Administrative Regulations
Office of the Mayor

Title: PRIVACY OF PROTECTED HEALTH INFORMATION
A.R. Number: 5.10 **Effective Date:** 2/1/2007 **Page:** 1 of 5
Supersedes: Privacy of Protected Health Information **A.R.:** 5.15 **DATED:** 9/1/2004

I. POLICY

Additional privacy regulations issued under the federal Health Insurance Portability and Accountability Act of 1996 ("HIPAA") require the maintenance of privacy of Protected Health Information ("PHI") and restrict the use and disclosure of PHI. As a sponsor of a group health plan, the City is not a covered entity under HIPAA. This policy outlines various privacy protocols and procedures intended to ensure the confidentiality, security, and integrity of PHI.

II. DEFINITIONS

A. Protected Health Information ("PHI") - means individually identifiable health information, as defined by HIPAA, that is created or received by the City and that relates to past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and that identifies the individual or for which there is a reasonable basis to believe the information can be used to identify the individual. PHI includes information of persons living or deceased.

B. Summary Health Information (SHI) - Summary Health Information is information on the claims history of covered individuals. Employers may obtain Summary Health Information only for the purpose of changing or terminating their plan or obtaining bids. Individually identifiable information is deleted from Summary Health Information, except this information can be aggregated at the five-digit Zip code level.

C. HIPAA – Health Insurance Portability and Accountability Act of 1996.

D. Business Associates - contracts with outside persons or organizations, examples of these outside persons include laboratories that conduct medical tests and analyze medical statistics.

E. HIPAA Privacy Officer – The individual named by the City of Richmond as it's Privacy Officer for HIPPA compliance in accordance with HIPPA regulations.

III. PROCEDURES

This procedure describes how medical information about an employee may be used and disclosed and how the employee can get access to this information. Notice of Privacy Practices – Protected Health Information applies to Protected Health Information (PHI) associated with various governmental functions performed by the City. This procedure describes how the City may use and disclose personal health information to carry out its operations and for other purposes that are permitted or required by law. The City is required by the privacy regulations issued under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") to maintain the privacy of Protected Health Information and to provide individuals notice of its legal duties and privacy practices concerning Protected Health Information. In the event applicable law, other than HIPAA, prohibits or materially limits its uses and disclosures of Protected Health Information, as set forth below, the City will follow the more stringent standard.

The City is required to abide by the terms of this regulation so long as it remains in effect. The City reserves the right to change the terms of this procedure as necessary and to make it effective for all Protected Health Information it maintains. If the City makes material changes to its privacy practices, revised notices and procedures will be available within City offices and copies may be obtained by contacting the City at the telephone number or address provided in this Regulation or on the City's Web site at www.richmondgov.com.

A. Uses and Disclosures of your Protected Health Information

The following categories describe different ways that the City uses and discloses PHI. For each category of uses and disclosures an explanation is provided and, where appropriate, examples are given. Not every use or disclosure in a category will be listed. However, all of the ways the City is permitted or required to use and disclose PHI will fall within one of the categories.

1. Your Authorization – Except as outlined below, the City will not use or disclose your PHI unless you have signed a form authorizing the use or disclosure. You have the right to revoke that authorization in writing except to the extent that the City has taken action in reliance upon the authorization.

2. To Carry Out Treatment Functions – The City may use or disclose your PHI without your permission for health care providers to provide you with treatment.

3. To Carry Out Certain Operations Relating to Your Benefit Plan – The City may use and disclose your PHI as necessary of its health care operations. Examples of health care operations include activities relating to the creation, renewal, or replacement of a Health Plan.

4. Business Associates – Certain aspects and components of the City's services are performed through contracts with outside persons or organizations. Examples of these outside persons include laboratories that conduct medical tests and analyze medical statistics. At times, it may be necessary for the City to provide your PHI to one or more of these outside persons or organizations.

5. To Carry Out Certain Government Operations – The City may use or disclose your PHI without your permission to carry out certain limited activities relating to various governmental functions. Examples include review of applications for the Shared Leave Program, certifications required by the Passport to Wellness Program, review of applications for Family Medical Leave Act, review of disability retirement requests, and other specialized government functions. The City will make reasonable efforts to limit such uses and disclosures to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.

6. Other Uses and Disclosures – The City may make certain other uses and disclosures of your PHI without your authorization.

   - The City may use or disclose your PHI for any purpose required by law.

   - The City may disclose your PHI for public health activities, such as reporting a disease, injury, birth and death, and for public health investigations.

- The City may disclose your PHI to the proper authorities if child abuse or neglect is suspected; the City may also disclose your PHI if there is reasonable belief that you are a victim of abuse, neglect, or domestic violence.

- The City may disclose your PHI if authorized by law to a government oversight agency conducting audits, investigations, or civil or criminal proceedings.

- The City may disclose your PHI in the course of a judicial or administrative proceeding, to respond to a subpoena or discovery request, or other court order.

- The City may disclose your PHI to the proper authorities for law enforcement purposes.

- The City may disclose your PHI to coroners, medical examiners, and/or funeral directors consistent with law.

- The City may use or disclose your PHI to prevent or lessen a serious and imminent threat to your health or safety or the health and safety of the general public.

- The City may use or disclose your PHI for organ, eye or tissue donation.

- The City may use or disclose your PHI for research purposes, but only as permitted by law.

- The City may use or disclose your PHI if you are a member of the military as required by armed forces services, and we may also disclose your PHI for other specialized government functions such as national security or intelligence activities.

- The City may disclose your PHI to workers' compensation agencies for your workers' compensation benefit determination and as necessary to comply with workers' compensation laws.

- The City will, if required by law, release your PHI to the Secretary of the Department of Health and Human Services for enforcement of HIPAA.

B. Your Rights

1. Access to Your PHI **–** You have the right to inspect and or to obtain a copy your PHI that is included in certain records we maintain. Under limited circumstances, we may deny you access to a portion of your records. If you request copies, we may charge you copying and mailing costs. Certain requests for access to your PHI must be in writing, must state that you want access to your PHI and must be signed by you or your representative.

2. Amendments to Your PHI – You have the right to request that PHI that we maintain about you be amended or corrected. We are not obligated to make all requested amendments but will give each request careful consideration. If we determine that the record is inaccurate, and the law permits us to amend it, we will correct it. To be considered, your amendment request must be in writing, must be signed by you or your representative, and must state the reasons for the amendment/correction request. If your doctor or another person created the information that you want to change, you should ask that person to amend the information.

3. Accounting for Disclosures of Your PHI – You have the right to receive an accounting of certain disclosures made by us of your PHI. To be considered, your accounting requests must be in writing and signed by you or your representative. The accounting that we provide will not include disclosures made before April 14, 2003, disclosures made in the course of conducting governmental operations, disclosures made for treatment, payment or health care operations, disclosures made earlier than six years before the date of your request, and certain other disclosures that are accepted by law. The first accounting in any 12-month period is free; however, the City may charge you a reasonable fee for each additional accounting you request within the same 12-month period.

4. Restrictions on Use and Disclosure of Your PHI - You have the right to request restriction on certain of the City's uses and disclosures of your PHI for insurance payment or health care operations, disclosures made to persons involved in your care, and disclosures for disaster relief purposes. For example, you may request that the City not disclose your PHI to your spouse. Your request must describe in detail the restriction you are requesting. HIPAA does not require the City to agree to your request. The City will accommodate reasonable requests when appropriate. The City retains the right to terminate an agreed-to restriction if the City believes such termination is appropriate. In the event of a termination by the City, the City will notify you of such termination. You also have the right to terminate, in writing, any agreed-to restriction. Requests forms can be obtained by contacting the City at the address below.

5. Request for Confidential Communications – You have the right to request that communications regarding your PHI be made by alternative means or at alternative locations. For example, you may request that messages not be left on voice mail or sent to a particular address. The City will accommodate reasonable requests; however, the City is not required to agree to all requests.

6. Right to a Copy of the Notice – You have the right to a paper copy of this Notice upon request.

7. Complaints – If you believe your privacy rights have been violated, you can file a complaint with the City at the address below. You may also file a complaint in writing with the Secretary of the U.S. Department of Health and Human Services, Office for Civil Rights, 150 S. Independence Mall West, Suite 372; Public Ledger Building, Philadelphia, PA 19106-9111. Main Line (215) 861-4441. Hotline (800) 368-1019. FAX (215) 861-4431. TDD (215) 861-4440. For all complaints filed by e-mail send to: OCRComplaint@hhs.gov. Complaints must be filed in writing, either on paper or electronically; name the entity that is the subject of the complaint and describe the acts or omissions believed to be in violation of the applicable requirements of HIPAA, and be filed within 180 days of the believed violation.

C. For More Information or Complaints

If you have questions or need further assistance regarding this Notice, are concerned that the City has violated your privacy rights or disagree with a decision that the City made about access to your PHI, you may contact the Privacy Officer at:

HIPAA Privacy Officer
City of Richmond, Department of Human Resources
900 East Broad Street, Suite 902
Richmond, Virginia 23219
Telephone Number: (804) 646-5660
FAX Number: (804) 646-5856

IV. REGULATION UPDATE

The Office of the Mayor and the Department of Human Resources shall be responsible for modifications to this Regulation.

V. EXHIBITS

A. Authorization for Disclosure of Protected Health Information

B. Questions and Answers for Privacy of Protected Health Information

APPROVED:

MAYOR

City of Richmond, Virginia

Department of Human Resources

Authorization for Disclosure of Protected Health Information

As the person signing this authorization, I understand that I am giving permission to (entity) to disclose (name of document) to the person(s) or organization(s) I have indicated below.

I designate (insert name of individual) as my personal representative to act on my behalf in making health care related decisions, receiving health care information, and/or disclosing my personal health information.

I understand that (entity name) may disclose my (state specific document) for the purpose of (ex.--billing my insurance company or sending info to my attorney).

The provisions of treatment, payment, enrollment in a health plan, or eligibility for benefits to me cannot be conditioned on my signing of this authorization.

The original or a copy of this authorization shall be included with my original records for at least six years.

I have a right to revoke this authorization at any time, except to the extent that action has been taken by (entity) in reliance to this request. I understand that if I choose to revoke this authorization, I must submit a written statement to (entity). The written statement will be effective upon delivery to the provider in possession of my health information.

Revocation of this authorization is not valid if this authorization was obtained as a condition of obtaining insurance coverage.

There is a potential for any information disclosed by this authorization to be rediscovered by the recipient and no longer protected by the federal privacy regulations.

I authorize (entity) to disclose my health information to the following organization(s) or person(s):

_____

_____ _____

Signature Date

This information may be disclosed immediately for the following time period:

Begin Date:_____ End Date:_____

I prefer that you contact me in a way other than my address or my phone number. I wish to be contacted in the following manner:

_____

_____

_____

_____ _____

Signature Date

City of Richmond

What is HIPAA?

HIPAA is the Health Insurance Portability and Accountability Act passed in 1996. This legislation established portability of coverage rights and outlined rules for the electronic transfer of data. Out of these rules came recognition of the need to ensure the privacy of personal health information. Because of the size of our plan these privacy regulations become effective April 14, 2003. One requirement of the legislation is that everyone who handles personal health information be trained on how to treat this information prior to the April 14th deadline. The following information has been identified as the key components of this legislation. It is important in your job position that you understand these rules and adopt them into your daily business practices.

What does HIPAA protect?

HIPAA specifically protects certain 'Individually Identifiable Health Information" which the legislation calls "Protected Health Information" or PHI. HIPAA only protects this information as it relates to medical and dental programs. It does not extend to other benefits that use PHI such as Worker's Compensation, Life Insurance, Disability Insurance, Family Medical Leave Act (FMLA) or ADA.

PHI is best understood as any information that could be used by someone else to identify medical information about a specific individual. It obviously includes name and social security number, but also includes address information, demographic information such as date of birth and gender, and claim information such as date of service, place of service and diagnosis.

How do I distinguish information that should be protected under HIPAA from other non-protected personal information?

HIPAA protects information as it comes into the Health Plan and as it leaves the Health Plan. The Health Plan can be considered anyone involved in the treatment, payment, and operations of the health program. Therefore, it includes medical providers, insurance carriers, and employers who sponsor health benefits.

Because the concept of the Health Plan is somewhat difficult to define, the safest recommended course of action is to treat all personal information as confidential and "Top Secret". In other words, treat all personal information *AS IF* it were protected by HIPAA. This conservative approach will protect the organization from any breach of privacy. Remember, companies are sued today for breaches in privacy under other laws such as FMLA and ADA. Just because it is not protected by HIPAA doesn't mean the organization can't get in trouble if private health information is not treated confidentially.

What is my responsibility in protecting personal health information?

- On a global basis, your responsibility is to ensure that when you receive or use PHI that you treat it confidentially and in compliance with the HIPAA guidelines discussed below.

- HIPAA is clear – do not discuss PHI openly where others can overhear; obtain only the information you absolutely need to know, and disclose only the "minimum necessary" to meet a valid request for PHI.

- Evaluate your work location and current practices to identify potential security leaks:

    - Do your files lock or is there a lock on the file room?
    - Are there faxes received that contain PHI (i.e., EOBs, doctor's bills)?
    - Is the fax machine located where inappropriate persons could see these faxes?
    - Is your computer screen facing people as they approach your desk?
    - How do you store information? If you do not have files for medical information separate from general personnel files, you should establish separate, secure medical files.
    - Are computers password-protected? Who has access to your e-mail?

- Before you discuss PHI with individuals over the telephone, how do you verify identity?
- Do you ever send PHI electronically? Is it encrypted or password protected?
- How do you dispose of PHI? Do you have a shredder?

- Once you have done a thorough evaluation, conduct a "cost/harm" analysis of each breach. Ask yourself, "What is the risk of inappropriate disclosure"? What is the harm of this disclosure? What will it cost to close the leak? What will it cost to not close the leak?
- If you decide not to close a leak, document how and why this decision was made.
- Keep a copy of your security evaluation in event of a complaint or an audit.

Specific HIPAA Privacy Issues

- Enrollment forms for medical and dental – you should store these forms separately from personnel files and make sure they are secure.
- E-mail – if transmitting data (i.e., eligibility information), consider encrypting the file. You can also password protect attachments and call recipient with password and add a "confidentiality" tag to e-mails.
- Voice Mails – do not leave PHI on a voice mail; instead, leave your name and number and ask for a return call. Also, don't listen to voice mail on a speakerphone.
- Telephone conversations – verify the identity of the speaker in a reasonable way and speak in a hushed or quiet voice if you do not have a private office.
- Assisting employees and family members with claims:
  - You can always disclose PHI to the individual who is also the claimant; however, you may find that the carrier or the provider will require a signed authorization before they will share information with you. You should keep blank authorization forms on hand for use.
  - If a family member asks you to help resolve a claim issue on a claimant, you are okay to do so without an authorization from the claimant because this is considered part of normal plan operations.
  - If someone requests PHI on someone other than themselves for a reason other than to get a claim paid, you should get a signed authorization from the individual first.
  - If the request comes from an adult personal representative (i.e., power of attorney), verify the identity and obtain a copy of the power of attorney for your files; then you can release PHI as if you were talking to the individual.
  - If a parent requests information on a child, you may disclose PHI if it is to resolve a claim. In other situations, generally you can disclose information to a parent unless state laws allow a child to get specific medical treatment without parental consent. If a parent is requesting specific medical information, you may request an opinion of the Deputy Privacy Official or Legal Counsel.
  - Disclosure to a provider – to facilitate claim payments, you may disclose PHI to providers; however, the provider may require an authorization from the claimant.
  - Disclosure in response to subpoena or court order – you may disclose the requested information in response to a court order. In the event of a subpoena, we recommend you obtain legal advice to determine the legitimacy of the subpoena. PHI that is disclosed as the result of a subpoena should be logged in the HIPAA Privacy Disclosure Log unless the subpoena is part of a criminal investigation.
  - Worker's Compensation – In some states, you will need a signed authorization form to provide PHI for a worker's compensation claim if the PHI comes from the Plan. Doctors may also require a signed authorization before they will release any medical information even though Worker's Compensation is not protected by HIPAA.
  - Pre-employment screening results – you can require a signed authorization releasing the test results as a condition for consideration for employment. Screening centers

will not release results to you without an authorization.

- Disclosures required for administration of STD, LTD, FMLA, ADA – you may need a signed authorization form to get providers to release information necessary to administer these plans. For example, if you need medical information to justify the continuation of STD benefits. It is recommended that you have the employee sign and authorization form at the time they complete the initial paperwork for the benefit.

- Disclosure of PHI to supervisors – never give a supervisor an employee's medical file. If you need to disclosure information for "return-to-work" consideration, you must get a signed authorization from the employee first.

- Do not release information about an employee's visit to the Employee Assistance Program (EAP) to a supervisor without the employee's signed authorization.

What do I do if I discover there has been an inappropriate disclosure?

If it was one-time disclosure, it does not need to be logged. If it is systemic, it should be reported to the Privacy Official, and logged on the Disclosure Log.

What if I get complaints about a breach of HIPAA privacy?

You need to report all breaches to the Privacy Officer who will investigate. You should assist the individual in their complaint by providing a complaint form.

Now that I have reviewed the HIPAA Privacy requirements and understand the need to keep protected health information (PHI) confidential and secure, what do I need to do in the future?

In addition to keeping all personal health information confidential, you need to ensure that all new hires or temporary employees who will handle this type of information are trained as well. Individuals who are trained should sign an ongoing training log so that your training efforts are documented in the event of an audit.