

**CITY OF MILWAUKEE BASIC HEALTH PLAN
POLICIES AND PROCEDURES**

Introduction: It is the Plan's policy to comply with the Privacy Rules. In adopting the policies and procedures set out herein, no third party rights are intended to be created. In particular, these policies and procedures create no rights for Plan participants or their dependents. The Plan has the right to change the policies and procedures set out herein at any time without notice. The policies and procedures set out herein may reflect standards that are more stringent than those in the Privacy Rules, but are not intended to legally obligate the Plan or the Employer to meet any such more stringent standard. Accordingly, these policies and procedures are explicitly not binding on the Plan or the Employer.

These Policies and Procedures for Maintaining Written Policies and Procedures will be in effect from and after the Effective Date.

The Privacy Rules require the Plan to implement policies and procedures with respect to PHI that are reasonably designed, taking into account the size of the Plan and the type of activities that relate to PHI undertaken by the Plan, to ensure compliance with the Privacy Rules. The Privacy Rules also require that policies and procedures that the Plan implements pursuant to this requirement, and any changes that the Plan makes to those policies and procedures, be documented either on paper or in electronic form. The Privacy Rules require the Plan to change its policies and procedures, and to promptly implement and document the change, whenever there is a change in law that necessitates a change to the Plan's policies or procedures. The Plan may change its policies and procedures at any time, but the Privacy Rules require that the Plan document any change before it becomes effective. If the change relates to a privacy practice described in the Plan's notice of privacy practices, the notice also must be revised before the change can become effective. The Plan may make the changes effective for PHI that it created or received prior to the effective date of change only if its notice of privacy practices states that the Plan has the right to do so.

Definitions: Certain terms are given particular meanings when used in these Policies and Procedures for Maintaining Written Policies and Procedures with initial capital letters, as set out below.

BUSINESS ASSOCIATE means an individual or entity identified as a Business Associate of the Plan from time to time pursuant to the Plan's Policies and Procedures for Identifying Business Associates.

DESIGNATED EMPLOYEES means those individuals in the Employer's workforce that are identified as members of the Plan's workforce in CCFN No. _____.

DESIGNATED INFORMATION means information in connection with the Plan that concerns enrollment, payment, claims adjudication or case or medical management information or that is used, in whole or in part, by or on behalf of the Plan, to make decisions about Individuals.

DESIGNATED RECORD SET means that group of records identified as the Plan's Designated Record Set from time to time pursuant to the Plan's Policies and Procedures for Identifying Designated Record Set.

EFFECTIVE DATE means April 14, 2003.

EMPLOYER means the City of Milwaukee, a municipal corporation organized and existing under the laws of the State of Wisconsin.

EXCEPTED SITUATIONS means:

- A Designated Employee violates the plan's policies and procedures by making disclosures to health oversight agencies, public health authorities, appropriate health care accreditation organizations, or an attorney retained by the workforce member, because of a good faith belief that the plan has engaged in unlawful conduct or violated professional or clinical standards, or is potentially endangering workers or the public.
- A Designated Employee is the victim of a crime and discloses PHI to a law enforcement official, if the disclosure is about the suspected perpetrator and only limited information is disclosed, as provided in the Privacy Rules.

- A Designated Employee files a complaint with the Secretary or testifies, assists or participates in an investigation, compliance review, proceeding or hearing.

INDIVIDUAL means a person who is the subject of PHI.

LEGAL MATERIALS means information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding.

PERMISSIBLE PURPOSES means the performing of data aggregation services relating to the health care operations of the Plan, the proper management and administration of the Business Associate or the carrying out of the legal responsibilities of the Business Associate.

PHI means information that is created or received by the Employer or a Business Associate on behalf of the Plan, and relates to the 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.

PLAN means the City of Milwaukee Basic Health Plan.

PLAN CONTACT means the person or office designated by the Plan in writing from time to time as the Plan's Contact Person or Office.

PLAN PHI means PHI that the Employer or a Business Associate receives or creates in connection with the Plan.

PRIVACY OFFICIAL means a person designated by the Plan in writing from time to time as the Plan's Privacy Official.

PRIVACY RULES means Standards for Privacy of Individually Identifiable Health Information adopted by the Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act of 1996, and found at 45 CFR Part 160 and Part 164, subparts A and E, as the same may be revised or recodified from time to time.

PSYCHOTHERAPY NOTES means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session, or a group, joint, or family counseling session, which notes are separated from the rest of the individual's medical record. Psychotherapy Notes excludes notes regarding medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, treatment plan, symptoms, prognosis, and progress to date.

SECRETARY means the Secretary of Health and Human Services (HHS) or any other officer or employee of HHS to whom the authority involved has been delegated.

TPA means an entity or person retained by the Plan to adjudicate and pay claims under the Plan.

1. POLICIES AND PROCEDURES FOR MAINTAINING WRITTEN POLICIES AND PROCEDURES

<i>Policies for Maintaining Written Policies and Procedures</i>	<i>Procedures for Maintaining Written Policies and Procedures</i>
It is the Plan’s policy to adopt and implement policies and procedures as required by the Privacy Rules.	The Privacy Official, in consultation with the City Attorney, will formulate policies and procedures that are reasonably designed, taking into account the size of the Plan and the type of activities that relate to PHI undertaken by the Plan, to ensure compliance with the Privacy Rules. The Privacy Official shall indicate final adoption of a policy or procedure on behalf of the Plan by noting the Common Council Resolution approving same and maintaining a certified copy of that resolution. The Privacy Official will maintain the originals of all such policies and procedures in his or her office or other secure location.
It is the Plan’s policy to change its policies and procedures, and to promptly implement and document the change, whenever there is a change in law that necessitates a change to the Plan’s policies or procedures.	The Privacy Official, in consultation with the City Attorney, will monitor to determine when changes in the law occur that require changes to the Plan’s policies and procedures, and, prior to the effective date of such changes will determine what changes are needed in the Plan’s policies and procedures, and will recommend to the Common Council the adoption of appropriately revised policies and procedures.
It is the Plan’s policy to reserve the right to change its policies and procedures at any time, and to document any such change before it becomes effective.	The Privacy Official, in consultation with the City Attorney, will recommend any changes to Plan’s policies and procedures, and any such changes shall be approved in a duly-adopted Common Council resolution before any change is implemented.
It is the Plan’s policy to make any changes to its policies and procedures effective as of whatever date the Privacy Official specifies for such change, and to make such changes effective for PHI that was created or received prior to the effective date of changes, except that, if the change relates to a privacy practice described in the Plan’s notice of privacy practices, the notice must be revised before the change can become effective.	The Privacy Official, in consultation with the City Attorney, will ensure that the Plan’s notice of privacy practices states that the Plan may make changes to its policies and procedures effective for PHI that it created or received prior to the effective date of change.
It is the Plan’s policy to permit its Business Associates that are TPAs to follow their own policies and procedures to the extent that the Plan relies on those TPAs to carry out Plan functions that are required or affected by the Privacy Rules, and to require the TPA to indemnify the Plan and the City of Milwaukee in connection with any violation of the Privacy Rules.	To the extent that Policies and Procedures of TPA reflect Plan operations, the Privacy Official will maintain the policies and procedures it receives from the Plan’s TPAs with the Plan’s policies and procedures. The Privacy Official will review the policies and procedures received from the Plan’s TPA(s), consultation with the City Attorney, to ensure that such policies and procedures reflect compliance with the Privacy Rules.
It is the Plan’s policy that all of the Designated Employees must comply with the Plan’s policies and procedures that are duly adopted by the Privacy Official from time to time.	All Designated Employees will receive a copy of these Policies and Procedures and receive training as provided in section 7 of these Policies and Procedures.

2. POLICIES FOR DISCLOSING PHI TO PLAN SPONSOR

<i>Policies for Disclosing PHI to Plan Sponsor</i>	<i>Procedures for Disclosing PHI to Plan Sponsor</i>
----------------------------------------------------	------------------------------------------------------

<i>Policies for Disclosing PHI to Plan Sponsor</i>	<i>Procedures for Disclosing PHI to Plan Sponsor</i>
It is the Plan's policy that the Plan will disclose PHI to the Employer and will allow the Employer to use and further disclose such PHI only in accordance with the terms of CCFN No. _____, and only if the Employer has provided the certification required by the Privacy Rules.	The Privacy Official will ensure that the Employer has provided the certification required by the Privacy Rules in connection with that Plan document. In accordance with the Plan's Policies and Procedures on Training Workforce Members, the Privacy Official will provide a copy of the employer certification to each Designated Employee and explain how that document restricts the PHI that those Designated Employees can use and disclose in connection with the Plan. The Privacy Official will ensure that the Plan's notice of privacy practices includes a statement that the Employer will receive, use and disclose PHI for various Plan administration purposes.
It is the Plan's policy that the Employer is prohibited from using PHI in connection with employment-related purposes or for purposes of any benefit plan or program other than the Plan, unless that program is part of an organized health care arrangement (as defined in the Privacy Rules) that includes the Plan.	[RESERVED]

3. POLICIES AND PROCEDURES FOR IDENTIFYING BUSINESS ASSOCIATES

<i>Policies for Identifying Business Associates</i>	<i>Procedures for Identifying Business Associates</i>
It is the Plan's policy to identify each of the persons or entities that provide services in connection with the Plan and to determine which of those service providers are business associates (as defined in the Privacy Rules) of the Plan.	<p>Before the Effective Date, the Privacy Official will complete a Services Worksheet and Inventory of Business Associates with respect to all then-current service providers with respect to the Plan. Only those service providers included on the Inventory of Business Associates will be treated as Business Associates of the Plan. Thereafter, the Privacy Official will review the Services Worksheet and Inventory of Business Associates on a monthly basis to determine if it remains accurate and complete. In addition to making such changes as are indicated upon regular review:</p> <ul style="list-style-type: none"> • Whenever the duties of a service provider with respect to the Plan are or will be changing, prior to that change going into effect (or as soon thereafter as the Privacy Official becomes aware of the change), the Privacy Official will review the Services Worksheet information previously completed with respect to that service provider to determine whether the change in the services provided to the Plan changes the service provider's business associate status, and, if so, will revise the Plan's Inventory of Business Associates to reflect that change. • Whenever a new person or entity is or will be providing services in connection with the Plan, prior to that person or entity beginning to perform such services (or as soon thereafter as the Privacy Official becomes aware of the change), the Privacy Official will complete the Services Worksheet and Inventory of Business with respect to that new service provider. If the Privacy Official determines that the new service provider should be included on the Inventory of Business Associates, that service provider will be treated as a Business Associate of the Plan.

4. POLICIES AND PROCEDURES FOR RETAINING BUSINESS ASSOCIATES

<i>Policies for Retaining Business Associates</i>	<i>Procedures for Retaining Business Associates</i>

<i>Policies for Retaining Business Associates</i>	<i>Procedures for Retaining Business Associates</i>
It is the Plan's policy to require each Business Associate to enter into a contract that meets the requirements of the Privacy Rules.	From and after the Effective Date, the Plan will require all Business Associates to enter into a contract that meets the requirements of these Policies and Procedures for Retaining Business Associates before the earlier of: <ul style="list-style-type: none"> ● The date a Business Associate receives any PHI in connection with the Plan, or ● The date the Business Associate performs any services in connection with the Plan.
It is the Plan's policy to include in its contracts with Business Associates all of the provisions required by section 164.504(e) of the Privacy Rules, as well as provisions that allow for a Business Associate to use and disclose PHI created or received pursuant to such contract to the extent necessary for the Permissible Purposes, provided, in the case of each of the Permissible Purposes, that the applicable requirements of the Privacy Rules for allowing such uses and disclosures are met.	The Privacy Official will consult with the City Attorney in negotiating any contracts with Business Associate to ensure compliance with the Privacy Rules, and will obtain Common Council authorization before entering into such contracts.
It is the Plan's Policy to require its TPAs, in addition to agreeing to the provisions required by section 164.504(e) of the Privacy Rules, to assume the Plan's administrative responsibilities under the Privacy Rules to the extent feasible, and to include provisions permitting this and requiring the TPA to indemnify the Plan and the Plan Sponsor for any violation of the Privacy Rules by the TPA.	The Privacy Official will consult with the City Attorney in negotiating any contracts with TPAs to ensure compliance with the Privacy Rules, and will obtain Common Council authorization before entering into such contracts.

5. POLICIES AND PROCEDURES FOR VERIFYING IDENTITY AND AUTHORITY

<i>Policies for Verifying Identity and Authority</i>	<i>Procedures for Verifying Identity and Authority</i>
It is the Plan's policy that, from and after the Effective Date, the Employer will not allow access to or disclose Plan PHI to any person requesting such access or disclosure without first verifying the identity of such person, and such person's authority for such access or disclosure, unless the person's identity and authority are known to the Employer.	In accordance with the Plan's Policies and Procedures on Training, the Privacy Official will provide a copy of these Policies and Procedures on Verifying Identity and Authority to each Designated Employee and review the following procedures for responding to requests from persons who are not known to the Designated Employee responding to a request: <ul style="list-style-type: none"> ● In the case of an Individual requesting his or her own PHI in person: <ul style="list-style-type: none"> ○ Request a photo i.d. (e.g., valid and current driver's license or passport) and verify that the person making the request is the person identified and is the subject of the requested PHI. If in doubt about the validity of the i.d., or whether it belongs to the person presenting it, contact the Privacy Official, who will make a final determination. ○ Make a copy of the photo i.d., and file it with the information for which access or disclosure is requested in

<i>Policies for Verifying Identity and Authority</i>	<i>Procedures for Verifying Identity and Authority</i>
	<p>the Individual's Plan file.</p> <ul style="list-style-type: none"> • In the case of a parent requesting access to or disclosure of a minor child's PHI: <ul style="list-style-type: none"> ○ Verify the identity of the parent as described above for verifying an individual's identity. ○ Request proof of the relationship between the minor child whose information is requested and the parent (e.g., birth certificate, adoption order, court order). If in doubt about the validity of the documentation or whether it represents parental authority, contact the Privacy Official, who will make a final determination. ○ If the child is age 16 or older, request a written representation from the parent that the child is not an emancipated minor. ○ Make a copy of the documentation of the relationship and the written statement, if any, and file it with the information for which access or disclosure is requested in the Individual's Plan file. • In the case of a personal representative requesting access to or disclosure of an Individual's Plan PHI: <ul style="list-style-type: none"> ○ Verify the identity of the requester as described above for verifying an Individual's identity. ○ Request valid power of attorney or other court order establishing the requester as the Individual's personal representative. If in doubt about the validity of the documentation or whether it represents authority to act as a personal representative, contact the Privacy Official, who will make a final determination. ○ Make a copy of the documentation of the personal representation, and file it with the information for which access or disclosure is requested in the Individual's Plan file. • In the case of a caller requesting PHI over the telephone: <ul style="list-style-type: none"> ○ Refer all calls from providers to the appropriate TPA.

6. POLICIES AND PROCEDURES FOR REASONABLE SAFEGUARDS FOR PHI

<i>Policies for Reasonable Safeguards for PHI</i>	<i>Procedures for Reasonable Safeguards for PHI</i>
<p>It is the Plan's policy, from and after the Effective Date, to implement measures that reasonably safeguard PHI from intentional or unintentional misuse or inappropriate disclosure.</p>	<p>The Privacy Official, in consultation with the City Attorney, will determine from time to time the appropriate administrative, physical and technical safeguards to put in place pursuant to section 164.530 of the Privacy Rules to reasonably assure that:</p> <ul style="list-style-type: none"> • Employees of the Employer other than the Designated Employees are not able access PHI; • Designated Employees have access only to the minimum necessary PHI that they need to perform their job duties that constitute Plan Administration Functions; • Designated Employees whose job duties include functions for which use of PHI is prohibited do not use PHI for such purposes; and • PHI is securely transmitted and stored.

7. POLICIES AND PROCEDURES FOR TRAINING WORKFORCE MEMBERS

<i>Policies for Training Workforce Members</i>	<i>Procedures for Training Workforce Members</i>
<p>It is the Plan’s policy to train all of the Designated Employees on the Plan’s policies and procedures in connection with its obligations under the Privacy Rules, and to provide training to other members of the Employer’s workforce as needed to make them aware of issues arising due to the Plan’s obligations under the Privacy Rules that may affect their work.</p>	<p>Before the Effective Date, the Privacy Office will develop training schedules and educate the various Designated Employees on the impact that the Plan’s obligations will have on their job duties. In developing such schedules and programs, the Privacy Office will consider the following:</p> <ul style="list-style-type: none"> • New Designated Employees, or Designated Employees with new job functions, to be provided appropriate training for their new job duties, and • Retraining affected Designated Employees in the event that the Plan makes material changes to its policies and procedures.

8. POLICIES AND PROCEDURES FOR SANCTIONING WORKFORCE MEMBERS

<i>Policies for Sanctioning Workforce Members</i>	<i>Procedures for Sanctioning Workforce Members</i>
<p>It is the Plan’s policy that sanctions will be imposed in accordance with applicable collective bargaining agreements, ordinances, and City Service Commission Rules in the event that a Designated Employee fails to comply with the Plan’s policies and procedures other than in Excepted Situations.</p>	<p style="text-align: center;">[RESERVED]</p>

9. POLICIES AND PROCEDURES FOR REFRAINING FROM INTIMIDATING OR RETALIATORY ACTS

<i>Policies for Refraining from Intimidating or Retaliatory Acts</i>	<i>Procedures for Refraining from Intimidating or Retaliatory Acts</i>
<p>It is the Plan’s policy that neither the Plan, the Employer nor any Designated Employee will intimidate, threaten, coerce, discriminate against, or otherwise retaliate against any Individual for exercising that Individual’s rights under the Privacy Rules, for filing a complaint in connection with the Plan’s privacy practices, for participating in an investigation of privacy practices, or opposing any improper practice under the Privacy Rules.</p>	<p style="text-align: center;">[RESERVED]</p>

10. POLICIES AND PROCEDURES FOR RESPONDING TO REQUESTS FOR RESTRICTIONS

<i>Policies for Responding to Requests for Restrictions</i>	<i>Procedures for Responding to Requests for Restrictions</i>
<p>It is the Plan's policy to afford Individuals the opportunity, as required by the Privacy Rules, to request the Plan to implement restrictions on the uses and disclosures that the Plan makes of the Individual's PHI, and to require Individuals to submit their requests for such restrictions in writing.</p>	<p>From and after the Effective Date, an Individual may request restrictions on the uses and disclosures that the Plan makes of PHI of which the Individual is the subject by completing such form as the Plan maintains for that purpose from time to time and submitting such completed form to the Plan Contact at the following address or fax number:</p> <p style="text-align: center;">Michael J. Brady Director of Employee Benefits 200 East Wells Street, Room 706 Milwaukee, WI 53202 Phone (414) 286-3751 Fax (414) 286-0800</p> <p>An Individual's request for restrictions will be considered made when such form is received by the Plan Contact, properly completed. The Plan Contact will refer each such request to the appropriate TPA. The Privacy Official will ensure that the Plan's notice of privacy practices states that such requests must be made in writing.</p>
<p>It is the Plan's policy that, from and after the Effective Date, the Employer generally will not agree to any restrictions on the uses and disclosures the Plan makes of an Individual's PHI.</p>	<p>In accordance with the Plan's Policies and Procedures on Training Workforce Members, the Privacy Official will provide a copy of these Policies and Procedures to each Designated Employee and instruct each of them to alert the Privacy Official of any interaction with an Individual that could be misconstrued as an agreement to restrict the uses and disclosures the Plan makes of that Individual's PHI. The Privacy Official will ensure that the Plan's notice of privacy practices states that no restriction is agreed to by the Plan unless expressly accepted by the Plan in writing.</p>
<p>It is the Plan's policy to require that each of its Business Associates that is a TPA to receive and respond to requests for restrictions, and to implement or deny restrictions, on behalf of the Plan, in accordance with the requirements of the Privacy Rules as applicable to the Plan, to the extent that such restrictions are requested in connection with the health benefits program for which the TPA provides claims administration.</p>	<p>The Plan will require that the TPA, on behalf of the Plan and in accordance with the requirements applicable to the Plan under the Privacy Rules, respond to requests for restrictions. The Privacy Official, in consultation with the City Attorney, will review the TPAs Policies and Procedures with respect to requests for restriction.</p> <p>Any individual making requests for restrictions shall also be referred to the TPA.</p>
<p>It is the Plan's policy to maintain documentation of the handling of all requests for restrictions that it receives.</p>	<p>The Privacy Official, in consultation with the City Attorney, will review the policies and procedures received from the Plan's TPA(s) pursuant to the Business Associate contract with that TPA, to ensure that such policies and procedures provide that, the TPA, on behalf of the Plan, will document requests for restrictions and responses, if any, thereto, and will retain the documentation as required by §164.530(j) of the Privacy Rules</p>

11. POLICIES AND PROCEDURES FOR RESPONDING TO REQUESTS FOR CONFIDENTIAL COMMUNICATIONS

<i>Policies for Responding to Requests for Confidential Communications</i>	<i>Procedures for Responding to Requests for Confidential Communications</i>
----------------------------------------------------------------------------	------------------------------------------------------------------------------

<i>Policies for Responding to Requests for Confidential Communications</i>	<i>Procedures for Responding to Requests for Confidential Communications</i>
<p>It is the Plan's policy to afford Individuals the opportunity, as required by the Privacy Rules, to request the Plan to communicate with the Individual regarding the Individual's PHI at an alternate location or by alternate means ("confidential communications"), and to require Individuals to submit their requests for such confidential communications in writing.</p>	<p>From and after the Effective Date, an Individual may request that the Plan provide confidential communications of PHI of which the Individual is the subject by completing such form as the Plan maintains for that purpose from time to time and submitting such completed form to the Plan Contact at the following address or fax number:</p> <p style="padding-left: 40px;">Michael J. Brady, Director of Employee Relations 200 E. Wells Street, Room 706 Milwaukee, WI 53202 Phone (414) 286-3751 Fax (414) 286-0800</p> <p>An Individual's request for confidential communications will be considered made when such form is received by the Plan Contact, properly completed. The Plan Contact will refer each such request to the appropriate TPA. The Privacy Official will ensure that the Plan's notice of privacy practices states that such requests must be made in writing.</p>
<p>It is the Plan's policy that, from and after the Effective Date, the Employer will not agree to confidential communications of an Individual's PHI unless the Individual's request for confidential communications contains a statement that disclosure of all or part of the Individual's PHI could endanger the Individual, and the Individual provides information about how any payment issues with respect to the Plan will be handled, if applicable, and specifies an alternative address or other method of contact.</p>	<p>In accordance with the Plan's Policies and Procedures on Training Workforce Members, the Privacy Official will provide a copy of these Policies and Procedures on Responding to Requests for Confidential Communications to each Designated Employee and instruct each of them to alert the Privacy Official of any interaction with an Individual that could be construed as an agreement to use confidential communications for that Individual's PHI. The Privacy Official will ensure that the Plan's notice of privacy practices states that no agreement by the Plan to use confidential communications is effective unless expressly accepted by the Plan in writing. In the event that the Plan Contact receives a request for confidential communications stating that disclosure of all or part of the Individual's PHI could endanger the Individual, the Plan Contact will notify the Privacy Official and will note that statement in the transmittal of the request to the appropriate TPA(s). The Privacy Official will follow up with the appropriate TPA(s) to determine whether they decide, on behalf of the Plan, to honor the request, and, if so, the Privacy Official will notify Designated Employees whose job duties may involve communicating PHI to that Individual of the alternate location or means of communication.</p>
<p>It is the Plan's policy to request that each of its TPAs receive and respond to requests for confidential communications, and to implement or deny confidential communications, in accordance with the requirements of the Privacy, to the extent that such confidential communications are requested in connection with the health benefits program for which the TPA provides claims administration.</p>	<p>The Plan will request that its TPAs, in accordance with the requirements applicable under the Privacy Rules, to</p>

<i>Policies for Responding to Requests for Confidential Communications</i>	<i>Procedures for Responding to Requests for Confidential Communications</i>
It is the Plan's policy to maintain documentation of the handling of all requests for confidential communications that it receives.	The Privacy Official will review the policies and procedures received from the Plan's TPA(s), in consultation with the City Attorney, to ensure that such policies and procedures provide that, the TPA, on behalf of the Plan, will document requests for confidential communications and responses, if any, thereto, and will retain the documentation as required by §164.530(j) of the Privacy Rules. .
It is the Plan's policy to respond to requests for confidential communications only from the Individual for whose information confidential communications are sought, except in cases where the person requesting information can show authority to act on behalf of the Individual.	The Privacy Official will review the policies and procedures received from the Plan's TPA(s), in consultation with the City Attorney, to ensure that such policies and procedures provide that, the TPA, on behalf of the Plan, will not respond to a request for confidential communications from any individual other than the Individual whose PHI is requested to be communicated confidentially unless the TPA has verified the identity and authority of that other individual in accordance with policies and procedures similar in substance to the Plan's Policies and Procedures for Verifying Identity and Authority.

12. POLICIES AND PROCEDURES FOR IDENTIFYING DESIGNATED RECORD SET

<i>Policies for Identifying Designated Record Set</i>	<i>Procedures for Identifying Designated Record Set</i>
It is the Plan's policy to require the Employer to identify those records held by the Employer that constitute part of the Designated Record Set.	Before the Effective Date, the Privacy Official will create a listing of all Designated Information, including the location thereof, that is maintained or received by the Employer. Thereafter, the Privacy Official will review that listing on a semiannual basis to determine whether it remains accurate and complete and make such changes as are indicated by that review.
It is the policy of the Plan to require each of its Business Associates that is a TPA to provide access to a Designated Record Set upon request, to the Plan or an individual in order to meet the requirements of 45 CFR 164.524. .	The Privacy Official will review the policies and procedures received from the Plan's TPA(s), in consultation with the City Attorney, to ensure that such policies and procedures provide that, the TPA, on behalf of the Plan, meets the requirements of 45 CFR 164.524. The Privacy Official will maintain the policies and procedures it receives from the Plan's TPAs with the Plan's policies and procedures.

13. POLICIES AND PROCEDURES FOR PROVIDING INDIVIDUALS ACCESS TO THEIR PHI

<i>Policies for Providing Individuals Access to Their PHI</i>	<i>Procedures for Providing Individuals Access to Their PHI</i>
----------------------------------------------------------------------	------------------------------------------------------------------------

<i>Policies for Providing Individuals Access to Their PHI</i>	<i>Procedures for Providing Individuals Access to Their PHI</i>
<p>It is the Plan's policy to afford Individuals access to their PHI in the Plan's Designated Record Set as required by the Privacy Rules, and to require Individuals to submit their requests for such access in writing.</p>	<p>From and after the Effective Date, an Individual may obtain access to PHI of which the Individual is the subject that the Plan maintains in the Designated Record Set by completing such form as the Plan maintains for that purpose from time to time and submitting such completed form to the Plan Contact at the following address or fax number:</p> <p style="padding-left: 40px;">Michael J. Brady, Director of Employee Relations 200 E. Wells Street, Room 706 Milwaukee, WI 53202 Phone (414) 286-3751 Fax (414) 286-0800</p> <p>An Individual's request for access will be considered made when such form is received by the Plan Contact, properly completed. The Plan Contact will refer each such request to the appropriate TPA. The Privacy Official will ensure that the Plan's notice of privacy practices states that such requests must be made in writing.</p>
<p>It is the Plan's policy to require each of its Business Associates that is a TPA to receive and respond to requests for access to PHI as required by the Privacy Rules..</p>	<p>In each of its contracts with Business Associates that are TPAs, the Plan will require the TPA to comply with the requirements of the Privacy Rules with respect to individuals' access to PHI.</p>
<p>It is the Plan's policy to require its TPAs to respond to Individuals' properly submitted requests for access on a timely basis in accordance with the requirements of the Privacy Rules.</p>	<p>The Privacy Official, in consultation with the City Attorney, will review the policies and procedures received from the Plan's TPA(s) pursuant to the Business Associate contract with that TPA, to ensure that such policies and procedures provide that the TPA will respond to a properly submitted request for access in accordance with the requirements of the Privacy Rules.</p> <p>In each of its contracts with its Business Associates that are not TPAs, the Plan will require such Business Associates to comply with the requirements of section 164.524 of the Privacy Rules in connection with Individuals' requests for access by making PHI concerning an Individual available for purposes of responding to the Individual's request for access.</p> <p>If an Individual requests access to PHI in the Designated Record Set directly from the Plan or the Employer, the Plan Contact will notify the appropriate TPA(s) in writing of such request within five (5) business days of the Individual's request.</p>
<p>It is the Plan's policy to maintain documentation of the handling of all requests for access it receives.</p>	<p>The Privacy Official, in consultation with the City Attorney, will review the policies and procedures received from the Plan's TPA(s) pursuant to the Business Associate contract with that TPA, to ensure that such policies and procedures provide that, the TPA, on behalf of the Plan, will document requests for access and responses thereto, and will retain the documentation as required by §164.530(j) of the Privacy Rules</p>
<p>It is the Plan's policy to grant access only to the Individual whose information is sought, except in cases where the person requesting information can show authority to act on behalf of the Individual.</p>	<p>The Privacy Official, in consultation with the City Attorney, will review the policies and procedures received from the Plan's TPA(s) pursuant to the Business Associate contract with that TPA, to ensure that such policies and procedures provide that, the TPA, on behalf of the Plan, will not provide access to any individual other than the Individual whose PHI is requested to be accessed unless the TPA has verified the identity and authority of that other individual in accordance with policies and procedures for verifying identity and authority.</p>

14. POLICIES AND PROCEDURES FOR ALLOWING INDIVIDUALS TO AMEND THEIR PHI

<i>Policies for Allowing Individuals to Amend Their PHI</i>	<i>Procedures for Allowing Individuals to Amend Their PHI</i>
<p>It is the Plan’s policy to afford Individuals the opportunity to request amendments to their PHI in the Plan’s Designated Record Set as required by the Privacy Rules, and to require Individuals to submit their requests for such amendments in writing.</p>	<p>The Plan will refer any Individuals requesting amendment of their PHI to the appropriate TPA. If the request involves PHI held by the Plan, the Plan will:</p> <ul style="list-style-type: none"> • Verify the identity of an Individual or the authority of a personal representative exercising such amendment rights, • Determine whether to accept or deny a requested amendment in whole or in part, • Provide notice of the decision to the Individual, • Administer any appeal, accept any statements of disagreement and create appropriate rebuttal statements, and • Maintain any such requests, responses, amendments and/or statements as part of the Designated Record Set . <p>The Plan will also identify and notify third-parties of amendments as required by the Privacy Rules.</p>
<p>It is the Plan’s policy to require that each of its Business Associates that is a TPA to make any amendments to PHI that the Plan directs or agrees to pursuant to section 164.526 of the Privacy Rules.</p>	<p>The Plan’s agreements with Business Associates that are TPAs will require that the TPAs receive and respond to Individuals’ requests for amendments to their PHI in accordance with the requirements applicable under section 164.526 of the Privacy Rules.</p>
<p>It is the Plan’s policy to require its TPAs to respond to Individuals’ properly submitted requests for amendments on a timely basis in accordance with the requirements of the Privacy Rules.</p>	<p>The Plan’s agreements with Business Associates that are TPAs will require that the TPAs receive and respond to Individuals’ requests for amendments to their PHI in accordance with the requirements applicable under the Privacy Rules.</p> <p>If an Individual requests amendments to PHI in the Designated Record Set directly from the Plan or the Employer, the Plan Contact will notify Business Associate in writing of such request within five (5) business days of the Individual’s request.</p>
<p>It is the Plan’s policy to maintain documentation of the handling of all requests for amendments it receives.</p>	<p>The Plan will maintain documentation of all requests for amendments that it receives, the Plan’s determination on the request, it’s response to the Individual requesting the amendment, and any subsequent actions or inquiries with respect to such request, including informing the Individual of the right to file a complaint with the Department of Health and Social Services.</p>
<p>It is the Plan’s policy to allow amendment requests only from the Individual whose PHI is at issue, except in cases where the person requesting the amendment can show authority to act on behalf of the Individual whose PHI is at issue.</p>	<p>The Privacy Official, will not allow an amendment request from any individual other than the Individual whose PHI is at issue unless the it has verified the identity and authority of that other individual in accordance with the Plan’s Policies and Procedures for Verifying Identity and Authority.</p>
<p>It is the Plan’s policy that, when informed of an amendment made to PHI in the Plan’s designated record set by another covered entity, the Plan will amend its designated record set to reflect that amendment.</p>	<p>The Privacy Official, in consultation with the City Attorney, will review the policies and procedures received from the Plan’s TPA(s) pursuant to the Business Associate contract with that TPA, to ensure that such policies and procedures provide that, the TPA will amend PHI in its possession to reflect amendments which other covered entities have accepted, and will require other Business Associates of the Plan or the Employer to amend PHI in their possession as necessary to reflect such amendments.</p>

15. POLICIES AND PROCEDURES FOR ACCOUNTING TO INDIVIDUALS FOR DISCLOSURE OF PHI

<i>Policies for Accounting to Individuals for Disclosure of Their PHI</i>	<i>Procedures for Accounting to Individuals for Disclosure of Their PHI</i>
<p>It is the Plan's policy to provide Individuals an accounting of disclosure of their PHI as required by the Privacy Rules, and to require Individuals to submit their requests for such an accounting in writing.</p>	<p>From and after the Effective Date, an Individual may obtain accounting of certain disclosures of PHI of which the Individual is the subject that the Plan has made since the Effective Date and no more than six (6) years before the date of the Individual's request, by completing such form as the Plan maintains for that purpose from time to time and submitting such completed form to the Plan Contact at the following address or fax number:</p> <p style="text-align: center;">Michael J. Brady, Director of Employee Relations 200 E. Wells Street, Room 706 Milwaukee, WI 53202</p> <p style="text-align: center;">Phone (414) 286-3751 Fax (414) 286-0800</p> <p>An Individual's request for access will be considered made when such form is received by the Plan Contact, properly completed. The Plan Contact shall refer each such request to the appropriate TPA. The Privacy Official will ensure that the Plan's notice of privacy practices states that such requests must be made in writing.</p>
<p>It is the Plan's policy that the Employer will not make any disclosures that are subject to the accounting requirement unless required by law to do so.</p>	<p>In accordance with the Plan's Policies and Procedures on Training, the Privacy Official will provide a copy of these Policies and Procedures on Accounting to Individuals for Disclosures of Their PHI to each Designated Employee and instruct each of them to alert the Privacy Official of any disclosures they make of PHI that they believe may be required by applicable law. The Privacy Official will make a determination about whether the disclosure is required by applicable law, and, if so, will keep a record of such disclosure for purposes of providing an accounting of disclosures to an Individual.</p>
<p>It is the Plan's policy to require each of its Business Associates that is a TPA to document disclosures of PHI and information related to such disclosures as would be required for the Plan to respond to a request by an individual for an accounting of disclosures of PHI in accordance with Section 164.528 of the Privacy Rules, and to provide to the Plan (or an individual upon the Plan's request) such information, in order to permit the Plan to respond to a request by an individual for an accounting of disclosures of PHI in accordance with section 164. 528 of the Privacy Rules.</p>	<p>In accordance with the Plan's Policies and Procedures for Retaining Business Associates, in each of its contracts with its Business Associates that are TPAs, the Plan will require the TPA, on behalf of the Plan and in accordance with the requirements applicable to the Plan under the Privacy Rules, to document disclosures of PHI and information related to such disclosures as would be required for the Plan to respond to a request by an individual for an accounting of disclosures of PHI in accordance with 45 CFR 164.528, and to provide to the Plan (or an individual upon the Plan's request) such information, in order to permit the Plan to respond to a request by an individual for an accounting of disclosures of PHI in accordance with section 164. 528 of the Privacy Rules. .</p>
<p>It is the Plan's policy to require its TPAs to</p>	<p>The Plan's contracts with Business Associates that are TPAs will include a provision requiring the TPAs to respond to an Individual's request for accounting of PHI as required</p>

<i>Policies for Accounting to Individuals for Disclosure of Their PHI</i>	<i>Procedures for Accounting to Individuals for Disclosure of Their PHI</i>
respond to Individual's requests for accounting as required by the Privacy Rules.	by the Privacy Rules.
It is the Plan's policy to maintain documentation of the handling of all requests for accounting it receives.	The Privacy Official, in consultation with the City Attorney, will review the policies and procedures received from the Plan's TPA(s) pursuant to the Business Associate contract with that TPA, to ensure that such policies and procedures provide that, the TPA, on behalf of the Plan, will document requests for accounting and responses thereto, and will retain the documentation as required by §164.530(j) of the Privacy Rules.
It is the Plan's policy to provide an accounting only to the Individual whose information is sought, except in cases where the person requesting information can show authority to act on behalf of the Individual.	The Privacy Official, in consultation with the City Attorney, will review the policies and procedures received from the Plan's TPA(s) pursuant to the Business Associate contract with that TPA, to ensure that such policies and procedures provide that, the TPA, on behalf of the Plan, will not provide an accounting to any individual other than the Individual whose PHI is requested to be accessed unless the TPA has verified the identity and authority of that other individual in accordance with policies and procedures similar in substance to the Plan's Policies and Procedures for Verifying Identity and Authority.

1045-2003-542:64523