

File Reference No.: 20030243

ORDINANCE NO.: 6491

AN ORDINANCE

AMENDING

City Code Section 4-12-2 to adopt a new Code Section 4-12-2-025 entitled Employee Health Insurance and Protected Health Information and amending City Code Section 4-4-11 to adopt a new Code Section 4-4-11-30 entitled Information Security Policy.

NOW, THEREFORE, BE IT HEREBY ORDAINED BY THE MAYOR AND COUNCIL OF THE CITY OF MARIETTA, GEORGIA:

Section 1: That a new City Code Section 4-12-2-025 be adopted to read as follows:

4-12-2-025 Employee Health Insurance and Protected Health Information

A. Purpose: To establish privacy procedures to assure that the confidentiality of individually identifiable health information is protected, to inform employees of their privacy rights and obligations and how their Protected Health Information (PHI) may be used and disclosed.

B. Policy: The City of Marietta/BLW (Plan Sponsor) established and maintains a Group Health Plan (the "Plan") for its employees and covered dependents. The Plan is a covered entity and is required to comply with the Health Insurance Portability and Accountability Act (HIPAA) of 1996. The Plan Sponsor is not a covered entity but is responsible for ensuring that the Group Health Plan is in compliance with the privacy regulations. The privacy regulations will give employees and covered dependents more control and access to their PHI. It will limit the use and disclosure of health information; enable participants to find out how their information may be used and what disclosures of their information have been made. Medical information relating to Family and Medical Leave, fitness-for-duty and workers compensation is not covered under the regulations. It is the policy of the City of Marietta Group Health Plan to protect the privacy of protected health information and to comply with HIPAA Standards for Privacy of Individually Identifiable Health Information. Where State law is more restrictive than the privacy regulations, Georgia State law will prevail. The City/BLW specifically reserves the right to add to, change or abolish the provisions of this policy, in whole or in part, based upon pertinent action by any appropriate legislative, judicial or regulatory authority.

C. Definitions:

Covered Entities - Health plans (includes health flexible spending accounts), health care clearinghouses and those health care providers who conduct certain financial and administrative transactions electronically.

Protected Health Information - Individually identifiable health information that is maintained or communicated in any form (electronic, paper, or oral) by a covered entity.

D. Uses and Disclosures of Protected Health Information (PHI):

1. Required Uses and Disclosures:

The Plan is required to give employees and dependents access to their own protected health information (PHI) upon request and will disclose PHI to the Secretary of the Department of Health and Human Services when needed to investigate or determine if the City/BLW is in compliance with the privacy rules.

2. Permitted Uses and Disclosures to carry out treatment, payment and health care operations:

a. The Plan and/or its business associates may use and disclose protected health information without the employee's consent, authorization or opportunity to agree or object to carry out treatment, payment or health care operations.

Treatment includes the provision, coordination or management of health care. For example, the Plan may tell a doctor who is treating a covered individual that the individual has previously been treated for a condition that may affect his treatment of the individual.

As defined by the privacy rule, payment includes but is not limited to actions to make coverage determinations and payment (including billing, claims management, subrogation, plan reimbursement, reviews for medical necessity, appropriateness of care, utilization review and pre-authorization). For example, the Plan may tell a doctor whether the employee is eligible for coverage or what percentage of the bill will be paid by the Plan.

Health care operations include but are not limited to quality assessment and improvement, reviewing competence or qualifications of health care professionals, underwriting, premium rating and other insurance activities relating to creating or renewing insurance contracts. It also includes disease management, case management, conducting or arranging for medical review, legal services and auditing functions including fraud and abuse, compliance programs, business planning and development, business management and general administrative activities. For example, the Plan may use information about the employee claims to refer the employee to a disease management program, reimburse business associates for claims paid on behalf of the Plan or project future benefit costs or audit the accuracy of its claims processing functions.

b. The Plan may disclose information to business associates as needed to enable them to provide business services on behalf of the Plan. Business associate services may include claims administration, legal, actuarial, consulting, accounting and financial services. For example, the Plan may disclose

information to a consultant that performs actuarial services, cost sharing methodology, budgeting and plan design changes on behalf of the Plan.

The Plan requires all business associates to sign contracts agreeing (1) not to use or disclose the PHI other than as permitted by the contract or as required by law; (2) use appropriate safeguards to prevent the use or disclosure of the information other than as provided by the contract or by the privacy rules; (3) assist the Plan in complying with the regulations by providing participants upon request access to protected health information disclosures.

c. Where the Plan Sponsor does not already have access to PHI by virtue of its role in administering the Plan, the Plan will not disclose PHI to the Plan Sponsor except when the disclosure is (1) limited summary health information for insurance placement or settlor functions; (2) enrollment and disenrollment information; (3) involved in plan administration when the Plan Sponsor complies with certain administrative requirements involving an amendment of the Plan document and the erection of proper firewalls; and (4) authorized by the individual to whom it applies. The Plan Sponsor has amended the Plan Document and certified that the Plan Sponsor will appropriately safeguard and limit the use and disclosure of protected health information to carry out plan administration functions. Plan administration functions do not include employment-related functions or functions in connection with other benefits.

3. Uses and Disclosures that require the employee's written authorization:

Any written authorization for the Plan to disclose PHI other than as described herein shall be in plain language and satisfy the following requirements:

- It must include a description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion. The authorization may by its terms apply to all health information.
- It must include the name or other identification of the person or class of persons authorized to use or disclose the PHI.
- The authorization must specify the name or other specific identification of the person or class of persons to whom the Plan is authorized to make the requested use or disclosure.
- The authorization must describe the purpose of the requested use or disclosure.
- The authorization must include an expiration date or an expiration event. An expiration event must relate to the individual or the purpose of the use or disclosure.
- The authorization must be dated and include a signature of the individual or the individual's authorized representative. When an authorized representative signs the authorization, it must include a description of the representative's authority to act for the individual.

- The authorization must include a statement describing the individual's right to revoke the authorization and of the mechanism for making such a revocation, as to disclosures that have not taken place before the revocation is received by the Plan.
- The authorization must state either that the Plan may not condition treatment, payment, enrollment or eligibility on the individual's execution of an authorization or, when this is not accurate, describe the consequences of not providing the authorization.
- The authorization must include a statement that once information is disclosed pursuant to the authorization, the recipient's use of the information is not subject to the privacy rules.

The Plan will provide the individual with a copy of the signed authorization. The Plan may but is not required to maintain a standard authorization form that can be completed by covered individuals.

Generally, the Plan will obtain the employee's written authorization before any uses and disclosures will be made pertaining to psychotherapy notes obtained from a psychotherapist. The Plan may use and disclose such notes when needed by the Plan to defend against litigation filed by the employee or covered dependent.

4. Uses and disclosures that require that the employee be given an opportunity to agree or disagree prior to the use or release:

Disclosures of employees' PHI to family members, other relatives and to employees' close personal friends are allowed if the information is directly relevant to the family or friend's involvement with the employee's care or payment for that care and the employee has either agreed to the disclosure or has been given an opportunity to object and have not objected.

5. Uses and disclosures for which consent, authorization or opportunity to object is not required:

Use and disclosure of the employee's PHI is allowed without the employee's consent, authorization or request under the following circumstances:

- When required by law.
- When permitted for purposes of public health activities.
- When authorized by law to report information about abuse, neglect or domestic violence to public authorities.
- When requested by a public health oversight agency for oversight activities authorized by law.
- When required for judicial or administrative proceedings.
- When required for law enforcement purposes.
- When consistent with applicable law and standards of ethical conduct if the Plan, in good faith believes the use or disclosure is necessary to prevent or lessen a serious and

imminent threat to the health or safety of a person or the public and the disclosure is to a person reasonably able to prevent or lessen the threat, including the target of the threat.

- When authorized by law to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death or other duties as authorized by law.
- When authorized by and to the extent necessary to comply with worker's compensation or similar programs established by law.

Except as otherwise indicated in this policy, uses and disclosures will be made only with the employee's written authorization subject to the employee's right to revoke such authorizations.

6. Verification of identity of person requesting PHI:

The Plan will verify the identify of any person requesting PHI by requesting the person's name, address, business affiliation, phone number and signature, and/or such other identification as it deems appropriate. The Plan will document the responses it receives and, when appropriate, take steps to confirm that the information is accurate.

7. Minimum Necessary:

The Plan and Plan Sponsor will make every reasonable effort to limit their use and disclosure of PHI to the minimum necessary unless there is a specific exception to the rules. The minimum necessary standard will not apply, for example to disclosures authorized by the individual or to information that is used for treatment.

8. De-identified PHI:

Information that has been de-identified so that all identifying information is removed may be disclosed.

E. Participant Rights and Responsibilities:

1. Right to Request Restrictions on PHI Uses and Disclosures - Participants may request that the Plan restrict the use or disclosure of the participant's PHI, even for treatment, payment, or health care operations. However, the Plan is not required to agree to the restriction.

2. Right to Inspect and Copy PHI - A participant generally has a right with some exceptions to inspect and obtain a copy of his or her protected health information. The requested information will be provided within 30 days if the information is maintained on site or within 60 days if the information is maintained offsite. A single 30-day extension is allowed if the Plan is unable to comply with the deadline provided the Plan notifies the participant within the original 30-day time limit.

3. Right to Amend PHI - Participants have a right to request amendment to the participant's PHI. The Plan must comply within 60 days unless the Plan did not create the PHI or believes the amendment is inaccurate. A single 30-day extension is allowed if the Plan is unable to comply within the deadline. If the request is denied, the Plan will provide the participant with a written denial that explains the basis of the denial. The participant may submit a written statement

disagreeing with the denial and have a statement included with any future disclosure of the participant's PHI.

4. Right to Receive an Accounting of PHI Disclosures - At the participant's request, the Plan will provide the participant with an accounting of disclosures of PHI by the Plan during the six years prior to the date of the request. However, the Plan is not required to provide an accounting for:

- Disclosures made prior to the April 14, 2003 compliance date.
- Disclosures to carry out treatment, payment or health care operations.
- Disclosures made to the participant.
- Disclosures made under some of the exceptions, such as for law enforcement purposes.
- Disclosures the individual has authorized.

5. Right to Request Alternative Communications of PHI - Participants may request and the Plan must accommodate reasonable requests by individuals to receive communications of protected health information from the Plan by alternative means or at alternative locations, if the individual clearly states that the disclosure of all or part of that information could endanger the individual.

F. Personal Representative:

The Employee or his or her personal representative will be required to complete a form to request access to this information. A personal representative will be required to produce evidence of his or her authority to act on the employee's behalf before that person will be given access to the employee's PHI or allowed to take any action for the employee. Proof of such authority may take one of the following forms:

- A power of attorney for health care purposes, notarized by a notary public;
- A court order of appointment of the person as the conservator or guardian of the individual;
- An individual who is the parent of a minor child.

The Plan retains discretion to deny access to PHI to a personal representative to provide protection to those vulnerable people who depend on others to exercise their rights under these rules and who may be subject to abuse or neglect. This also applies to personal representatives of minors.

To request access to PHI or to obtain a form for this purpose, please contact the Benefits Manager whose office is located in the Personnel Department. The Benefits Manager has thirty days to respond to the employee's request and 60 days if someone else holds the information or it is offsite. If the employee's request is denied, the employee or his or her personal representative will be provided with a written denial setting forth the basis of the denial, the complaint

procedure and how the employee or personal representative may file a complaint to the Secretary of Health and Human Services.

G. Responsibilities of Department Heads, Division Managers and Supervisors:

1. To attend training sessions on the important role supervisors and managers have in protecting the confidentiality of medical information. The training will include a discussion of the privacy policy and procedure, what PHI is and the types of PHI, complaint procedures and steps to take when reasonable suspicion exists that an employee has violated the privacy policy.
2. To maintain and post the department/and or division poster notifying employees of the Plan's privacy practices in a conspicuous location.
3. To notify the privacy officer of any use or disclosure of PHI that is inconsistent with the privacy policy.
4. To agree not to use or disclose health information for employment related actions.

H. Plan Sponsor Responsibility:

1. Administration

- The Benefits Manager will serve as the Privacy Officer for the City/BLW. The Privacy Officer shall be responsible for the privacy program and shall regularly review the implementation of this policy and relevant privacy practices to assure that the confidentiality of individually identifiable health information is protected. If the employee has any questions regarding these policies, contact the Privacy Officer whose office is located in the Personnel Department.
- The Privacy Officer is designated as the person to whom complaints should be brought. Contact the Personnel Department to reach the Privacy Officer or to obtain additional information about the Plan's Notice of Privacy Practices.
- When performing plan administration functions on behalf of the Plan, only the following employees or classes of employees will be given access to PHI to accomplish the intended purpose of the use, disclosure or request: Benefits Manager, Payroll Manager, MIS Director, Finance Director and staff designated by the Benefits Manager, Payroll Manager, Finance Director and MIS Director.

2. Safeguards:

The Plan will comply with the security standards of the Act and have implemented technology and security policies to protect the personal data that is under the Plan's control from unauthorized access, improper use or disclosure, alteration, and unlawful or accidental destruction. The MIS Director will serve as the Security Officer. The Security Officer and

Privacy Officer have the responsibility of monitoring the program and maintaining appropriate administrative, technical and physical safeguards to protect the privacy of protected health information. The safeguards implemented include but are not limited to:

- Requiring all employees and business associates who have access to or are associated with the processing of employee data to respect the employee's confidentiality. If the Plan discovers that an employee or business associate has intentionally or unintentionally disclosed personal information about any of the participants, the Plan will take immediate action to prevent further occurrences.
- Providing training classes on the privacy and security policies and procedures to all employees involved in payment, health care operations and security. Training will also be provided to all new employees with plan administration responsibilities within a reasonable period of time after the employee joins the workforce. If there is a material change in the policies and procedures, retraining will be provided to all employees whose functions are affected by this material change.
- Requiring all employees involved in health care operations and security or having potential access to health care information to sign a confidentiality agreement to respect the confidentiality of PHI.
- Developing appropriate firewalls to prevent individuals from accessing health information without authorization, including creating and using passwords and changing them periodically to limit access to unauthorized individuals and storing paper records in locked file cabinets or storage rooms.
- Maintaining and storing information in a physically secure area and destroying records according to record retention schedules.

3. Complaints:

- The employee and covered dependents may file a complaint with the Privacy Officer or the Secretary of the U. S. Department of Health and Human Services, 200 Independence Avenue S.W., Washington, D.C. 20201, if the employee or covered dependent believes that his or her privacy rights have been violated. A complaint should be filed within a reasonable time after the employee or covered family member discovers that his or her privacy rights have been violated. The employee and covered dependent is encouraged to contact the Privacy Official initially to resolve complaints before seeking outside assistance.
- Although supervisors and managers of the City/BLW are to take appropriate action when they have reason to suspect that the privacy policy has been violated, employees should not assume that the Privacy Officer or Security Officer is aware of any problem.

4. Formal Privacy Rights Complaint Procedure:

Any employee who, in good faith, believes his or her privacy rights have been violated should:

- Complete the City/BLW PHI complaint form and submit the completed and signed form to the Privacy Officer with a copy to the Personnel Director within seven (7) calendar days following the incident that led the employee to believe that his or her privacy rights have been violated. The Privacy Officer has the authority and responsibility to investigate all complaints brought to his or her attention.
- Describe the infraction in detail including persons involved (if known), PHI involved, dates and relevant facts.
- The Privacy Officer will meet with the employee and document what the employee perceives the complaint to be and what remedy the employee believes should be taken if the complaint is upheld.
- The Privacy Officer will interview all individuals involved in the complaint and other employees who have access to the PHI in question by virtue of carrying out the employees' job duties on behalf of the Plan.
- The Privacy Officer will review all the facts and provide a detailed report of his or her findings to the Personnel Director within seven (7) calendar days following receipt of the complaint.
- The Personnel Director will review the evidence and supporting documentation and communicate a decision in writing to the employee within seven (7) calendar days following receipt of the Privacy Officer's report.
- If the Personnel Director's decision does not resolve the privacy issue to the satisfaction of the employee, the employee may file a formal complaint as outlined in Article 4-4-22 of the personnel rules and regulations (Grievance and Appeals Policy) and initiate the complaint at step 3. The employee must submit the complaint with all supporting documentation including a copy of the Director of Personnel's decision to the City Manager within seven (7) calendar days from receipt of the Personnel Director's decision.
- The City Manager will review the documentation and communicate a decision in writing to the employee within thirty (30) days following receipt of the written complaint. Such decision will exhaust all remedies with the Plan Sponsor.
- At all times during the investigation, reasonable steps will be taken to maintain confidentiality of the case within the limits of federal and state law. Employees will not be retaliated against for filing a complaint about the Plan's privacy and security practices.

5. Remedial Action:

If the evidence indicates that the employee or covered dependent's privacy has been breached, appropriate disciplinary action will be taken. Depending on the severity of the action and its damaging effects to the complainant, the violator(s) shall be subject to appropriate disciplinary action up to and including termination of employment.

6. Mitigation

The Plan will make reasonable efforts to mitigate any harmful effects the complainant experiences arising from the use or disclosure of protective health information that violates the privacy or security rules or the Plan's privacy policy and practices.

Section 2: That a new City Code Section 4-4-11-30 entitled Information Security Policy be adopted to read as follows:

4-4-11-30 Information Security Policy

A. Purpose: This document is designed to provide the City/BLW *minimum* security policies for protection of City/BLW assets inclusive of information, computers and networks.

B. Information Custodianship: Information, such as data, electronic mail, documents and software, are City/BLW assets. In determining the value of an asset, consideration shall be given not only to the sensitivity of the information, but also to the consequences of unauthorized disclosure, modification, destruction, or unavailability of the information. The value of these assets will determine the level of controls needed to provide adequate safeguards, backup and access controls. However, ownership, custodial responsibility and rights to these assets are herein established.

- **Records.** A "record" includes any information kept, held, filed, produced or reproduced by, with or for a department in any form or media including, but not limited to, reports, statements, examinations, memoranda, opinions, folders, files, books, manuals, pamphlets, forms, papers, designs, drawings, maps, images, photos, letters, microfilms, computer tapes or discs, rules, regulations or codes.
- **Property of a Department.** All records, software, and hardware that are part of a department's information system are considered property of the City/BLW and shall be used for City/BLW business purposes only.
- **Designation of Responsibility.** Department Heads, or their designee, have the responsibility to ensure that all City/BLW information resources, regardless of medium, are used, maintained, disclosed and disposed of according to law, regulation or policy.
- **Copyright and Licensing of Vendor Hardware and Software.** Departments shall adhere to copyright laws and licensing agreements.

- **Records Retention and Destruction.** City/BLW information shall be retained and/or destroyed in accordance with records retention schedules developed in cooperation with the State Archives and Records Administration (SARA) and policies and procedures established by the City/BLW, unless required otherwise by applicable laws.
- **State and Federal Access, Privacy and Confidentiality Laws.** All information, regardless of the medium in which it is maintained or communicated, is subject to pertinent state and federal laws governing access, the protection of privacy and prohibitions against unauthorized disclosure.
- **Access Categories - Classification of Information.** Information classification provides a means for separating information into categories with different protective requirements. The City/BLW determines, in advance, the extent to which information shall be disclosed to specified users. Determinations shall be made based on the nature of the information and the duties of City/BLW employees. The following general categories of information serve to provide guidance in identifying appropriate users or recipients:
 - **Public Information** is information accessible under Freedom of Information Law and the Georgia Open Records Act and is available to any person, notwithstanding one's status or interest within the limitations as provided in those laws.
 - **Restricted Information** pertains to information that is not public information, but can be disclosed to or used by City/BLW representatives to carry out their duties, so long as there is no legal bar to disclosure.
 - **Confidential Information including Protected Health Information (PHI)** is information that is protected by law. Access to confidential information is prohibited unless permitted by an exception in law.

C. Physical Access Security: The Department Head shall put into place appropriate safeguards to limit physical access to any computer or computer related device.

- **Secure Locations.** Mainframe, servers and other essential computer devices shall be stored in a location that protects them from unauthorized physical access. Physical access to such equipment potentially provides access to information stored therein.
- **Location Selection.** Physical locations for all computer related equipment shall be selected to protect against equipment and information loss by flood, fire, and other disasters, natural or man-made.
- **Review of New Connections to Outside Sources.** Proposed access to or from a network external to the City/BLW shall be reviewed and approved by the Department Head or designee prior to establishment of the connection. Final approval shall be obtained from the Director of MIS.
- **Review of Installation.** Installation, upgrade, changes or repairs of computer equipment and computer related devices (hardware, software, firmware) must be reviewed by the MIS Department for potential physical security risks.

- **Platform-specific Physical Security.** Platform-specific physical security shall be established, implemented and periodically reviewed and revised as necessary to address physical vulnerabilities of that platform.
- **City/BLW Laptop, Notebook and Portable Computer Devices.** Portable computing devices shall not be left unattended at any time unless the device has been secured. When traveling, portable computers shall remain with the employee's carry-on hand luggage.

D. Information Security: The Security Officer (MIS Director or designee) is responsible for the security of all electronic information resources. Specific procedures will be developed and disseminated by the Security Officer to conform to the following policies. These procedures will be reviewed frequently to reflect changes in personnel and technology.

E. Information Security Administration Functions: The Security Officer will formally delegate responsibility for information security matters. Multiple individuals across organizational lines may be involved as long as there is a clear separation of duties and responsibilities which provide effective checks, balances and accountability.

F. Logon Security: Access to computer systems requires identification and authentication. Any exceptions to this rule require approval of the Security Officer or designee.

G. Remote Access to City/BLW Information: Remote external access to a City/BLW network, which contains restricted or confidential information, requires extended authentication procedures. Any method for providing this remote access (e.g., modem, firewall) requires Security Officer or designee approval prior to its installation.

H. External Network Access to City/BLW Information: External network access to a City/BLW network which contains restricted or confidential information including PHI requires at least a firewall. Firewalls provide network security similar to the installation of a perimeter security system on a building by blocking or permitting traffic.

I. Transaction Controls and Database Security: Transactions entered into the City/BLW production databases shall be checked for accuracy and authenticity. Database management systems (DBMS) shall implement security and authorization subsystems adequate to protect against unauthorized access and modification.

J. Downloading Software: The Security Officer, upon request of a Department Head, will determine whether downloading of software from an external site will be permitted.

K. City/BLW Owned IT Components: City/BLW hardware shall be reviewed and cleansed (sanitized) before being reassigned or discarded. The Security Officer shall work with MIS Department staff to ensure compliance with this policy. Department Heads shall maintain adequate documentation of hardware/software taken off City/BLW premises by employees.

L. Electronic Communications: When transmitting confidential information, such as Protected Health Information (PHI), on an external network (outside the firewall), City/BLW shall employ

a secure technology rendering the information unusable to an unauthorized or intercepting third party.

M. Virus Protection: All City/BLW computers shall be equipped with up to date virus protection software. The MIS Department will ensure that all network attached PCs are virus protected.

N. City/BLW Security Management: Accountability and appropriate separation of duties and responsibilities are essential elements of security administration. Departments shall develop security awareness among all staff.

- **Security Training.** All employees, agents and others who access City/BLW computer systems shall be provided with sufficient training and/or supporting reference materials to allow them to properly protect City/BLW information.
- **Employment Changes.** Department Heads or their designees shall report changes in employment status of their staff to the Security Officer and/or Systems Administrator in the MIS Department.
- **Audit Trails.** The Department Head shall maintain audit trail records of individuals accessing City/BLW records sufficient to meet the requirements of the law, the City/BLW internal controls and audit requirements, and as necessary, disaster recovery requirements.

O. Information Recovery: All business applications shall have backup and recovery procedures that are documented, maintained and the backup media stored off site. The City/BLW shall test these procedures on an annual basis.

P. Data Exchange Agreements: Third Party Agreements: All agreements with third parties such as vendors, other government agencies, or contractors shall include requirements to adhere to City/BLW information security policies.

Q. Vendor/Contractor Agreements: All vendor agreements shall contain a requirement that any City/BLW information obtained as a result of such an agreement shall be the property of the City/BLW and shall not be utilized, including but not limited to, secondary release or disclosure, without written authorization of the City/BLW.

R. Employee/Agent Responsibilities: As a condition of continued employment, all employees/agents by signature of the City/BLW's Personnel Policies and Procedures, as may be amended, indicate that they have read and understand the City/BLW's policies and procedures regarding information security, and agree to comply in all respects to those policies and procedures.

- **Password Protection.** Employees/agents shall not post or share their personal passwords, and shall develop secure passwords according to MIS Department security guidelines.
- **Use of Automatic Logons.** Employees/agents shall not facilitate any logon procedure with local programming such as keyboard programming or scripting.

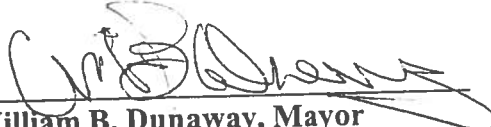
- **Unattended Computers.** Unattended computers shall be logged off or protected in such a way as to protect the computer and network from unauthorized access.

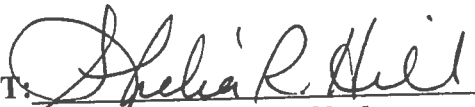
S. Reporting Suspicious Events: Any observations of suspicious activity shall be reported to the appropriate department head and/or the Information Security Officer. Suspicious activity can include: signs of unauthorized equipment usage during evenings and weekends, phone requests from unidentifiable callers for access to PHI, unidentifiable files found on file servers, and unusual activity recorded in log files.

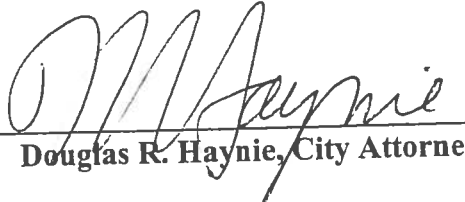
Section 3: It is hereby declared to be the intention of this Ordinance that its sections, paragraphs, sentences, clauses, phrases and words are severable, and if any section, paragraph, clause, phrase or word of this Ordinance is declared to be unconstitutional or invalid, it shall not affect any of the remaining sections, paragraphs, clauses, phrases or words of this Ordinance.

Section 4: All Ordinances or parts of Ordinances in conflict with this Ordinance are hereby repealed.

Section 5: This Ordinance shall become effective upon the signature or without the signature of the Mayor, subject to Georgia laws 1983, page 4119.

DATE: March 12, 2003 APPROVED: 
 William B. Dunaway, Mayor

ATTEST: 
 Shelia R. Hill, City Clerk

APPROVED AS TO FORM: 
 Douglas R. Haynie, City Attorney