false identity.

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

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

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

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

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

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

11. 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 specified 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 the City's network will be primarily for business or professional development.

2. Use of the Internet via the City's 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 a member's personal health information without appropriate authorization.
    b. Transmission of information inside or outside of the City without a legitimate business need for the information.
    c. Use for marketing purposes without explicit permission of the workforce member.

2. Sensitive subject matter (HIV, mental health, etc.) should not be sent over e-mail.

3. Workforce members will be instructed to put category of transaction in subject line of message for filtering: "claims question", "eligibility", "enrollment", "billing question".

4. Workforce members will be instructed to put their name and member identification number in the body of the message.

5. All messages will be printed, with replies and confirmation of receipt, and placed in member's record.

6. A message to inform the workforce member of completion of request will be sent.

7. The sharing of City e-mail accounts with family members is strictly prohibited.

8. Workforce members will double-check all "To:" fields prior to sending messages.

9. No less than weekly backups of mail onto long-term storage will be performed.

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

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

12. Workforce member's authorization should be obtained before forwarding protected health information to an external third party not bound by a Business Associate Agreement with the City.

13. Workforce member's e-mail addresses will not be supplied to third parties for advertising or any other use.

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.

MONITORING OF WORKSTATION USE

Workforce members that use the City's information systems and workstation assets should have no expectation of privacy. To appropriately manage its information system assets and enforce appropriate security measures, the City may log, review, or monitor any data (ePHI and non-ePHI) stored or transmitted on its information system assets.

REMOVAL OF WORKFORCE MEMBERS PRIVILEGES

The City may remove or deactivate any workforce member's user privileges, including but not limited to, user access accounts and access to secured areas, when necessary to preserve the integrity, confidentiality and availability of its facilities, user services, and data.

REPORTING COMPLAINTS

Complaints or concerns about another's use of the organization's computer resources should be directed to the Security Officer or your immediate supervisor.

SECURITY REMINDERS:

1. The City will issue security updates to the workforce when changes to the HIPAA Security Rule or the City's HIPAA Security policies and procedures occur.

2. The City will issue warnings to the workforce of potential, discovered or reported threats, breaches, vulnerabilities or other HIPAA security incidents.

3. The City will issue security reminders to the workforce at least once every 12 months.

PROTECTION FROM MALICIOUS SOFTWARE

The City will implement hardware and software to guard against, detect and report to the appropriate persons new and potential threats from malicious code such as viruses, worms, denial of service attacks, or any other computer program or code designed to interfere with the normal operation of a system or its contents and procedures.

1. The City will train its workforce to identify and protect against malicious code and software.

2. Workforce members must notify the HIPAA Security Officer if a virus, worm or other malicious code has been identified and is a potential threat to other systems or networks.

3. The Security Officer is responsible for ensuring that any system that has been infected by a virus, worm or other malicious code is immediately cleaned and properly secured or isolated from the rest of the network.

4. A virus detection system must be implemented on all workstations including a procedure to ensure that the virus detection software is maintained and up to date.

LOG-IN MONITORING

1. The City must implement software to log and document failed login attempts on each system containing ePHI.

2. The organization must review such login activity reports and logs on a periodic basis. The interval of the login activity review must not exceed, but may be less than, 180 days.

3. All failed login attempts of a suspicious nature, such as continuous attempts, must be reported immediately to the HIPAA Security Officer.

PASSWORD MANAGEMENT

To ensure that passwords created and used by the City's workforce to access any network, system, or application used to access, transmit, receive, or store ePHI are properly safeguarded and to ensure that the workforce is made aware of all password related policies, the following minimum procedures must be followed:

1. All workforce members that access networks, systems, or applications used to access, transmit, receive, or store ePHI must be supplied with a unique user identification and password to access the aforementioned ePHI.

2. All workforce members must supply a password in conjunction with their unique user identification to gain access to any application or database system used to create, transmit, receive, or store ePHI.

3. A generic user identification and password may be utilized for access to shared or common area workstations so long as the login provides no access to ePHI. An additional unique user identification and password must be supplied to access applications and database systems containing ePHI.

4. All passwords used to gain access to any network, system, or application used to access, transmit, receive, or store ePHI must be of sufficient complexity to ensure that it is not easily guessable.

5. Managers of networks, systems, or applications used to access, transmit, receive, or store ePHI, must ensure that passwords set by workforce members meet the minimum level of complexity.

6. Managers of networks, systems, or applications used to access, transmit, receive, or store ePHI are responsible for making workforce members aware of all password-related policies and procedures, and any changes to those policies and procedures.

7. Password aging times may be implemented in a manner commensurate with the criticality and sensitivity of the ePHI contained within each network, system, application or database, but are not required.

8. Workforce members are responsible for the proper use and protection of their passwords and must adhere to the following guidelines:

    - Passwords are only to be used for legitimate access to networks, systems, or applications.
    - Passwords must not be disclosed to other workforce members or individuals.
    - Workforce members must not allow other workforce members or individuals to use their password.
    - Passwords must not be written down, posted, or exposed in an unsecure manner such as on a notepad or posted on the workstation.

SECURITY TRAINING PROGRAM

1. The City is responsible for ensuring that its workforce members who have access to ePHI, have the appropriate level of HIPAA Security training so that all workforce members who access, receive, transmit or otherwise use ePHI or who set up, manage or maintain systems and workstations that access, receive, transmit, or store ePHI are familiar with the City's HIPAA Security policies and procedures and their responsibilities regarding such policies and procedures. Appropriate training must consist of, but is not limited to, the following requirements:

    - HIPAA Security Policies
    - HIPAA Business Associate Policy
    - HIPAA Sanction Policy
    - Confidentiality, Integrity and Availability
    - Individual Security Responsibilities
    - Common Security Threats and Vulnerabilities

2. The City is responsible for ensuring all information technology staff members and all workforce members who are responsible for the setup, installation or management of computer systems and networks containing ePHI have the appropriate level of HIPAA Security training. HIPAA Security training for these workforce members must consist of,

but is not limited to, the following requirements:

- HIPAA Security Policies
- HIPAA Business Associate Policy
- HIPAA Sanction Policy
- Confidentiality, Integrity and Availability
- Individual Security Responsibilities
- Common Security Threats and Vulnerabilities
- Password Structure and Management Procedures
- Server, desktop computer, and mobile computer system security procedures, including security patch and update procedures and virus and malicious code procedures
- Device and media control procedures
- Incident response and reporting procedures

3. The City must ensure that the appropriate information technology staff members are aware of and trained to comply with the following HIPAA Security plans and procedures:

   - Log-in monitoring procedures
   - Audit Control and Review Plan
   - Data Backup Plan
   - Disaster Recovery Plan

4. The City must maintain formal documentation of the current level of HIPAA training for each of its workforce members.

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

Official Document
Approved by City Council: November 5, 2020

Will Wyatt, Human Resources Director

RESOLUTION 30-2020-21

A RESOLUTION ADOPTING PERSONNEL POLICY 20-4 PERTAINING TO HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) SECURITY POLICY

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

That Personnel Policy 20-4, pertaining to Health Insurance Portability and Accountability Act (HIPAA) Security Policy, is hereby adopted.

Mayor

ATTEST:

City Clerk

ADOPTED: November 5, 2020