39

City of West Allis
Matter Summary

7525 W. Greenfield Ave.
West Allis, WI 53214

File Number	Title	Status
R-2006-0087	Resolution	In Committee

Resolution relative to adopting policies to comply with the Security Rule of the Health Insurance Portability and Accountability Act.

Introduced: 3/7/2006

Controlling Body: Administration & Finance Committee

COMMITTEE RECOMMENDATION Adopt

ACTION DATE: MAR 07 2006

	MOVER	SECONDER	AYE	NO	PRESENT	EXCUSED
Barczak			✓			
Czaplewski			✓			
Dobrowski						
Kopplin						
Lajsic	✓		✓			
Narlock						
Reinke						✓
Sengstock						
Vitale						
Weigel		✓	✓			
TOTAL			4			1

SIGNATURE OF COMMITTEE MEMBER

Chair _____ Vice-Chair _____ Member _____

COMMON COUNCIL ACTION **ADOPT**

ACTION DATE: MAR 07 2006

	MOVER	SECONDER	AYE	NO	PRESENT	EXCUSED
Barczak		✓	✓			
Czaplewski	✓		✓			
Dobrowski			✓			
Kopplin			✓			
Lajsic			✓			
Narlock			✓			
Reinke						✓
Sengstock			✓			
Vitale			✓			
Weigel			✓			
TOTAL			9	–		1

City of West Allis

Resolution

7525 W. Greenfield Ave.
West Allis, WI 53214

File Number: R-2006-0087

Final Action:
MAR 0 7 2006

Resolution Relative to Adopting Policies to Comply with the Security Rule of the Health Insurance Portability and Accountability Act.

WHEREAS, the City of West Allis must comply with the Security Rule of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"); and,

WHEREAS, the HIPAA Security Rule requires the City of West Allis, as a group health plan, a health care provider and a plan sponsor with access to protected health information, to comply with various security standards which are designed to safeguard all individually identifiable health information that is in electronic form; and,

WHEREAS, it is desirable to have general city-wide policies which address the responsibility of the City of West Allis to safeguard electronic protected health information through administrative procedures, physical safeguards and technical security services and mechanisms.

NOW, THEREFORE, BE IT RESOLVED by the Common Council of the City of West Allis that the attached policies, implementing the security standards of the HIPAA Security Rule, be and are hereby approved for inclusion in the City's Policies & Procedures Manual.

BE IT FURTHER RESOLVED that the City Administrative Officer is authorized and directed to include such policies in the City of West Allis Policies & Procedures Manual and to distribute said policies to all departments, divisions, and offices.

ATTR-Resolution-HIPAA Security Rule

ADOPTED March 7, 2006

Paul M. Ziehler

Paul M. Ziehler, City Admin. Officer, Clerk/Treas.

APPROVED March 9, 2006

Jeannette Bell

Jeannette Bell, Mayor

HIPAA Security Rule – Policies

1. HIPAA Security Management Process
2. HIPAA Assigned Security Responsibility
3. Workforce Security
4. Information Access Management
5. Security Incident Process – Incident Reporting & Sanctions
6. Contingency Planning
7. Evaluation
8. Business Associate Agreements
9. Workstation Use and Security
10. Device and Media Controls – Disposal and Reuse
11. Access Controls
12. Audit Controls
13. Integrity and Transmission Security

HIPAA Security Management Process

1.0 POLICY STATEMENT:

It is the policy of the City of West Allis (the "City") to implement policies and procedures to prevent, detect, contain and correct security violations.

2.0 PURPOSE:

The security management process calls for a risk assessment and analysis to be performed to determine the value of assets and the corresponding exposure to threats and vulnerabilities. Each City Department will utilize this information, as applicable, to manage countermeasures leading to an acceptable level of assurance that systems are secure.

3.0 DEFINITIONS:

Electronic Protected Health Information (EPHI) – Any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media.

Protected Health Information (PHI) – Individually identifiable health information that is created by or received by the City, including demographic information, that identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:

- Past, present, or future physical or mental health or condition of an individual.
- The provision of health care to an individual.
- The past, present, or future payment for the provision of health care to an individual.

3.0 POLICY AND PROCEDURAL STANDARDS:

3.1 POLICY

The security management process will include:

3.1.1 A risk analysis assessing potential risks to the confidentiality, integrity and accessibility of the City's EPHI.

3.1.2 Security measures to reduce risks.

3.1.3 A policy implementing appropriate sanctions against employees who fail to comply with the City's security policies and procedures.

3.1.4 Procedures to regularly review records of information system activity.

3.2 PROCEDURES

The security management process will include the following components:

3.2.1 A risk analysis that includes an accurate and thorough assessment of potential risks and vulnerabilities to the confidentiality, integrity and availability of EPHI held by the City.

3.2.2 A risk management process that implements security measures sufficient to reduce identified risks and vulnerabilities to a reasonable and appropriate level.

3.2.3 A sanction policy and procedures designed to implement appropriate sanctions against employees who fail to comply with the City's security policies and procedures.

3.2.4 Implementation of an information system activity review process that provides regular records reviewing all information system activity, including audit logs, access tracking reports and security incident notifications.

HIPAA Assigned Security Responsibility

1.0 POLICY STATEMENT:

It is the policy of the City of West Allis to have one official designated as the Security Official who is responsible for the development and implementation of the policies and procedures required.

2.0 PURPOSE:

The purpose of this policy is to assure that the responsibility for data security is assigned to a specific individual to provide organizational focus and importance to security and that the assignment is documented. Responsibilities include:

- The management and supervision of the use of security measures to protect data.
- The management and conduct of all personnel in relation to that data.

3.0 DEFINITIONS:

Electronic Protected Health Information (EPHI) – Any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media.

Protected Health Information (PHI) – Individually identifiable health information that is created by or received by the City, including demographic information, that identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:

- Past, present, or future physical or mental health or condition of an individual.
- The provision of health care to an individual.
- The past, present, or future payment for the provision of health care to an individual.

4.0 ASSIGNMENT OF SECURITY RESPONSIBILITY:

The City Administrative Officer of the City of West Allis is designated as the Security Official for the City.

5.0 POLICY AND PROCEDURAL STANDARDS:

5.1 SECURITY RESPONSIBILITY

5.1.1 The Security Official shall be responsible for the development and implementation of policies and procedures to safeguard EPHI within the City's organizational requirements.

5.1.2 The Security Official shall be responsible for supervising the conduct of all personnel in relation to the protection of EPHI.

5.1.3 The Security Official shall designate individuals within each department/division requiring access to EPHI to coordinate and be responsible for the security activities within their department/division.

5.1.4 Each department/division requiring access to EPHI shall have documented security procedures to protect data.

5.1.5 Each department/division requiring access to EPHI shall have security procedures regarding the conduct of their personnel in relation to protection of data.

HIPAA Security Rule
Workforce Security

1.0 POLICY STATEMENT:

It is the policy of the City of West Allis (the "City") to ensure that only employees who require access to electronic protected health information (EPHI) to perform their job duties have such access and that all others do not.

2.0 ORGANIZATIONS AFFECTED:

This policy applies to all departments and employees of the City.

3.0 PURPOSE:

The workforce security process requires authorization and supervision procedures to manage access to protected information utilizing appropriate clearance procedures to approve access and termination procedures when removing access.

4.0 DEFINITIONS:

Electronic Protected Health Information (EPHI) – Any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media.

Protected Health Information (PHI) – Individually identifiable health information that is created by or received by the City, including demographic information, that identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:

- Past, present or future physical or mental health or condition of an individual.
- The provision of health care to an individual.
- The past, present, or future payment for the provision of health care to an individual.

5.0 POLICY AND PROCEDURAL STANDARDS:

5.1 AUTHORIZATION AND SUPERVISION

5.1.1 Each Department, in conjunction with the Information Services Division, shall implement procedures (1) to ensure that those employees requiring access to EPHI have the appropriate access to such information, AND (2) to prevent employees, or any others, who should not have access to EPHI from having access.

5.1.2 Each Department shall document those employees/positions within the Department that have authority to access EPHI.

5.2 WORKFORCE CLEARANCE PROCEDURE

5.2.1 Each Department shall have a screening process for granting access to EPHI.

5.2.2 The City shall assess the potential risk related to the hiring, promotion and transfer of employees into positions allowing access to EPHI.

5.2.3 The City shall require that all employees given access to EPHI receive training on the EPHI security requirements and on City policies that implement the EPHI security requirements.

5.2.4 Each Department shall keep records of any unauthorized access and/or inappropriate disclosure of EPHI and immediately notify the Personnel Division any time there is an unauthorized access or disclosure.

5.2.5 The City shall take preventative measures to ensure that unauthorized persons are prevented from accessing EPHI.

5.3 TERMINATION PROCEDURE

5.3.1 The City shall document procedures for denying physical and electronic access to terminated employees.

5.3.2 The City shall document procedures for processing change of authorization status for employees.

5.3.3 The City shall document procedures that require individuals who are terminated to surrender any EPHI in their possession before they depart.

5.3.4 The City shall have a documented termination procedure to remove employees from access lists when they no longer need to have access, or when they are terminated, and that shows the procedure for removing access is being followed.

HIPAA Security Rule
Information Access Management

1.0 POLICY STATEMENT:

It is the policy of the City of West Allis to maintain information access controls creating the ability to know whom and when a person may view, modify, or disclose electronic protected health information (EPHI).

2.0 ORGANIZATIONS AFFECTED:

This policy applies to all departments and employees of the City of West Allis having access to EPHI.

3.0 PURPOSE:

Access management protects information resources from unauthorized viewing, modification, or disclosure.

4.0 DEFINITIONS:

Electronic Protected Health Information (EPHI) – Any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media.

Protected Health Information (PHI) – Individually identifiable health information that is created by or received by the City, including demographic information, that identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:

- Past, present, or future physical or mental health or condition of an individual.
- The provision of health care to an individual.
- The past, present, or future payment for the provision of health care to an individual.

5.0 POLICY AND PROCEDURAL STANDARDS:

5.1 ACCESS AUTHORIZATION

5.1.1 The individual in each department/division designated by the Security Official to coordinate and be responsible for the security responsibilities within their department/division, shall establish the information access procedure within their department/division in accordance with City of West Allis procedure.

5.1.2 The individuals designated to assume the security responsibilities, including access procedures, within their department/division shall receive training in HIPAA and any other legal requirements, as needed.

5.1.3 Each department/division requiring access to EPHI shall have an access authorization procedure.

5.1.4 Each department/division requiring access to EPHI shall define what is "authorized use" of EPHI and shall ensure that employees understand what such use is.

5.1.5 Each department/division having access to EPHI shall have a procedure for the secure transfer of EPHI to another authorized person or entity.

5.1.6 Each department/division having access to EPHI shall periodically review with its employees the policies and procedures for access to EPHI.

5.1.7 Each department/division requiring access to EPHI shall have a process to rapidly validate who, in their department/division, has access to EPHI.

5.2 ACCESS ESTABLISHMENT AND MODIFICATION

5.2.1 Each department/division having access to EPHI shall implement procedures that require an individual to acknowledge the responsibility granted with the access to EPHI.

5.2.2 Each department/division having access to EPHI shall implement procedures that require training of an individual prior to gaining access to EPHI.

5.2.3 Each department/division requiring access to EPHI shall notify the Personnel Division and the Information Services Division of any access changes that must be made as a result of a change in a job description, an employee transfer, an employee resignation or termination, or other such actions.

5.2.4 Each department or division requiring access to EPHI shall immediately change all passwords that may have been known or compromised by an employee who is terminated or resigns.

5.2.5 Each department/division requiring access to EPHI shall, in conjunction with the Information Services Division, have a plan in place to deal with external threats to information security.

HIPAA Security Rule
Security Incident Process – Incident Reporting & Sanctions

1.0 POLICY STATEMENT:

It is the policy of the City of West Allis (the "City") to report and respond to information security incidents and to establish and apply sanctions against officers and employees who violate the City's privacy and/or security policies that relate to the privacy and security of protected health information (PHI) whether in written or electronic form.

2.0 ORGANIZATIONS AFFECTED:

This policy applies to all departments and employees of the City of West Allis.

3.0 PURPOSE:

The purpose of this policy is to assure that City Departments and Divisions employ a consistent and effective method of identifying, documenting, and reporting privacy and security incidents and responding accordingly.

4.0 DEFINITION:

Protected Health Information (PHI) – Individually identifiable health information that is created by or received by the City, including demographic information, that identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:

- Past, present, or future physical or mental health or condition of an individual.
- The provision of health care to an individual.
- The past, present, or future payment for the provision of health care to an individual.

5.0 POLICY AND PROCEDURAL STANDARDS:

5.1 POLICY

5.1.1 Officers and employees are subject to disciplinary action, up to and including termination, for violation of privacy and security policies and procedures. Disciplinary action is utilized in order to hold officers and employees accountable for their behavior as it relates to the use and disclosure of PHI.

5.1.2 Officers and employees are trained on the consequences of violating privacy and security policies. Training occurs upon initial employment and then on a routine and recurring basis.

5.1.3 Officers and employees will be treated fairly and equitably in the imposition of sanctions for privacy and security violations. Discipline will be applied consistently throughout the Departments and Divisions of the City. Any and all breaches of privacy and security policies will result in immediate consequences regardless of job status or reason for violation.

5.1.4 Discipline will be imposed in accordance with the applicable procedures set forth in the Revised Municipal Code, the Civil Service Commission Rules and Regulations, and the Policies and Procedures Manual.

5.1.5 Management reserves the right to monitor system and media device activity to ensure the enforcement of policies.

5.1.6 Disciplinary actions due to breaches of privacy or security of PHI will be reported to, documented by and retained in the Personnel Division. The documentation shall be retained for six years.

5.2 PROCEDURE

5.2.1 Any known or suspected violation of the City's Privacy and/or Security Policies and Procedures shall be reported immediately to the Personnel Manager.

5.2.2 Upon receipt of the report or notification, the Personnel Manager shall convene as deemed necessary with the Privacy and/or Security Official, the appointing authority of the officer/employee alleged to have violated the policies and procedures, the Information Services Manager and the City Attorney's Office to determine the appropriate action to be taken including investigation, mitigation of potential damage caused by the violation, and discipline. It shall be the responsibility of the appointing authority to address the alleged violation with the officer/employee and to determine and impose the appropriate discipline, if any. Said action shall be reported to the Personnel Division.

5.2.3 The Personnel Manager shall document disciplinary actions, and shall retain the documentation for at least six years.

HIPAA Security Rule
Contingency Planning

1.0 POLICY STATEMENT:

It is the policy of the City of West Allis (the "City") to maintain a contingency plan for short-term losses and interruptions to the critical functions of information systems.

2.0 PURPOSE:

The contingency plan addresses the steps taken to maintain critical functions in the event of losses, disruptions, or disasters impacting information systems. When developing requirements for a contingency plan, provisions for periodic data backup, availability of critical facilities in conjunction with centralized Information Services (IS) operations, and disaster recovery procedures shall be taken into account.

To satisfy the requirements of contingency planning, the following elements shall be included in the contingency plan:

- Strategies and procedures to ensure contingency of information systems.
- Periodic recovery testing to ensure viability of recovery plans.
- Procedures to store and recover media from offsite storage ensuring the availability of that media.
- Processes to monitor computer and network operations to mitigate interruptions.
- Recovery tools and offsite facilities to support timely recovery in the event of a disaster.

3.0 DEFINITIONS:

Electronic Protected Health Information (EPHI) – Any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media.

Protected Health Information (PHI) – Individually identifiable health information that is created by or received by the City, including demographic information, that identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:

- Past, present, or future physical or mental health or condition of an individual.
- The provision of health care to an individual.
- The past, present, or future payment for the provision of health care to an individual.

4.0 POLICY AND PROCEDURAL STANDARDS

4.1 POLICY

4.1.1 In order to assure that electronic protected health information is available, secure, and has not been changed or tampered with, the City maintains a Contingency Plan. The Contingency Plan provides a mechanism to:

- Avoid interruptions to critical functions even while undergoing a loss of electricity, fire, vandalism, true disaster, or other occurrence where systems and data are threatened.
- Minimize impact on total business operations, minimize interruptions to critical functions so that they occur only infrequently, are brief in duration, and do not result in detrimental consequences.
- Address complications and consequences of normal lost processing time, operations degradation, lost equipment replacement processes, insurance funds, alternative processing sites, temporary office space, equipment, key personnel, telephones, and other business basic equipment.

4.1.2 The Information Services Manager, working with other key management personnel, is responsible to create, obtain Common Council approval, implement, and maintain a comprehensive Contingency Plan including the following components:

- Data Back up Plan – Provides for the creation and maintenance of an exact retrievable copy of all City EPHI. It may also include maintenance and retrieval of paper files of protected health information.
- Disaster Recovery Plan – Defines procedures to restore any loss of data and equipment due to an emergency, power loss, fire, vandalism, natural disaster, or other occurrences.
- Emergency Mode Operation Plan – Allows for continuation of critical business processes for protection and security of PHI even during emergency mode operations.
- Testing and Revision – Allows for routine testing of contingency plans as necessary in accordance with the City's system complexity.
- Applications and Data Criticality – Based upon system complexity and importance, this process allows for the prioritization of system applications and related data in order to support resumption of normal business/system processing.

5.0 PROCEDURE:

5.1. LEVEL OF EMERGENCY RESPONSE

In an unexpected event such as a fire, loss of electricity, vandalism or other disaster the City's usual security measures may become disabled, or may be ignored or not observed by employees. Therefore, responses must be preplanned, communicated and documented in training materials so that employees can carry out a series of actions and reactions that range from manual to highly complex processes. Based upon the level of functional loss (short term disruption of computer systems versus projected number of days in alternative working site), various responses will be performed. All actions will result in maintaining the ongoing operations of those functions deemed most critical to the City.

5.2 PRIORITIZE ACTIONS BASED ON PROBABILITY

The IS Manager will work with others to develop a list of possible threats that have a certain probability of occurring on-site. The level of probability that will trigger a specific level of

contingency plan is a component of the Risk Analysis and Management process. However, some more common threats ranging in probability from high to low may include:

- Computer System disruption in connectivity resulting in delayed processing time or rework.
- Loss of electrical power, lights, telephones and other office equipment due to thunderstorm, power outage and other such natural events.
- Fire, earthquake, tornado or other disaster where all or part of the actual facility is destroyed, resulting in need to set up temporary work location.

5.3 DATA BACK UP PLAN

5.3.1 The City requires the creation and maintenance of an exact retrievable copy of the City's EPHI. As such, back-ups are created in the most appropriate form (zipped diskette, tape, CD Rom, FTP copy, etc.) and in a timely manner.

5.3.2 Scheduling, Labeling, and Off-Site Storage. One copy (daily, weekly, or monthly version) is labeled and maintained on the City's premises in a secure manner. An additional copy is maintained off-site in a manner that is environmentally secure and limited by physical access controls to protect improper modification, allowing access only by the IS Manager or designee.

5.3.3 In the instance that back-up data is used to restore system operations, all system defaults will be reset by the IS Manager.

5.3.4 Old production programs shall be retained as back up until testing and revision plans procure satisfactory results.

5.4 DISASTER RECOVERY PLAN – REQUIRED PROCEDURE TO RESTORE LOSS OF DATA

The IS Manager will work with others as necessary to compile and maintain the information outlined below to be stored in multiple formats, on and off site to be used in the event of an emergency. This critical Disaster Recovery Plan Outline allows for orderly resumption of activities and resumption of system recovery to the point of failure.

Establish Comprehensive Lists
List of officers/employees responsible to carry out response contingency processing (include name and emergency contact information), and (as deemed necessary):

- Inventories
- Floor Plans
- List of back up systems/data, location and contact
- Critical forms and supplies stocked off-site
- Contract for back-up agreement for space, processing hardware and software and resources on an emergency basis, including method of retracting and utilizing data history
- Processing priorities pre-approved by management. (Sequence of importance of each application)
- System application and documentation (current copies of all applications need to be located on an off site in a secure manner)

- Testing an Revision Plans
- List of job categories and/or individuals responsible for recovery of computer and other systems Job categories may include restoring operations, and/or retrieving previously backed-up data
- List of all critical business partners and emergency contact information [*Note: Step-by-step procedures are very important in a Disaster Recovery Plan. Often during a disaster emotions are running high and even the best employees might forget an important step*]

5.5 EMERGENCY MODE OPERATION PLAN

The City requires defined processes to protect EPHI during and immediately after a crisis while operating in emergency mode. Basic elements include definition of the notification process, clear pre-defined instructions on work around procedures, crisis management information and business continuity planning. This may include administrative safeguards, physical safeguards and access of workforce to site (or alternative sites), limitation of electronic and other technical safeguards including access via "Electronic Access Control" to protect and secure PHI even during emergency mode operations. This most likely includes adequate manual processes for use until automated operations are restored.

5.6 TESTING AND REVISION

Based upon Risk Analysis results, system and configuration complexity, each component of the Contingency Plan is identified, evaluated, and prioritized for any necessary routine testing and adjustment or revision. Test plans (for the level of testing deemed appropriate) should be clearly documented and include instruction to notify involved parties of the occurrence of the test, disaster simulation, and relocation as well as a defined timeline.

HIPAA Security Rule
Evaluation

1.0 POLICY STATEMENT:

It is the policy of the City of West Allis (the "City") to evaluate its compliance with the Security Rule policies and procedures, both technical and non-technical in nature, which have been implemented in order to ensure the confidentiality, integrity, and availability of all protected health information.

2.0 PURPOSE:

To assure that the City has an effective method available for evaluating the success of the respective policies and procedures.

3.0 POLICY AND PROCEDURAL STANDARDS:

3.1 POLICY

The City, by means of the Information Services Division, in conjunction with Department/Division Heads as deemed necessary, shall perform periodic technical and non-technical evaluations, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of protected information.

3.2 PROCEDURES

3.2.1 Based upon workforce experience, objectivity, and availability, the Information Services Division shall conduct internal evaluations of the City's security compliance.

3.2.2 The goal of the evaluation is to conduct a review of the City's security safeguards in order to demonstrate and document compliance with the HIPAA Security regulations on an ongoing basis.

3.2.3 An evaluation may include:

- Evaluating risk analysis findings to make sure all vulnerabilities have been fixed or corrected to an acceptable level.
- Periodic audit or review of procedures such as sanction and termination policies to make sure they were conducted in accordance with written policies and procedures.
- Review or testing of access controls to assure they balance the protection of electronic protected health information while allowing appropriate access so as not to negatively impact the health care process.

HIPAA Security
Business Associate Agreements

1.0 POLICY STATEMENT:

It is the policy of the City of West Allis (the "City") to only share protected health information (PHI) with a business associate pursuant to a written agreement that provides assurance that appropriate safeguards providing for the confidentiality, integrity, and availability of protected data will be maintained.

2.0 ORGANIZATIONS AFFECTED:

This policy applies to all City departments having access to PHI.

3.0 PURPOSE:

The purpose of this policy is to set forth the requirements necessary to document the City's efforts to assure that business associates comply with privacy and security standards, and that the City knows of and has an opportunity to take remedial action regarding any breach there under.

4.0 DEFINITIONS:

Business Associate – A person or organization that performs a function or activity involving the use or disclosure of PHI, on behalf of the City. A person or organization who only assists in the performance of the function or activity is also a business associate. This includes a person or organization that receives PHI *from* the City, and one who obtains PHI *for* the City. This includes, for example: data analysis; processing or administration; billing; collections; benefit management; legal services; consulting; management and administrative services; or any other service in which the person or organization obtains PHI from or for the City.

Protected Health Information (PHI) – Individually identifiable health information that is created by or received by the City, including demographic information, that identifies an individual, or provides a reasonable basis to believe that information can be used to identify an individual, and relates to:

- Past, present, or future physical or mental health or condition of an individual.
- The provision of health care to an individual.
- The past, present, or future payment of the provision of health care to an individual.

5.0 POLICY AND PROCEDURAL STANDARDS:

5.1 POLICY STANDARDS

5.1.1 City Departments having access to PHI shall be able to identify the situations where a business associate agreement must be in place.

5.2 ORGANIZATION REQUIREMENTS

5.2.1 City departments having access to PHI shall implement procedures to establish and manage agreements with business associates.

5.2.2 The business associate agreements shall contain all of the provisions as defined in the Administrative Simplification Act.

5.3 ADMINISTRATIVE STANDARDS

5.3.1 Written business associate agreements shall be executed with each organization that is used to create, receive, maintain, or transmit electronic PHI on the City's behalf. The Agreement shall contain assurances that the business associate will appropriately safeguard the confidentiality, integrity and availability of the data.

5.3.2 Business associate agreements will be entered into with all third parties that process PHI.

5.3.3 The business associate agreements shall explicitly state requirements for ensuring the confidentiality and integrity of data.

5.3.4 The business associate agreements shall explicitly state requirements for the availability of data.

5.3.5 The business associate agreements shall require business associates to report any security incidents of which they become aware.

5.3.6 The business associate agreements shall require that the business associates make their policies and procedures and their documentation related to their safeguards available to the Secretary of the Federal Department of Health and Human Services when determining compliance with applicable security regulations.

5.3.7 The business associate agreements shall authorize remediation or termination of any contract for services related to electronic PHI if the City determines that the business associate has violated the agreement.

5.4 PROCEDURAL STANDARDS

5.4.1 The City shall maintain the right to audit the security measures of third parties who process its PHI.

HIPAA Security Rule
Workstation Use and Security

1.0 POLICY STATEMENT:

It is the policy of the City of West Allis (the "City") to specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of workstations that can access EPHI. It is also the City's policy to restrict access to authorized users by implementing physical safeguards for all workstations that access EPHI.

2.0 ORGANIZATIONS AFFECTED:

This policy applies to all departments and employees of the City of West Allis.

3.0 PURPOSE:

Establishing appropriate workstation utilization procedures and preventing unauthorized viewing of information visible on monitors and physical access to the system itself in order to prevent the incidental and unauthorized access and release of information.

4.0 DEFINITIONS:

Electronic Protected Health Information (EPHI) – Any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media.

Protected Health Information (PHI) – Individually identifiable health information that is created by or received by the City, including demographic information, that identifies an individual, or provides a reasonable basis to believe that information can be used to identify an individual, and relates to:

- Past, present, or future physical or mental health or condition of an individual.
- The provision of health care to an individual.
- The past, present, or future payment for the provision of health care to an individual.

5.0 POLICY AND PROCEDURAL STANDARDS:

5.1 POLICY

5.1.1 The City will have secure work areas containing workstations with physical safeguards to minimize the possibility of unauthorized observation or access to PHI. Areas where sensitive information is regularly accessed, entered or utilized will be secured using barriers to prevent public viewing of PHI.

5.1.2 If an employee accessing sensitive information must leave the workstation at any time, it will be his or her responsibility to remove the information being accessed from the workstation screen, or to cover or file information being accessed in hard copy. At no time will such information be allowed to remain in plain view and unattended.

5.1.3 Printers and fax machines, copy machines, and shredders will be located in the most secure areas available, and will not be located in or near areas frequented by the public. The City will also provide appropriate security measures for portable workstations containing PHI.

5.2 PROCEDURES

5.2.1 PHI can never be left unattended. Therefore employees with access to PHI must always lock or log out of their station before leaving it unattended. Employees must always lock away or turnover or otherwise make hard copy containing PHI inaccessible to local foot traffic.

5.2.2 City workstations and work areas that are used to access PHI are located in controlled areas that have physical protections including locks, key cards, or similar devices.

5.2.3 The City utilizes workstation inactivity timeouts and password-protected "screen savers."

5.2.4 The City takes steps to prevent unauthorized persons from casually viewing workstations or work areas located in public areas by locating monitors behind petitions or similar barrier, or by installing blinds, covers or enclosures about monitors, using polarizing filters, or other similar approved methods.

5.2.5 The City positions monitors away from outside windows and public areas.

5.2.6 In order to emphasize the security of the physical environment and location considerations where electronic computing devices containing PHI are kept, the individuals who have been assigned the responsibility within each department/division for the EPHI security activities, will periodically review the location and placement of all workstations, printers, facsimile machines, copy machines, shredders, and all other areas where sensitive information is accessed, reviewed or processed within their department/division. This may include inspecting content of data contained on workstations in order to determine if it is business related and appropriate. If necessary, the individuals so assigned will make changes to assure compliance with the requirements of this policy, which may include relocation or physical changes to the work area. All changes will be documented.

HIPAA Security Rule
Device and Media Controls – Disposal and Reuse

1.0 POLICY STATEMENT:

It is the policy of the City of West Allis to ensure the privacy and security of electronic protected health information (EPHI) in the maintenance, retention, and eventual destruction/disposal of such media.

2.0 ORGANIZATIONS AFFECTED:

This policy applies to all departments and employees of the City of West Allis.

3.0 PURPOSE:

Device and media controls are designed to control the disposal and reuse of any and all electronic media containing EPHI.

4.0 DEFINITIONS:

Electronic Protected Health Information (EPHI) – Any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media.

Protected Health Information (PHI) – Individually identifiable health information that is created by or received by the City, including demographic information, that identifies an individual, or provides a reasonable basis to believe that information can be used to identify an individual, and relates to:

- Past, present, or future physical or mental health or condition of an individual.
- The provision of health care to an individual.
- The past, present, or future payment for the provision of health care to an individual.

5.0 POLICY AND PROCEDURAL STANDARDS:

5.1 DEVICE AND MEDIA DISPOSAL AND REUSE

5.1.1 The Information Services (IS) Manager is responsible for retrieval, sanitization and proper disposal of all devices and media containing EPHI. All devices and media equipment including storage media in personal computers and other hardware containing EPHI shall be sanitized prior to disposal or reuse. Documentation of the sanitization and/or disposal procedure taken for any such device or media shall be maintained by the IS Manager.

5.1.2 The disposal and sanitization of EPHI shall be carried out in accordance with federal and state law and as defined in the City of West Allis record retention policy.

HIPAA Security Rule
Access Controls

1.0 POLICY STATEMENT:

It is the policy of the City of West Allis (the "City") to maintain mechanisms for access control to information technology resources and sensitive data for routine and emergency operations.

2.0 DEFINITIONS:

Electronic Protected Health Information (EPHI) – Any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media.

Protected Health Information (PHI) – Individually identifiable health information that is created by or received by the City, including demographic information, that identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:

- Past, present, or future physical or mental health or condition of an individual.
- The provision of health care to an individual.
- The past, present, or future payment for the provision of health care to an individual.

3.0 POLICY AND PROCEDURAL STANDARDS:

3.1 POLICY

3.1.1 The City will implement technical policies and procedures for electronic information systems that maintain EPHI to allow access only to those persons or software programs that have been granted access rights.

3.1.2 The Information Services Division, in coordination with department heads and the Privacy Officer/Security Official, will be responsible for development, implementation and monitoring of policies and procedures that allow access only to those persons or software programs that have been granted access rights.

3.1.3 Access controls will include:

- Unique User Identification: The assignment of unique name and/or number for identifying and tracking user activity.
- Emergency Access Procedure: Establish and implement procedures obtaining necessary EPHI during an emergency.
- Automatic Log-off: Implementation of automatic log-off mechanisms that terminate access after a predetermined time of inactivity.
- Encryption and Decryption: Implementation of a mechanism to encrypt and decrypt EPHI, to the extent reasonable, as a means of controlling access to EPHI.

3.1.4 Access controls are intended to regulate the following functions:

- Provide authorized users access on information systems to perform functions necessary for their related workforce duties.
- Regulate access according to the person or class of persons and functions they perform.

3.2 PROCEDURES

3.2.1 The Information Services Division will be responsible for development, implementation and monitoring of policies and procedures for technical access controls.

3.2.2 Technical access controls will be implemented based on authorization of access determined by department heads over EPHI.

3.2.3 The Information Services Division will determine and implement appropriate technical access controls for the City.

HIPAA Security Rule
Audit Controls

1.0 POLICY STATEMENT:

It is the policy of the City of West Allis (the "City") to maintain processes for recording and auditing information system activity with respect to electronic protected health information (EPHI).

2.0 PURPOSE:

When implementing technical safeguards the City is required to maintain logs of system activity. These system activity logs are required in order to recreate pertinent system events (including physical activities) and actions taken by system users and administrators. The audit process of examining logged information is required in order to identify questionable data access activities, investigate breaches, access the security program, and aid in responding to potential weaknesses.

3.0 PROCEDURES:

3.1 The Information Services (IS) Division will evaluate current hardware and software to determine whether they contain the capability to record and examine activity in the information systems that contain EPHI.

- Can the hardware/software audit access?
- Can the hardware/software track activity in the system?
- Can the hardware/software track who is logging in and/or off, who is changing files and/or what are they changing?

3.2 Based on the findings of the above evaluation, the IS Division will take appropriate action.

- If the current hardware and software are capable of recording and examining activity in the information system, the IS Division will continue to monitor and update the systems as appropriate and reasonable.
- If the current hardware and software do not have recording and examining capabilities, the IS Division, to the extent reasonable, will need to update the hardware and software to accomplish these activities.

3.3 The IS Division shall implement and maintain audit logs for the purpose of examining and recording access activity of EPHI. The audit logs should provide a chronological trail of computer events that gives information about an operating system, an application or user access. The audit logs will be used to monitor computer activity to assist in determining:

- Whether a security incident has occurred.
- Whether there is an indication of unauthorized access.
- Whether there is unusual employee access.
- Whether there is unusual activity that requires further investigation.

3.4 The IS Division will document the examination and recording activities of the information system. The documentation shall be maintained by the IS Division for a minimum of six years from the date of creation.

HIPAA Security Rule
Integrity and Transmission Security

1.0 POLICY STATEMENT:

It is the policy of the City of West Allis (the "City") to protect electronic protected health information (EPHI) from improper alteration and/or destruction and to maintain security measures to guard against unauthorized interception, redirection and/or modification of protected health information (PHI) transmitted by the City over electronic networks.

2.0 POLICY AND PROCEDURAL STANDARDS:

2.1 POLICY

2.1.1 The City, by means of the Information Services (IS) Division, will implement electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner.

2.1.2 The City, by means of the IS Division, will, to the extent reasonable, develop, implement and monitor technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network.

2.2 PROCEDURES

2.2.1 The IS Division will implement all reasonable mechanisms to ensure data accuracy and transmission security when it is transferred between computers, read from electronic media, and/or transmitted over an electronic communications network.

2.2.2 Mechanisms to ensure data accuracy and transmission security may include:

- Prevention of exposure to excessive heat or magnetic fields.
- Intrusion detection systems that provide an alert when hacking occur.
- Continuing and dependable computer backup.
- Updated programs that have resolved known "bugs."
- Use of anti-virus software.
- Assurance of integrity by network configuration.
- Encryption mechanisms.

2.2.3 The IS Division will document implementation of all electronic mechanisms to corroborate that EPHI has not been accessed, altered or destroyed in an unauthorized manner and will document all activities related to technical security measures relating to transmission of EPHI.

2.2.4 The documentation will be maintained and retained for a period of at least six years from the date of creation.