HEALTH BENEFITS PLAN
FOR
STATE AND LOCAL EMPLOYEES

HIPAA Privacy Policy and Procedure Manual

Department of Human Resource Management
Office of Health Benefits Programs

TABLE OF CONTENTS

SECTION ONE: MEMBERS' RIGHTS

This section contains policies that implement the specific rights that are granted to members by the federal HIPAA privacy regulations. "Members" are beneficiaries of the employee health benefit plan. This includes employees, their dependents, retirees (if covered), and COBRA enrollees.

These policies should be integrated with existing policies that govern privacy issues, as well as additional rights not addressed in HIPAA.

Federal HIPAA standards pre-empt state standards only when the state requirement is both contrary to the federal standard and less stringent than the federal standard.

MEMBER REQUESTS TO RESTRICT THE USE OR DISCLOSURE OF PROTECTED HEALTH INFORMATION

RESPONSIBILITY: Privacy Official, Employee Services

BACKGROUND:

Federal privacy regulations give members the right to request that the Health Benefits Plan for State and Local Employees (Plan) restrict the use or disclosure of some or all of their protected health information. However, the regulations make it clear that the Plan is not required to agree to any such request.

POLICY:

Any restriction on the use or disclosure of PHI to which the Plan agrees must be fully documented to assure that all members of the Plan's workforce are aware of the restriction and can abide by it.

Restricted information will not be used or disclosed in violation of the restriction unless such a use or disclosure is necessary for treatment of the member in an emergency.

A restriction on the use or disclosure of protected health information may be terminated if the member agrees to the termination, either in writing or orally. The Plan may terminate such a restriction without the member's agreement, but in that case the restriction will still apply to protected health information obtained while the restriction was in effect.

Any restriction on the use or disclosure of protected health information, and the termination of any such restriction, will be fully documented. The documentation of an agreed restriction will be kept for as long as it is in force, plus six years. Documentation of termination of a restriction will be kept for at least six years.

PROCEDURE:

1. Any member of the Office of Health Benefits or any agency/local employer Benefit Administrator (BA), who receives a request from a member to restrict the use or disclosure of protected health information, will refer the request to the Privacy Official (or designee).

2. If the Privacy Official agrees to restrict the use or disclosure of certain protected health information, he or she shall record the restriction in sufficient detail to permit other members of the workforce and Business Associates to comply with it.

3. Any subsequent termination of the restriction will be documented in the same way as the initial restriction. Such documentation will include identification, including dates of service, of any PHI to which the terminated restriction still applies. Documentation of termination of a restriction will include the effective date, a notation as to whether the member agreed or not, and a notation of whether such agreement was oral or in writing. If in writing, a copy of the writing will be filed with documentation of the restriction and the termination.

4. The Privacy Official will work with the Plan's Business Associate to flag protected health information that is subject to a restriction. Users of the information, whether in electronic or paper form, will be referred to a location where they can read the restriction, and termination of the restriction if applicable.

5. The Privacy Official and the Plan's Business Associates will develop procedures to restrict access within the organization to information whose use is subject to a restriction under this policy.

ALTERNATIVE COMMUNICATION OF HEALTH INFORMATION

RESPONSIBILITY: Privacy Official

BACKGROUND:

To protect their confidentiality, some members may want to have communications that contain their protected health information (PHI) sent to them by alternative means, or to an alternative address. The Health Benefits Plan for State and Local Employees (the Plan) will accommodate such requests as long as they are reasonable.

In this context, "alternative" means different from the usual. For instance, a member may request that explanations of benefits (EOBs) be sent to a post office box rather than to the address listed in the Plan's benefit eligibility records. Or a member may request that his or her PHI not be included on an EOB that is sent to the subscriber under whose health benefit contract the member is enrolled as a dependent.

POLICY:

Members may request that any communication of protected health information from the Plan be sent to them by alternative means or to an alternative address. The request may apply to all communications, or only to communication of certain specific information.

The Plan will comply with any such request that is "reasonable," provided that:

1. If the request involves a change in billing procedures, the member provides information on how payment will be handled. For instance, if a bill is sent directly to the member rather than to the employee/retiree, will the member pay the bill?

2. The member is specific in providing an alternative address and/or the alternative means of communication to be used.

3. The incremental cost of complying with the request for alternative communication is reasonable, or the member makes arrangements to pay the incremental cost.

4. The member clearly states that the disclosure of all or part of the information could endanger the member.

PROCEDURE:

1. Any member of the Office of Health Benefits or any agency/local employer BA, who receives a request from a member for alternative communication, will refer the request to the Privacy Official (or designee).

2. The Privacy Official (or designee) will determine the reasonableness of the request on the basis of the four criteria stated above.

3. The Privacy Official (or designee) will agree to the request if it is "reasonable," as defined above.

4. The Privacy Official (or designee) will document what decision was made, and the rationale for the decision. If applicable, the Privacy Official (or designee) will also document how the Plan proposes to comply with the request.

5. The Privacy Official (or designee) will confer with other members of the workforce and its business associates, as appropriate, to determine whether the Plan can comply with the request without unreasonable administrative difficulty, and to determine how the Plan will comply with the request.

RIGHT OF ACCESS TO PROTECTED HEALTH INFORMATION

RESPONSIBILITY: Privacy Official, Employee Services

BACKGROUND:

Members have a right to inspect, or to receive a copy of their protected health information (PHI) in the Health Benefits Plan for State and Local Employees's (Plan) records. Some exceptions apply, as defined further in this policy.

POLICY:

The Plan will provide members with access to certain protected health information that is in the custody of the Plan. Members may also receive a copy of such records.

This right applies only to protected health information that is stored in "designated record sets." It does not apply to protected health information stored in other forms, such as information stored in correspondence files.

In certain circumstances, the Plan may deny a member access to certain PHI, as provided for in this policy.

Form of Access

1. The Plan will provide the member with access to PHI in the form the member requests, if the information is readily producible in that form (e.g. paper or electronic medium).

2. If the information cannot be readily produced in the form requested by the member, it will be provided in readable hard copy.

3. The member may be provided with summary information if the member has agreed in advance that this is acceptable, and has agreed to pay the fee for creating the summary.

4. The member will be granted access to the information at a mutually convenient time and place, as discussed with the member. The member may also receive a copy of the information by mail upon request.

Denial of Access: Reasons For Which There Is Not a Right of Review

The Plan may deny the member access to certain information as follows. In these instances, the decision to deny access is final and the member will not be granted the opportunity to request a review of the decision.

1. Members do not have a right to have access to, or a copy of, the following types of information:

   1.1. Psychotherapy notes

   1.2. Information compiled for use in a criminal, civil or administrative proceeding or action

   1.3. Information to which members may not have access under the terms of the Clinical Laboratory Improvements Act (CLIA).

2. A member's access to protected health information that was created or obtained in the course of research that includes treatment (during a clinical trial, for example) may be temporarily suspended for as long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and the covered health care provider has informed the individual that the right of access will be reinstated upon completion of the research.

3. A member's access may be denied if the protected health information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

4. The Plan may deny a member's request for access to information if the Plan does not maintain the requested information in a designated record set. However, if the Plan does not maintain the requested information, but knows where the requested information is maintained, the notice of denial will inform the member where to direct the request for access.

Denial of Access: Reasons for Which There <u>Is</u> a Right of Review

The Plan may also deny access to certain information for the following reasons. When one of the following is the reason for the denial, the member will be granted the opportunity to request a review of the decision.

1. A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person; or

2. The protected health information makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or

3. The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional

judgment, that granting the personal representative access to the requested information is reasonably likely to cause substantial harm to the individual or another person. (Example: a record that identifies the member as a victim of abuse, and names the personal representative as the perpetrator.)

Federal HIPAA privacy regulations require that the determinations described in the three preceding paragraphs be made by a licensed health care professional.

When a member has been denied access to certain information, the member will be granted access to all other requested information to the extent possible.

Notice of Denial of Access

A notice of denial of access must contain all of the following:

1. Basis for the denial.

2. A statement of any review rights, if applicable.

3. A statement of how the member may complain to the Plan or to the Secretary, Department of Health and Human Services.

4. If access is denied because the Plan does not maintain the information, the notice of denial must include any information that the Plan has regarding the location of the requested information.

Review of Denial of Access

When the reason for denial of access is subject to review, that review will be conducted by a licensed health care professional designated by the Plan to act as a reviewer. The reviewer may not have participated in the original decision to deny access. The decision of the reviewer is final, and is binding on the Plan. The referral for review must be prompt, and the reviewer must complete the review within a reasonable period of time. The reviewer will determine the standards of this policy were properly applied in denying access. The Plan will promptly provide written notice of the reviewer's decision to the member.

Time Frames

The Plan must respond to requests for access to PHI within the following time frames:

1. Within 30 days of the date of the request, the Plan must provide access, request an extension, or issue a notice of denial for information that is maintained at the Plan's site.

2. Within 60 days of the date of the request, the Plan must provide access, request an extension, or issue a notice of denial for information that is not maintained at the Plan's site.

3. One extension of up to 30 days is permitted. Requests for extension must be in writing, and must state the reasons for the delay, and the date by which the member will either be granted access or receive a notice of denial.

Fees

Fees to produce either a copy of the requested information, or to produce a summary, may only include:

1. The cost of copying, including the cost of supplies and labor

2. Postage

3. The cost of preparing the summary, if agreed in advance by the member.

Designation of Responsibility for Receiving and Processing Member Requests for Access to PHI

The Privacy Official is responsible for receiving and processing all formal requests for access to protected health information in designated record sets.

PROCEDURE:

Routing

1. Members who request access to, and/or copies of, protected health information will be referred to the Employee Services department.

2. The Employee Services department will instruct the member how to make the request in writing.

3. Written requests for access to or copies of PHI will be routed to the Privacy Official for processing.

Processing

1. The Privacy Official will assure that the request from the member is documented in writing.

2. The Privacy Official will determine which PHI is subject to the request. This is based on the specifics of the request (is it limited to one site, or to certain times?), and on whether the information is in designated record sets.

3. The Privacy Official will determine, based on the type of information requested and applicable state law, whether access to any of the information requested is subject to denial.

4. The Privacy Official or the Plan's TPA will identify which physicians and other professionals have treated the member, and will confer with them regarding whether access to any information should be denied.

5. The Privacy Official will prepare a response to the member. If the response includes denial of access to any PHI, the response will be reviewed by a licensed health care professional, who shall make the final determination whether to deny access as proposed by the Privacy Official. This determination, and the rationale to support it, will be retained by the Privacy Official for six years.

6. If access to any information is to be denied, the response will include the required elements of a notice of denial of access. The response will comply with the time frames in this policy.

7. The Privacy Official will communicate with the member regarding form of access, time and location of access, and costs of any summary or copy of the information. This communication, and the member's responses, will be documented.

8. The Privacy Official will make the necessary arrangements for the member to have access to the requested information, and/or to receive copies of it.

9. The Privacy Official will receive any request for review of denial, and assure that it is processed in accordance with this policy. The Privacy Official will designate the health professional who performs the review. The reviewer must be someone who did not participate in the original decision to deny access to the information in question.

10. The Privacy Official must retain all documentation related to the request for a period of six years.

The Privacy Official may designate other trained members of the workforce to perform the duties assigned to the Privacy Official in this policy, subject to the supervision of the Privacy Official.

INDIVIDUAL REQUESTS TO AMEND HEALTH INFORMATION

RESPONSIBILITY: Privacy Official, Associate Director of Employee Services, Plan's TPAs

BACKGROUND:

Members have the right to request the Health Benefits Plan for State and Local Employees (Plan) to amend certain protected health information. The Plan will consider such requests in accordance with this policy.

POLICY:

Members may request the Plan to amend protected health information that it maintains in designated record sets.

The Plan will make the requested amendment UNLESS:

1. The request is not received in writing, stating a reason to support the requested amendment; or,
2. The Plan was not the originator of such information, unless the member provides a reasonable basis to believe that the originator is no longer available to act on the requested amendment; or,
3. The information to be amended is not maintained in a designated record set; or,
4. The member would not have access to the information under the provisions of the Plan's RIGHT OF ACCESS TO PROTECTED HEALTH INFORMATION policy; or,
5. The Plan considers the information to be accurate and complete.

Time frames

The Plan will respond to requests to amend protected health information within the following time frames:

1. Within 60 days from the date of the written request for amendment, the Plan will either make the requested amendment, request an extension, or issue a notice of denial of request.

2. One 30-day extension is permitted. A request for extension must be in writing, and must include the reason for the delay and the date by which the Plan will complete its action on the request.

Accepted Amendments

1. The amendment(s) will be made by identifying each amended datum, and providing a reference or link to the location of the amendment. No data will be erased. This applies to both paper and electronic records.

2. The member will be informed that the amendment was accepted, within the time frame specified by this policy.

3. The member will be requested to identify other entities to which the amended information needs to be communicated, and to authorize such communication.

4. The Plan will make reasonable efforts to provide the amended information to entities, which the member identifies as needing the amendment, and to others that the Plan knows to have received the unamended information and who may rely or may have relied on that information to the detriment of the member.

Denied Amendments

When a request to amend protected health information is denied, the notice of denial will:

1. Be sent in compliance with the time frames of this policy

2. State the basis for the denial, according to this policy

3. State that the member may appeal the denial in writing, with instructions how to file an appeal

4. State that, if the member does not appeal the denial, the member may request that the Plan provide copies of the member's request for amendment, and the notice of denial, with any future disclosures of the information that is the subject of the request to amend

5. Include a statement of how the member may complain to the Plan or to the Secretary, U. S. Department of Health and Human Services.

Appeal and Rebuttal

A member whose request to amend protected health information has been denied (in whole or in part) may appeal the denial by submitting a statement of disagreement. This is a statement of the reasons why the member disagrees with the denial.

If the Plan decides to make a requested amendment on the basis of a statement of disagreement, the amendment will be made in accordance with this policy.

If the Plan does not accept the reasoning of the statement of disagreement, it will send the member a written rebuttal, stating why it is still not accepting the requested amendment.

Record Keeping

If the amendment is denied, the Plan will identify each datum to which the denied request applied, and for each, provide a reference or link to a copy of the member's request for amendment, the denial letter, any statement of disagreement, and any rebuttal. This applies to both paper and electronic records.

Future Disclosures

1. Future disclosures of amended information will include the amendment.

2. If the member has appealed a denial of amendment, future disclosures of the subject information will include copies of the member's request for amendment, the denial letter, the statement of disagreement, and the rebuttal, or an accurate summary of the original request, the denial, the letter of disagreement and the rebuttal.

3. If the member has not appealed a denial of amendment, future disclosures of the subject information will include copies of the member's request for amendment, and the denial letter, or an accurate summary of the request and denial, only if the member has requested the Plan to do so.

Amendments Made by Others

If another entity amends protected health information which it had previously sent to the Plan, and informs the Plan of the amendment, the subject information will be amended in all the Plan's designated record sets in which it is maintained.

Designation of Responsibility for Receiving and Processing Member Requests for Amendment of PHI

The Privacy Official is responsible for receiving and processing individual requests for amendment of PHI

PROCEDURE:

1. The Privacy Official may designate trained members of the Plan's workforce to perform any of the duties assigned to the Privacy Official in this procedure, subject to the supervision of the Privacy Official.

2. Members who ask about amending protected health information will be referred to the Employee Services department.

3. The Employee Services department will instruct the member how to make the request in writing.

4. Written requests to amend PHI will be routed to the Privacy Official for processing.

Processing procedure

1. The Privacy Official will assure that the request from the member is documented in writing.

2. The Privacy Official will determine whether any of the subject information is not subject to amendment for the reasons stated in this policy.

3. The Privacy Official or the Plan's TPA will identify which physicians and other professionals originated the subject information, and will confer with them regarding whether any information should be amended. If the originator of the information is not available, the Privacy Official or TPA will confer with a designated physician or other professional in the same specialty.

4. The Privacy Official will prepare a response to the member. If amendment of any information is denied, the response will include the required elements of a notice of denial. The response will comply with the time frames in this policy.

5. The Privacy Official will receive any statement of disagreement, and will prepare any rebuttal with the assistance of the professional who originated the information in question or the designated professional if the originator is not available.

6. The Privacy Official will assemble the entire file to be appended to the affected designated record sets, including the original request, notice of denial, statement of disagreement, and rebuttal.

7. The Privacy Official will retain all documentation related to the request, whether it is granted or denied, for as long as the subject data are maintained in designated record sets.

Information management.

8. The TPA's Director of Claims and Enrollment, the TPAs member services department, along with the Plan's Employee Services department and Information Systems department, with the assistance of the Privacy Official, will implement necessary changes in record keeping, both paper end electronic, to effect the required references and links to documents pertaining to a request to amend PHI.

ACCOUNTING OF DISCLOSURES OF HEALTH INFORMATION

RESPONSIBILITY: Privacy Official, Business Associates,

BACKGROUND:

Members have a right to receive an accounting of disclosures of their protected health information. However, this is a limited right. Many routine disclosures are not reportable in this accounting. For instance, disclosures to health care providers for purposes of treatment, or to other health plans for purposes of payment, or to business associates for purposes of health care operations, are not reportable.

This policy identifies which disclosures are reportable, and how requests for an accounting for disclosures will be processed.

POLICY:

1. The Health Benefits Plan for State and Local Employees (Plan) members have a limited right to receive an accounting of the disclosures of their protected health information (PHI) made by the Plan. The accounting must contain all disclosures not listed under Exceptions, below.

2. Disclosures made under each of the following policies must be included in the accounting:

   - DISCLOSURES OF PROTECTED HEALTH INFORMATION THAT ARE REQUIRED BY LAW – GENERAL POLICY
   - DISCLOSURE OF PROTECTED HEALTH INFORMATION FOR PUBLIC HEALTH PURPOSES
   - DISCLOSURE OF PROTECTED HEALTH INFORMATION TO REPORT CHILD ABUSE, OR OTHER ABUSE, NEGLECT, OR DOMESTIC VIOLENCE
   - REPORTING PROTECTED HEALTH INFORMATION TO EMPLOYERS UNDER OSHA AND SIMILAR LAWS
   - DISCLOSURE OF PROTECTED HEALTH INFORMATION TO REGULATORS
   - SUBPOENAS, COURT ORDERS, DISCOVERY REQUESTS, OTHER LEGAL PROCESSES AND THE DISCLOSURE OF PROTECTED HEALTH INFORMATION
   - DISCLOSURE OF PROTECTED HEALTH INFORMATION FOR LAW ENFORCEMENT PURPOSES
   - USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION FOR PURPOSES OF RESEARCH
   - USE AND DISCLOSURES OF PSYCHOTHERAPY NOTES
   - DISCLOSURE OF PROTECTED HEALTH INFORMATION WITHOUT AUTHORIZATION, TO AVERT A SERIOUS THREAT TO HEALTH OR SAFETY

- DISCLOSURE OF PROTECTED HEALTH INFORMATION FOR CERTAIN GOVERNMENT FUNCTIONS (includes PHI of members of the military, or and disclosures related to protective services of the president and others, but excludes national security or intelligent purposes, as noted under "exceptions," below.)
- DISCLOSURE OF PROTECTED HEALTH INFORMATION TO WORKERS' COMPENSATION PROGRAMS
- EXTENSION OF PRIVACY PROTECTION TO DECEASED INDIVIDUALS
- DISCLOSURE OF PROTECTED HEALTH INFORMATION BY "WHISTLEBLOWERS"
- DISCLOSURES OF PROTECTED HEALTH INFORMATION BY WORKFORCE MEMBERS WHO ARE THE VICTIMS OF A CRIME

3. The accounting must include any other disclosure that is made without the member's written authorization, unless the disclosure falls within one of the exceptions listed below. This includes any disclosure made in violation of the Plan policy, or federal or state law, regarding the privacy, security or confidentiality of PHI.

4. The accounting must include disclosures made by business associates for any of the reasons listed above.

Exceptions

This right to an accounting of disclosures does <u>not</u> apply to:

1. Disclosures of PHI for treatment, payment, or health care operations.

2. Disclosure to a member of his or her own PHI.

3. Disclosure made under the authority of an authorization.

4. Disclosure of protected health information to personal representatives.

5. Disclosures to relatives, friends, and others involved in the member's care or payment for care, in accordance with the PROVIDING A MEMBER'S MEDICAL INFORMATION TO FAMILY, FRIENDS, OR OTHERS DIRECTLY INVOLVED IN THE MEMBER'S CARE policy.

6. Disclosures of PHI to disaster relief agencies in accordance with the DISCLOSURE OF PROTECTED HEALTH INFORMATION IN A DISASTER policy.

7. Disclosures to authorized federal officials for purposes of national security or intelligence, in accordance with the DISCLOSURE OF PROTECTED HEALTH INFORMATION FOR CERTAIN GOVERNMENT FUNCTIONS policy.

8. Disclosures of prisoners' PHI to correctional institutions or law enforcement officials in accordance with the DISCLOSURE OF PROTECTED HEALTH INFORMATION OF INMATES policy.

9. Disclosures that are incidental to any use or disclosure permitted under the Plan policies or applicable federal or state law. (An incidental disclosure is a secondary disclosure that cannot reasonably be prevented, is limited in nature, and that occurs as a by-product of an otherwise permitted use or disclosure. Example: a conversation that is overheard despite attempts by the speakers to avoid being heard.)

10. Disclosure of information in a limited data set.

11. Any disclosure that occurred prior to April 14, 2003.

12. Any disclosure that occurred more than six years prior to the date of the request for the accounting, or outside the time period to which the request applies, if the member has requested an accounting for disclosures over a shorter period (less than 6 years).

The Plan must also temporarily omit from such an accounting of disclosures certain disclosures made to regulators and law enforcement officials.

1. The regulatory or law enforcement agency must provide the Plan with a written statement that notifying the member about a disclosure of PHI to the agency would be reasonably likely to impede the agency's activities. The statement must specify the time period during which the member is not to be informed of the disclosure.

2. If the agency is not able to produce a written statement immediately, the Plan may act upon an oral statement for a period of no more than 30 days. The oral statement, including the identity of the agency and/official making the request, must be documented.

3. The suspension of the member's right to an accounting of the disclosure of PHI to the agency is only temporary, lasting only for the period of time requested in the written statement (or for no more than 30 days if no written statement is produced by the agency.)

Request for Accounting

A request for an accounting of disclosures of protected health information must be in writing. It must be dated, and must specify the time period to which the accounting applies, which may not be for a period of more than six years.

Content of Accounting

1. The accounting that is provided to the member must be in writing.

2. The accounting must include all disclosures except those listed under "Exceptions," above. This includes disclosures made by the Plan, and disclosures

by any business associate if the Plan provided the business associate with the PHI that was disclosed.

3. The accounting must include the following information:

   3.1. The date of disclosure,

   3.2. The name, and the address if known, of the entity or person who received the PHI,

   3.3. A brief description of the PHI disclosed,

   3.4. A brief statement of the purpose of the disclosure, and

   3.5. Any relevant documentation, such as a written request from a government or law enforcement agency.

4. **Summary information.** When the Plan has made multiple disclosures to a single person or organization for the same purpose, the accounting may include summary information rather than the detail of each such disclosure. However, the disclosures must have been for one of the following reasons, in order for summary information to be acceptable:

   4.1. Disclosures to the Secretary of the U. S. Department of Health and Human Services, to determine whether the Plan is complying with federal regulations regarding the privacy of PHI (i.e. 45 CFR Parts 160 and 164), or to investigate a complaint relative to these regulations.

   4.2. Disclosures in accordance with any of the following Plan policies:

   - DISCLOSURE OF PROTECTED HEALTH INFORMATION FOR PUBLIC HEALTH PURPOSES
   - DISCLOSURE OF PROTECTED HEALTH INFORMATION TO REPORT CHILD ABUSE, OR OTHER ABUSE, NEGLECT, OR DOMESTIC VIOLENCE
   - REPORTING PROTECTED HEALTH INFORMATION TO EMPLOYERS UNDER OSHA AND SIMILAR LAWS
   - DISCLOSURE OF PROTECTED HEALTH INFORMATION TO REGULATORS
   - SUBPOENAS, COURT ORDERS, DISCOVERY REQUESTS, OTHER LEGAL PROCESSES AND THE DISCLOSURE OF PROTECTED HEALTH INFORMATION
   - DISCLOSURE OF PROTECTED HEALTH INFORMATION FOR LAW ENFORCEMENT PURPOSES
   - USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION FOR PURPOSES OF RESEARCH (see also **Research**, below)
   - DISCLOSURE OF PROTECTED HEALTH INFORMATION WITHOUT AUTHORIZATION, TO AVERT A SERIOUS THREAT TO HEALTH OR SAFETY
   - DISCLOSURE OF PROTECTED HEALTH INFORMATION FOR CERTAIN GOVERNMENT FUNCTIONS (military, or protective services of the

president and others, but excluding national security or intelligent purposes, as noted under "exceptions," above.)

- DISCLOSURE OF PROTECTED HEALTH INFORMATION TO WORKERS' COMPENSATION PROGRAMS
- DISCLOSURES OF PROTECTED HEALTH INFORMATION BY WORKFORCE MEMBERS WHO ARE THE VICTIMS OF A CRIME
- EXTENSION OF PRIVACY PROTECTION TO DECEASED INDIVIDUALS

4.3. Summary information, to account for multiple disclosures to the same person or organization for the same reason, must contain the following information:

4.3.1. For the first disclosure made during the period of the accounting, all of the information required in #3, above.

4.3.2. The frequency, periodicity, or number of disclosures made during the accounting period.

4.3.3. The date of the last disclosure during the accounting period.

5. **Research.** The following applies if, during the period covered by the accounting, the Plan has made disclosures of protected health information for a particular research purpose in accordance with the USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION FOR PURPOSES OF RESEARCH policy, for 50 or more individuals.

5.1. An accounting for any of the individuals whose PHI may have been disclosed for the research purpose, may provide the following limited information:

5.1.1. The name of the protocol or other research activity;

5.1.2. A description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records;

5.1.3. A brief description of the type of protected health information that was disclosed;

5.1.4. The date or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period;

5.1.5. The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and

5.1.6. A statement that the protected health information of the individual may or may not have been disclosed for a particular protocol or other research activity.

5.2. If an individual receives an accounting that uses this research option, and if it is reasonably likely that the PHI of the individual was disclosed for the research protocol or activity, the Plan will assist the individual in contacting the entity that sponsored the research and the researcher, if so requested.

Time Frames

1. The Plan must provide the written accounting, or request an extension of time within 60 days of the date the request for the accounting was received.

2. One extension of 30 days is allowed. A request for extension must state the reasons for the delay and the date on which the accounting will be provided to the member.

Fees

1. The first accounting in any 12-month period will be provided without charge.

2. A reasonable, cost-based fee will be charged for any additional accounting requested during any 12-month period.

3. A member who will be subject to the fee for additional accountings will be informed of the fee, and will be given the chance to withdraw the request to avoid the fee, or to modify the request to reduce the fee.

Designation of Person Responsible for Receiving and Processing Requests for an Accounting of Disclosures

The Privacy Official is responsible for receiving and processing individual requests for an accounting for disclosures

PROCEDURE:

1. Any member who requests an accounting for disclosures of PHI will be referred to the Privacy Official.

2. The Privacy Official will assure compliance with the above policy to provide the accounting.

Information management

The TPA's Director of Claims and Enrollment, the TPA's member services department, along with the Plan's Employee Services department and Information Systems department, with the assistance of the Privacy Official, will develop mechanisms to record, for each accountable disclosure of protected health information, the information

that is required in the accounting. The information must be retained for at least six years, to support accounting for disclosures during a six-year period prior to the request for the accounting.

Processing of requests for accounting

The Privacy Official will:

1. Review the request to determine which disclosures are reportable.

2. Assemble the required information from records kept in accordance with the information management mechanisms developed by the TPA and the Plan's Employee Services department

3. Notify the member of the fee, if the request is a second or subsequent request in a 12-month period.

4. Prepare the written accounting.

5. Send or give the accounting to the member (payment is required in advance if a fee is due).

6. File a copy of the written accounting, and the written request. These documents must be retained on file for six years.

COMPLAINTS ABOUT PRIVACY PRACTICES

RESPONSIBILITY: Privacy Official, Employee Services, Director of Member Services

BACKGROUND:

Federal rules require the Health Benefits Plan for State and Local Employees (Plan) to have a means to receive complaints regarding its practices in using and disclosing protected health information. The rules do not specify how the Plan should respond to such complaints.

POLICY:

1. Complaints concerning the Plan's privacy practices will be directed to the Department of Human Resource Management, Office of Health Benefits. This will be noted in the Notice of Privacy Practices.

2. The Privacy Official, or his or her designee, will respond to complaints. When indicated by the nature of a complaint, the Privacy Official will investigate the situation, which gave rise to the complaint, and change privacy practices or initiate retraining when appropriate.

3. Complaints that indicate a possible violation of the Plan's policies or applicable law will be referred by the Privacy Official to the Director of Office of Health Benefits for possible action under the Plan policies regarding employee discipline. See also SANCTIONS FOR VIOLATING PRIVACY AND SECURITY POLICIES AND PROCEDURES.

4. Complaints regarding privacy practices, and responses to these complaints, will be kept on file by the Privacy Official for six years.

PROCEDURE:

Members who want to file complaints about the Plan's privacy practices, or about an alleged violation of the Plan's notice of privacy practices or state or federal law regarding the privacy of protected health information, will be referred to the Employee Services Department. All complaints must be in writing. The Employee Services Department will instruct the member as to the required form and content.

The complaint will be directed to the Privacy Official for action under this policy and under the other Plan's policies and procedures regarding the response to complaints. This includes taking action to mitigate any harm done as a result of the incident that gives rise to the complaint. See DUTY TO REPORT SECURITY OR PRIVACY BREACH AND MITIGATE THE EFFECT.

FREE EXERCISE OF PRIVACY RIGHTS

RESPONSIBILITY: Director of the Office of Health Benefits

BACKGROUND:

The Health Benefits Plan for State and Local Employees' (Plan) policies, and federal and state law, give members certain rights regarding the privacy of their protected health information. Federal regulations prohibit the Plan or Plan sponsor from taking any actions that would interfere with the free exercise of these rights.

POLICY:

The Plan or Plan sponsor shall not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against:

1. Any individual for the exercise by the individual of any right under, or for participation in, any process established by federal or state law or regulation, or the Plan's policies, including the filing of a complaint;
2. Any individual or other person for:
    - 2.1. Filing of a complaint with the Secretary of Health and Human Services in accordance with federal privacy regulations [45 CFR Part 160] or with the Plan's Notice of Privacy Practices, or any of its policies and procedures;
    - 2.2. Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under Part C – Administrative Simplification, of Title XI of the Social Security Act; or
    - 2.3. Opposing any act or practice made unlawful by federal privacy regulations promulgated under the authority of Part C, Title XI of the Social Security Act, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of protected health information in violation of those regulations.

No member of the workforce of the Plan or Plan sponsor shall require someone to waive the right to file a complaint with the Secretary of Health and Human Services, in accordance with federal privacy regulations [45 CFR Part 160], as a condition of the provision of treatment, payment, enrollment in a employee health benefit plan, eligibility for benefits.

SECTION TWO: GENERAL POLICIES REGARDING THE USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION

This section contains general polices regarding protected health information. These policies provide the foundation for maintaining member privacy.

GENERAL POLICY FOR AGENCIES AND LOCAL EMPLOYERS-- USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION

RESPONSIBILITY: Privacy Official

BACKGROUND:

Federal HIPAA privacy regulations do not require the Health Benefit Plan for State and Local Employees (Plan) to obtain an individual's written consent or authorization prior to using, disclosing, or requesting protected health information (PHI) for purposes of treatment, payment or health care operations. Nor do Federal privacy regulations require that providers of health care services obtain their patients' consent or authorization, before disclosing PHI to employee health benefits plans for payment purposes, or for certain operational activities of the employee health benefits plan, such as quality assurance.

State agencies and local employers do not have a right to PHI without a proper authorization. However Benefit Administrators (BAs) may continue to assist plan members with claim and eligibility problems as outline below (also see PROVIDING MEDICAL INFORMATION TO FAMILY, FRIENDS OR OTHERS DIRECTLY INVOLVED IN THE MEMBER'S CARE OR PAYMENT).

POLICY:
The Plan is committed to protect the privacy of members' health information, and to comply with applicable federal and state laws that protect the privacy and security of members' health information. This policy establishes the basic requirements for the use or disclosure of members' protected health information, consistent with this commitment.

A consent or authorization is not required where a member, personal representative, family member or close friend requests that a BA assist with a claim or eligibility problem.

Subject to

- The MINIMUM NECESSARY RULE,
- The Plan's NOTICE OF PRIVACY PRACTICES,
- The limitations imposed by the USE OR DISCLOSURE OF PSYCHOTHERAPY NOTES policy, and
- Any restrictions on the use or disclosure of PHI to which the Plan has agreed (see MEMBER REQUESTS TO RESTRICT THE USE OR DISCLOSURE OF PROTECTED HEALTH INFORMATION policy),

Except when providing such assistance, all other requests for PHI should be forwarded to the OHB Privacy Official.

PROCEDURE:

The Plan's Privacy Officer (or his or her designee) is required to:

1. Assure that all members of the Plan's workforce are thoroughly trained in the uses and disclosures of PHI that are permitted by this policy.
2. Assure that all members of the Plan's workforce are thoroughly trained in the provisions of other Plan policies that govern the use and disclosure of PHI.

AUTHORIZATION TO USE OR DISCLOSE PROTECTED HEALTH INFORMATION

RESPONSIBILITY: Privacy Official, State agency and local employer benefit administrators

BACKGROUND:

Federal and state laws, and the Health Benefits Plan for State and Local Employees (Plan) policy, permit the use and disclosure of protected health information (PHI) for certain purposes without obtaining the member's written authorization. For instance, an authorization is not required when a member requests that a Benefit Administrator (BA) assist him with a claim problem. PHI also may be disclosed without an authorization when required by law, or when permitted to assist law enforcement or other public purposes. These situations are addressed in other Plan policies.

In all other cases, request for PHI must be accompanied by a properly signed authorization and forwarded to the OHB Privacy Official.

POLICY:

1. A written authorization, signed by the member, or the member's personal representative, is required to permit the Health Benefits Plan for State and Local Employers (Plan) to use or disclose that member's protected health information (PHI) in any circumstance that is not:
    1.1. For treatment, payment, or health care operations (OHB staff only), or
    1.2. Where a member or personal representative, family member or close friend requests that a BA assist him with a claim problem.
2. THE (PLAN) will require individuals to submit signed authorizations to allow it to request certain protected health information as necessary for purposes of determining an individual's eligibility for benefits or enrollment, or for underwriting or risk rating determinations. In most instances, health care providers and other health plans will not be permitted to disclose the required PHI to the Plan without such an authorization from the individual.
    2.1. Such authorizations must:
        2.1.1. Authorize health care providers and other health plans to disclose the information to the Plan, and
        2.1.2. State the purpose for which the information is sought, and
        2.1.3. Authorize the Plan to use the information for the stated purpose.
3. In addition, authorization is specifically required:

3.1. For most uses and disclosures of psychotherapy notes. A provider may not disclose psychotherapy notes to the Plan unless either the Plan or the provider has obtained the member's written authorization for the disclosure. The Plan must obtain the member's authorization in order to use psychotherapy notes for any purpose.

4. The written authorization must be in the form prescribed by the Plan's policy STANDARDS FOR FORM AND CONTENT OF AUTHORIZATION FORMS. An authorization is invalid if:

   4.1. It does not comply in all respects with the Plan's STANDARDS FOR FORM AND CONTENT OF AUTHORIZATION FORMS, or

   4.2. One or more required elements is not completed or does not clearly express the member's desires, or

   4.3. It has been revoked by the member to whom the protected health information pertains, or by a personal representative authorized to act on the member's behalf, or

   4.4. It has expired, based on the expiration date or event, or

   4.5. Any material information contained in it is known by the Plan to be false.

5. Any use or disclosure under the terms of an authorization must be consistent with the provisions of that authorization.

6. Authorizations must be retained for at least six years after the date they cease to be in effect (due to expiration or revocation).

7. Members may revoke their authorizations at any time, except to the extent that the Plan has taken action in reliance of the authorization. The revocation must be in writing, and must be specific enough to permit identification of the original authorization that is being revoked.

   The Plan will not require an authorization as a precondition to payment, enrollment in the employee health benefit plan, or eligibility for benefits, except:

   7.1. If the information for which the authorization is sought is for purposes of determining an individual's eligibility for benefits or enrollment, the benefits or enrollment may be conditioned on receipt of the authorization; or

   7.2. If the information for which the authorization is sought is for underwriting or risk rating determinations, enrollment in the employee health benefit plan or eligibility for benefits may be conditioned on receipt of the authorization.

   7.3. The Plan will not condition payment, enrollment in the employee health benefit plan, or eligibility for benefits on the receipt of an authorization to use or disclose psychotherapy notes.

8. When the Plan requires a member to sign an authorization as a condition of receiving treatment, payment, enrollment in the employee health benefit plan, or

eligibility for benefits, the authorization may not be combined with any other authorization forms.

9. The MINIMUM NECESSARY RULE does not limit the amount of information that may be used or disclosed under the authority of an authorization.

10. When a conflict exists between two documents that authorize the use or disclosure of protected health information (PHI) pertaining to the same member, The Plan will honor the terms of the more recent document, based on the date of the signature. The later document will be interpreted as an amendment of the former document.

11. When an authorization to use or disclose PHI conflicts with a restriction on the use or disclosure of PHI to which the Plan has previously agreed, the Plan will honor the terms of the authorization.

12. When the Plan agrees to a restriction on the use or disclosure of PHI, the restriction will take precedence over any prior authorization to use or disclose the PHI to which the restriction applies.

13. When the member's intent is not clear, the Plan will attempt to resolve the conflict by communicating with the member, either in writing or orally. The Plan will honor the preferences expressed by the member in this communication.

14. If the communication is oral, it must be recorded in written form. Written records of such communication will be retained until the date superceded by a subsequent document or other instruction from the member, plus six years.

15. Communication with the member's personal representative is acceptable, instead of communicating with the member, in accordance with the Plan's policy regarding DISCLOSURE OF PROTECTED HEALTH INFORMATION TO PERSONAL REPRESENTATIVES.

PROCEDURE:

1. Requests for uses and disclosures of PHI without written authorization that have not previously been reviewed, will be directed to the Privacy Official. The Privacy Official will review such requests in accordance with applicable Plan policies, and respond in writing with a determination as to whether the requested use or disclosure is permitted under Plan policy, or federal and state law, or whether a written authorization from the member is required. The Privacy Official will retain a copy of this written determination for at least six years. If the Privacy Official determines

that an authorization is required prior to the requested use or disclosure, an authorization that complies with this policy must be obtained.

2. When a written authorization to use or disclose PHI is requested from a member, or is presented by or on behalf of a member, the authorization document will be sent to the OHB Privacy Official, for compliance with the Plan's policy regarding the content of authorization forms. See STANDARDS FOR FORM AND CONTENT OF AUTHORIZATION FORMS. This includes determining whether the correct form has been used and whether all required elements have been completed.

    2.1. In some instances, members will present forms designed by other organizations. These forms are acceptable, as long as all of the required information is present. If there is any question as to the validity of an authorization form, the member should be asked to use the Plan's authorization form instead.

If the authorization document does not comply, it is not valid and will be returned to the person from whom it was received, with a cover letter explaining the reason it was rejected, and inviting the member to submit the authorization in the form approved by the Plan. A copy of the Plan's authorization form will be included with the letter. A copy of the returned form and the cover letter will be filed and retained for at least six years

3. If the authorization document does comply, the requested information will be released in accordance with the provisions of the authorization form, using Plan's current policies regarding the copying and mailing of member records. The original authorization form will be retained for at least six years. A notation will be made on the authorization form to identify which information was disclosed, the date, the recipient, and the reason.

In the event of a conflict among authorizations, or between an authorization and a restriction, relating to the use or disclosure of protected health information, when there is reasonable doubt as to the member's true desires, the Privacy Official will:

1. Attempt to obtain a new, signed document that clarifies the individual's preference for disclosure of the information.

2. If it is not possible to obtain a signed document, the Privacy Official will discuss with the member his or her preference for disclosure of information.

3. If the preference is communicated orally, the Privacy Official will document the individual's preference and act in accordance with that preference.

4. The member's preferences regarding the conflict between documents will be forwarded to the Privacy Official, who will forward it for inclusion in other records maintained by the Plan pertaining to that member.

Revocation of authorization

Any member who wishes to revoke an authorization to use or disclose PHI will be directed to contact the Privacy Official. Such revocation must be in writing, and must be specific enough to permit identification of the original authorization that is being revoked. The Privacy Official will notify workforce members in possession of the revoked authorization that it has been revoked, and will determine the extent to which action has been taken in reliance upon the authorization. The Privacy Official, with the advice of the Office of the Attorney General, will prepare directions regarding how the member's PHI is to be handled following the revocation. This may include no further action on the initial authorization, or action to the extent that it is permitted because the Plan has already relied upon the authorization.

STANDARDS FOR FORM AND CONTENT OF AUTHORIZATION FORMS

RESPONSIBILITY: Privacy Official

BACKGROUND:

Federal and state laws, and the Health Benefits Plan for State and Local Employees (the Plan) policy, permit the use and disclosure of protected health information for certain purposes without obtaining the member's written authorization. For instance, an authorization is not required when PHI is used for treatment, for payment, or health care operations.

PHI also may be disclosed without an authorization when required by law, or when permitted to assist law enforcement or other public purposes. These situations are addressed in other Plan policies.

In all other cases, the member must sign an authorization form before the Plan may use or disclose the member's PHI. See the AUTHORIZATION TO USE OR DISCLOSE PROTECTED HEALTH INFORMATION policy. Federal regulations establish standards for the content of the authorization form.

This policy specifies the form and content of an authorization form in order for it to be valid.

POLICY:

1. An authorization to use or disclose protected health information (PHI) must contain the following core elements:

    1.1. A description of how the member may revoke the authorization

    1.2. A description of the information to be used or disclosed, that identifies the information in a specific and meaningful fashion. Examples: "laboratory results from July, 1998" or "all laboratory results" or "results of MRI performed in July, 1998" or "entire medical record." The description must be specific enough to indicate that the member has a clear understanding of how much information will be used or released.

    1.3. The name or other specific identification of the person or organization that is authorized to use or disclose the information. Examples: "Office of Health Benefits (OHB)" or "any health care provider."

    1.4. The name or other specific identification of the person or organization to which the Plan is authorized to make the disclosure. Examples: "ABC Life Insurance Co." or "John Smith, JD, attorney." If the authorization is intended to permit the Plan to use PHI internally, and does not authorize any disclosure of PHI to other parties, the correct entry is " The Health Benefits

Plan for State and Local Employees." An entry of "not applicable" or "NA" is not valid.

1.4.1. If the Plan is requesting the individual to sign an authorization in order to obtain PHI for use in eligibility, enrollment, underwriting, risk-rating, or other purposes for which an authorization is required, the form must BOTH authorize the disclosure of the PHI to the Plan, under paragraph 1.2, AND authorize the Plan's use of the information under paragraph 1.3.

1.5. A description of each purpose of the requested use or disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when a member initiates the authorization and does not, or elects not to, provide a statement of the purpose. If the information will be used for marketing, this must be stated on the authorization form. An expiration date, or an expiration event that relates to the member or to the reason for the use or disclosure. Examples: "December 31, 2002" or "one year from the date of this form" or "as long as enrolled in the employee health benefit plan authorized to receive the information." The statement "end of the research study," "none," or similar language is sufficient if the authorization is for a use or disclosure of protected health information for research, including for the creation and maintenance of a research database or research repository.

1.6. A statement that the member has the right to revoke the authorization in writing, and that the revocation does not apply:

1.6.1. To the extent that the Plan has taken action in reliance on the authorization; and

1.6.2. If the authorization is to permit disclosure of PHI to an insurance company, as a condition of obtaining coverage, to the extent that other law allows the insurer to contest claims or coverage.

1.7. A statement that the member does not have to sign the authorization as a condition of receiving treatment from the Plan, except:

1.7.1. If the treatment is research-related, provision of treatment may be conditioned on receipt of an authorization to use and disclose PHI related to this treatment as necessary for the research; or

1.7.2. If the purpose of the treatment services is to create PHI for disclosure to a third party, provision of the services may be conditioned on receipt of an authorization to disclose the PHI to that third party.

1.8. A statement that the individual does not have to sign the authorization as a precondition to payment, enrollment in the employee health benefit plan, or eligibility for benefits, except:

1.8.1. If the information for which the authorization is sought is for purposes of determining an individual's eligibility for benefits or

enrollment, the benefits or enrollment may be denied if the individual does not provide an authorization; or

1.8.2. If the information for which the authorization is sought is for underwriting or risk rating determinations, enrollment in the employee health benefit plan or eligibility for benefits may be denied if the individual does not provide an authorization.

1.8.3. The Plan will not condition payment, enrollment in the employee health benefit plan, or eligibility for benefits on the receipt of an authorization to use or disclose psychotherapy notes.

1.9. A statement that information that is disclosed in accordance with the authorization may be disclosed further by the recipient, and that the information may no longer be protected by federal privacy rules regarding protected health information.

1.10. If the authorization is for the use or disclosure of PHI for marketing, and the use or disclosure will involve direct or indirect remuneration to the Plan from a third party, the authorization must state that such remuneration is involved.

1.11. The member's signature, or the signature of the member's personal representative, with a description of the representative's authority to act for the member. Example: "power of attorney."

1.12. The date of the signature.

1.13. The form must be written in plain language

When the Plan requests a member or other individual to sign an authorization, the individual will be given a copy of the signed form.

2. The following additional standards apply to authorizations that are combined with other documents. An authorization that is combined with any other document except as listed below is not valid.

2.1. Authorizations may be combined with other authorizations in a single compound authorization, if none of the authorizations relates to the use or disclosure of psychiatric notes, and if none of the authorizations is required as a condition of receiving treatment, or other services from the Plan, or as a precondition to payment, enrollment, or eligibility for benefits.

2.2. Two or more authorizations that relate to the use and disclosure of psychiatric notes may be combined, but may not be combined with authorizations relating to any other type of PHI.

2.3. A research authorization may be combined with consent to participate in the research, with other authorizations to use or disclose PHI for the research, with other written permission for the same research study, and with the NOTICE OF PRIVACY PRACTICES, in a single document.

2.4. When the Plan requires a member to sign an authorization as a condition of receiving medical care, payment, enrollment in the employee health benefit

plan, or eligibility for benefits, the authorization may not be combined with any other authorization forms.

PROCEDURE:

1. The Privacy Official will create authorization forms that meet the standards of this policy, and will assure that an adequate supply of such forms is available at each location at which the Plan may request a member or other individual to complete an authorization.

File copies of authorization forms developed by the Plan will be kept for six years after the date a new form supercedes them.

2. File copies of authorization forms developed by the Plan will be kept for six years after the date a new form supercedes them.

3. Members of the Plan's workforce will only use authorization forms that have been approved by the Privacy Official when requesting a member's authorization for the use or disclosure of PHI.

4. The Privacy Official will assure that OHB have been trained to recognize valid and invalid authorizations

.

5. Any authorization form whose validity is in question will be forwarded to the Privacy Official for a final determination before any PHI is released or used in reliance on such form.

Health Benefits Plan for State and Local Employees
AUTHORIZATION
TO USE AND DISCLOSE
PROTECTED HEALTH INFORMATION

MEMBER

Name: _____

Date of Birth: _____ID Number: _____

DESCRIPTION OF INFORMATION TO BE USED OR DISCLOSED:

_____

_____

WHO IS AUTHORIZED TO USE OR DISCLOSE THE INFORMATION?

_____

_____

WHO IS AUTHORIZED TO RECEIVE THE INFORMATION?

_____

_____

REASON THE INFORMATION WILL BE USED OR DISCLOSED [if the member initiates the authorization, the statement "at the request of the individual" is sufficient]:

_____

_____

_____

EXPIRATION DATE OR EVENT:

_____

Notice to Member

You may revoke this authorization at any time. To revoke this authorization, send a written statement to the Office of Health Benefits, 12th Floor, Privacy Official, 101 N. Fourteenth St., Richmond VA 23219ADDRESS, CITY, STATE, ZIP. The statement must identify this authorization by referring to the date it was signed (below). The statement must include the date on which this authorization is no longer in force.

If you revoke this authorization, we may still use and disclose the information for the purposes listed above, if we have already taken action in reliance on this authorization. Also, if this authorization is to permit disclosure of information to an insurance company, in order for you to obtain insurance coverage, the insurance company may still have the legal right to use the information to contest a claim or to contest your coverage.

- You may refuse to sign this authorization. You do not need to sign this authorization to receive health care services.

You do not have to sign this authorization to receive payment, to enroll in Health Benefits Plan for State and Local Employees' health benefit plan, or to be eligible for benefits, except:

- If this authorization is sought is for the purpose of determining your eligibility for benefits or enrollment, then you must authorize the Plan to obtain the necessary information or the benefits or enrollment may be denied.
- Under Federal law, you do not have to authorize us to receive the private notes from counseling sessions, that are kept by a mental health professional, as a condition of payment, enrollment in a employee health benefit plan, or eligibility for Benefits person or organization that receives your information because of this authorization may have the legal right to disclose this information to other people or organizations without your knowledge or consent.

Signature: _____ Date: _____

If this authorization is signed by someone who is not the member listed at the top of this form, provide a description of the signer's authority to act for the member.

_____

The member will be provided with one copy of this form. [NOTE: This is optional if the member initiates the authorization.]

Form Auth 01- 04/15/03

Checklist to Validate Authorization Forms

An authorization to use or disclose protected health information (PHI) must contain the following elements:

- ❑ A description of the information to be used or disclosed, that identifies the information in a specific and meaningful fashion. Examples: "Plan claim payments for laboratory test from July, 1998" or "all laboratory results" or " denial of MRI performed in July, 1998". The description must be specific enough to indicate that the member has a clear understanding of how much information will be used or released.
- ❑ The name or other specific identification of who is authorized to use or disclose the information. Examples: Anthem or "any health care provider."
- ❑ The name or other specific identification of the person or organization to which the Plan is authorized to make the disclosure. Examples: John Doe, attorney at Law
- ❑ A description of each purpose of the requested use or disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when a member initiates the authorization and does not, or elects not to, provide a statement of the purpose.
- ❑ An expiration date, or an expiration event that relates to the member or to the reason for the use or disclosure. Examples: "December 31, 2002" or "one year from the date of this form" or "as long as enrolled in the employee health benefit plan authorized to receive the information."
- ❑ A statement that the member has the right to revoke the authorization in writing, and that the revocation does not apply:
- ❑ To the extent that the Plan has taken action in reliance on the authorization; and
- ❑ If the authorization is to permit disclosure of PHI to an insurance company, as a condition of obtaining coverage, to the extent that other law allows the insurer to contest claims or coverage.
- ❑ A description of how the member may revoke the authorization.
- ❑ A statement that the member does not have to sign the authorization as a condition of receiving treatment from a provider, except:
    - If the treatment is research-related, provision of treatment may be conditioned on receipt of an authorization to use and disclose PHI related to this treatment as necessary for the research; or
    - If the purpose of the treatment services is to create PHI for disclosure to a third party, provision of the services may be conditioned on receipt of an authorization to disclose the PHI to that third party.

- A statement that the individual does not have to sign the authorization as a precondition to payment, enrollment in the employee health benefit plan, or eligibility for benefits, except:
- If the information for which the authorization is sought is for purposes of determining an individual's eligibility for benefits or enrollment, the benefits or enrollment may be denied if the individual does not provide an authorization; or
- If the information for which the authorization is sought is for underwriting or risk rating determinations, enrollment in the employee health benefit plan or eligibility for benefits may be denied if the individual does not provide an authorization.
- The Plan will not condition payment, enrollment in the employee health benefit plan, or eligibility for benefits on the receipt of an authorization to use or disclose psychotherapy notes.
- A statement that information that is disclosed in accordance with the authorization may be disclosed further by the recipient, and that the information may no longer be protected by federal privacy rules regarding protected health information.
- The member's signature, or the signature of the member's personal representative, with a description of the representative's authority to act for the member. Example: "power of attorney."
- The date of the signature.
- The following additional standards apply to authorizations that are combined with other documents. An authorization that is combined with any other document except as listed below is not valid.
- Authorizations may be combined with other authorizations in a single compound authorization, if none of the authorizations relates to the use or disclosure of psychiatric notes, and if none of the authorizations is required as a precondition to payment, enrollment, or eligibility for benefits.
- Two or more authorizations that relate to the use and disclosure of psychiatric notes may be combined, but may not be combined with authorizations relating to any other type of PHI.

SECTION THREE: USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION WITHOUT MEMBER AUTHORIZATION

This section contains policies that address instances in which the organization may use protected health information (PHI), and disclose PHI to other people or organizations, without the written authorization of the person to whom the information pertains.

If a member of the workforce reads protected health information, then that is a "use" of information. If the member of the workforce gives the information to another member of the workforce, that is also considered a "use" of the information. If the member of the workforce gives the information to someone who is not part of the organization's workforce, that is a "disclosure."

Federal HIPAA privacy regulations contain an extensive list of situations in which PHI may be used or disclosed without authorization. Users should evaluate their own operations to determine which of these policies may not be applicable to them. In doing so, it is important to keep in mind that HIPAA's definition of treatment is quite broad. Employee health benefit plans may find that some of their activities, such as blood pressure or blood sugar screenings at health fairs, could be construed as treatment under HIPAA. To this extent, the use or disclosure of the PHI that employee health benefit plans obtain or create while conducting these activities may be governed by a provision of the HIPAA regulations that does not appear, at first, to apply to employee health benefit plans.

MINIMUM NECESSARY RULE

RESPONSIBILITY: Privacy Official, members of the Office of Health Benefits, agency and local employer benefit administrators

BACKGROUND:

Protected health information must be treated with the utmost confidentiality. Members of the Office of Health Benefits (OHB) as well as agency and local employer benefit administrators (BAs) are required to limit the amount of protected health information they use, request, or disclose to others, to the minimum amount necessary to achieve the specific purpose of that use, request, or disclosure.

This policy establishes the general rule regarding the minimum necessary limitation on the use or disclosure of protected health information.

POLICY:

1. BAs may not use, request, or disclose to others, any protected health information that is more than the minimum necessary to accomplish the purpose of the use, request, or disclosure.

2. Members of the workforce are required to comply with specific policies and procedures established to limit uses of, requests for, or disclosures of protected health information to the minimum amount necessary.

3. BAs may not use, disclose, or request an entire medical record except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure or request.

Exceptions:

1. When federal or state law requires a disclosure of protected health information, the minimum necessary amount of information is that which is required in order to comply with such law. Requests for PHI made by the federal government in the course of a complaint investigation or compliance review, undertaken under federal privacy rules, are deemed to meet the minimum necessary rule.

2. When disclosing a member's own information to that member, or to the member's personal representative, the minimum necessary rule does not apply.

DISCLOSURE VERIFICATION OF THE IDENTITY AND AUTHORITY OF A PERSON REQUESTING OF PROTECTED HEALTH INFORMATION

RESPONSIBILITY: All Members of The Health Benefits Plan for State and Local Employees' (Plan) Workforce Who Receive Requests for Protected Health Information

BACKGROUND:

There are a number of situations in which members of the Plan's workforce may be called on to disclose protected health information (PHI) in accordance with the Plan's policies. This includes disclosures to the member, disclosures to business associates, disclosures that are required by law, disclosures that are authorized by the member, and disclosures that are permitted by the Plan's policies without authorization.

Disclosures of protected health information must be made in accordance with the applicable Plan policy. In each case, the person who approves the disclosure needs to follow the requirements of this policy to determine that the person to whom the PHI is disclosed is authorized to receive it.

POLICY:

Members of the Plan's workforce who authorize the disclosure of PHI shall take reasonable steps to:

1. Verify the identity of the person to whom the PHI is disclosed, and

2. Verify the person's authority to receive the PHI.

Reasonable steps include the following, depending on the circumstance:

1. If the worker knows the identity and authority of the recipient of the PHI, no further documentation is necessary.

2. PHI may be disclosed to someone who is obviously involved in the member's care, or payment for care, without verifying the person's identity or relationship to the member. However, if possible, the member must be given the opportunity to agree or object to the disclosure. See the PROVIDING A MEMBER'S MEDICAL INFORMATION TO FAMILY, FRIENDS, OR OTHERS DIRECTLY INVOLVED IN THE MEMBER'S CARE policy.

3. PHI may be disclosed in accordance with the Plan's policies regarding disclosures to law enforcement officials, prison officials, or disaster relief agencies when the identity and authority of the recipient of the information may reasonably be inferred from the circumstances. All such request should be referred to the Plan's Privacy Official

PROVIDING MEDICAL INFORMATION TO FAMILY, FRIENDS, OR OTHERS DIRECTLY INVOLVED IN THE MEMBER'S CARE OR PAYMENT

RESPONSIBILITY: All members of the Health Benefits Plan for State and Local Employees (Plan) workforce, Privacy Official,

BACKGROUND:

Federal and state laws restrict the disclosure of protected health information (PHI). In most situations, the Plan may only disclose PHI to other providers of health care for purposes of treatment, to insurance companies and others involved in the payment for health care, to organizations with which the Plan has contracts for services that are integral to our operations, when permitted or required by law, or when the member authorizes the disclosure in writing.

However, it is permissible to disclose a limited amount of PHI to someone who is directly involved in a member's care, or payment for care, when necessary for the member's welfare. Typically, this involves responding to an inquiry or complaint from a relative on behalf of the member.

POLICY:

1. **Assistance with care or payment.** When a family member, personal representative, close friend, or other person is involved with a member's care, or with payment for care, members of the Plan's workforce may provide this person with a member's protected health information as follows:

    1.1 The information must be limited to the minimum necessary to permit the other person to provide appropriate assistance to the member, and must be directly relevant to the other person's involvement in the member's care or payment for care. See MINIMUM NECESSARY RULE.

    1.2 The information must be needed either to help the member with health care or with payment.

    1.3 The other person must clearly be involved in the member's care or payment for care. This may be someone who is known to be a family member or personal representative of the member, someone whom the member says is involved in his or her care, or someone whose involvement is obvious.

    1.4 Employer Benefit Administrators (BAs), family, friends, or others may be considered to be persons involved in the member's payment for care under this policy, if they present evidence that the member has asked them to make an inquiry on his or her behalf. For example, an employee, who is inquiring about the status of a spouse's claim, may be able to identify the claim by provider and date of service. This would be sufficient evidence that it was the spouse's intent for the employee to make the inquiry.

Explanation of Benefits (EOB). Protected health information that pertains to dependents may be included on an explanation of benefits that is sent to a subscriber. The contents of the EOB must be limited to the minimum necessary (see MINIMUM NECESSARY RULE). PHI of a dependent MAY NOT be included on an EOB if the dependent has requested that PHI be communicated to an alternate address and/or by alternate means to avoid endangering the dependent. See ALTERNATIVE COMMUNICATION OF HEALTH INFORMATION.

Notify family or friend. The Plan also may disclose protected health information to a family member, personal representative, or other person responsible for a member's care, as necessary to provide this person with notification of the member's location, general condition, or death.

Locate family or friend. The Plan also may disclose protected health information, as necessary, in order to locate or identify a family member, personal representative, or other person responsible for a member's care, in order to notify such person of the member's location, general condition, or death.

2. **Member present**. If the member is present, or otherwise available, the disclosures of PHI permitted by this policy may only be made in accordance with the member's desires. Generally, the worker should ask the member if he or she agrees to the disclosure, and should give the member the opportunity to object. However, the worker may also disclose PHI in accordance with this policy when, based on his or her professional judgment, it can be reasonably inferred from the circumstances that the member does not object to the disclosure.

3. **Member not present**. If the member is not present, or otherwise available, a worker may disclose PHI in accordance with this policy when it is in the member's best interest to do so. This determination may be made by the BA, based on his or her professional judgment and experience with the Plan's common practices in like situations. The same rule applies when the member is not capable of agreeing to or objecting to a disclosure of PHI permitted by this policy.

4. In all cases, the disclosure of PHI must be limited to information that is directly relevant to the other person's involvement in the member's care or payment for care.

5. The Plan workers may exercise their professional judgment in determining what PHI they disclose, and to whom, under this policy, based on their evaluation of the member's best interests.

PROCEDURE:

1. The Privacy Official will communicate this policy to all the Plan's workers.

2. When a worker, based on his or her professional judgment, determines that it would be in the best interest of a member to provide certain protected health information to a person involved in the member's care or payment for care, the worker should first ask the member if he or she agrees or objects. If the member objects, the worker may not disclose the PHI.

3. When circumstances demonstrate that the member does not object (such as when a family member accompanies a member to the Plan offices), the worker may make appropriate disclosures without first asking the member.

4. If the member is not available to agree or object, or is not able to participate in his or her health care due to incapacity, the worker may exercise professional judgment to act in the best interests of the member in disclosing protected health information to someone involved in the member's care.

5. The Privacy Official and the Plan's Business Associates will develop procedures for workers to identify personal representatives, family members and others involved in the member's care or payment for care, when the member is not present or otherwise not able to confirm identity. This includes people who visit the Plan's offices, people who call, and people who use internet services to access information. Procedures will be consistent with the Plan security policies used to authenticate the identity of users. For instance, a caller who identifies herself as a subscriber, and asks for information about a dependent's claim, may be asked to provide the contract number or other information from her identification card, and an address or telephone number. Requiring two pieces of information, one of which is not available from the ID card, provides better security than requesting a single piece of information.

6. The Privacy Official and the Plan's Business Associates will develop procedures to ensure that PHI pertaining to a dependent is omitted from EOBs when the dependent has requested that PHI be communicated to an alternative address and/or by alternative means to avoid a disclosure of PHI that could endanger the dependent. These procedures will be integrated with other procedures to comply with such a request. See ALTERNATIVE COMMUNICATION OF HEALTH INFORMATION.

DISCLOSURE OF PROTECTED HEALTH INFORMATION TO PERSONAL REPRESENTATIVES

RESPONSIBILITY: Privacy Official

BACKGROUND:

There are circumstances in which one person is legally authorized to act on behalf of another in making decisions related to health care. This includes parents and guardians of minor children, as well as other circumstances in which one person has the authority to make health care decisions on behalf of another. This authority extends to such personal representatives the right to examine and receive a copy of the individual's protected health information (PHI), to request an amendment of that PHI, to request an accounting for disclosures of PHI, and to authorize its disclosure to another.

POLICY:

In applying the Health Benefits Plan for State and Local Employees' (Plan) policies and procedures relating to the use or disclosure of protected health information, a personal representative will be treated the same as the individual to whom the PHI pertains. This includes the right to examine and receive a copy of the individual's protected health information (PHI), to request an amendment of that PHI, to request an accounting for disclosures of PHI, and to authorize its disclosure to another.

This policy gives personal representatives the same broad rights of access as apply to the member himself or herself. It is limited to persons who are legally authorized to act on behalf of the member. See PROVIDING MEDICAL INFORMATION TO FAMILY, FRIENDS, OR OTHERS DIRECTLY INVOLVED IN THE MEMBER'S CARE for other instances in which limited information may be disclosed to someone other than the member.

Exceptions:

1. When a request for PHI is from a parent, guardian, other person acting in loco parentis of an unemancipated minor, the following exceptions apply. For convenience, parents, guardians, other persons acting in loco parentis are referred to collectively as "parent," and the word is italicized to emphasize that this is intended to be read as a collective term that includes guardians and others acting in loco parentis).

    1.1. If the minor may lawfully receive a given health care service without the consent of a parent, (regardless of whether someone else has given consent or not) a parent of that minor will not be treated as a personal representative for purposes of PHI related to that health care service, unless the minor has requested that the parent be treated as a personal representative. This applies to the following situations:

1.1.1. State law allows a minor to consent to receive the service;

1.1.2. A minor consents to the service and state law does not require other consent; or

1.1.3. A court or other person authorized by law (other than a parent) consents to the service on the minor's behalf.

1.2. If the parent has agreed that PHI related to a given health care service will be kept confidential between the health care provider and the minor, that parent will not be treated as a personal representative for purposes of PHI related to that health care service.

1.3. The following apply to situations in which state law requires, permits, or prohibits disclosure of PHI to a parent:

1.3.1. If state law requires the disclosure of PHI to a parent, then PHI will be disclosed in accordance with such law even if the parent is not otherwise being treated as a personal representative under this policy.

1.3.2. If state law permits disclosure of PHI to a parent in situations in which the parent would not be treated as a personal representative under this policy, PHI will be disclosed when the health care professional who is responsible for the minor's care determines that the disclosure will not be detrimental to the minor.

1.3.3. If state law prohibits disclosure of PHI to a parent, even if the parent would be treated as a personal representative of a minor under this policy, no disclosure of PHI may be made if the disclosure would violate such state law.

1.4. If, in a given situation, state law does not specifically require, permit, or prohibit disclosure of PHI to a parent, the following apply:

1.4.1. If the parent would be treated as a personal representative of a minor under this policy, then exceptions of this policy do not apply;

If the parent would not be treated as a personal representative of a minor under this policy, then a licensed health care professional may provide a parent with access to certain PHI, or may deny such access. This decision is to be made in the exercise of professional judgment, consistent with state and other applicable law. This applies only to providing the parent with access to the information, and does not imply that the parent may receive a copy of the information, or otherwise exercise the rights of a personal representative.

2. When a request for PHI is from the executor, administrator, or other person who has authority to act on behalf of a deceased individual or of the individual's estate, only PHI that is necessary to allow the requestor to fulfill the responsibilities of

such personal representation (such as administration of the estate or the affairs of the decedent) may be disclosed.

3. Even when state law permits or requires disclosure of PHI to a personal representative, including the parent of a minor, the Health Benefits Plan for State and Local Employees will exercise professional judgment in the member's best interests, and refuse to treat a person as the personal representative of a member, if either of the following applies:

   1.1. There is a reasonable belief that the member has been or may be subjected to domestic violence, abuse, or neglect by such person; or

   1.2. There is a reasonable belief that treating the person as a personal representative (for instance, providing access to medical information) could endanger the member.

PROCEDURE:

1. Designated, trained members of the workforce will use the following criteria to identify a personal representative.

   1.1. A parent will be treated as the personal representative of an unemancipated minor unless one of the exceptions listed above applies. An adult will be recognized as the parent of an unemancipated minor child if:

      1.1.1. He or she identifies himself or herself as the parent, and the adult and child share the same address; or,

      1.1.2. If the child is identified on the employee's enrollment form, or other documentation as a dependent covered by that adult's health insurance; or,

      1.1.3. If the adult is known by the workforce member to be the child's parent or guardian; or,

      1.1.4. If the adult presents documentation of guardianship.

      [All others claiming to act as the personal representative of an individual must present written evidence of authority to act on behalf of the individual in making health care decisions. A copy of the written evidence of authority must be approved by the Privacy Official (or his or her designee) before the personal representative is to be granted access to the individual's PHI, or before a request to amend PHI, a request for an accounting of disclosures of PHI, an authorization to disclose PHI, or other request to act as a personal representative, will be honored. The Privacy Official will determine which information the personal representative may have access to, in accordance with this and other Plan policies and applicable federal and state laws.

2. The Privacy Official will assure that a sufficient number of workforce members have been trained in the provisions of this policy, and have been designated to determine whether persons who represent themselves as personal representatives may be treated as such under this policy.

3. The Privacy Official will annually review state law to determine:

    1.1. The circumstances in which a parent is not to be treated as a personal representative of an unemancipated minor in accordance with this policy; and,

    1.2. The circumstances in which disclosure of the minor's PHI to a parent is permitted, required, and prohibited under state law.

Based on this periodic review of state laws, the Privacy Official will prepare and maintain written guidelines to assist members of the workforce to determine when a parent is to be treated as a personal representative of an unemancipated minor, and when not, and when the minor's PHI must, may, or may not be disclosed to the parent. The guidelines will be reviewed and approved by the Office of the Attorney General before being distributed to members of the workforce.

4. Any member of the state's or local employer's workforce who has a reasonable belief that a person should not be treated as a personal representative due to one of the exceptions above must contact the Privacy Official before disclosing or providing access to an individual's PHI.

EXTENSION OF PRIVACY PROTECTION TO DECEASED INDIVIDUALS

RESPONSIBILITY: Privacy Official

BACKGROUND:

Federal and state laws require the Health Benefits Plan for State and Local Employees (Plan) to protect the confidentiality of members' protected health information (PHI). This protection continues after the member has died. This policy and procedure describe how the PHI of deceased members will be safeguarded, and how members of the Plan's workforce will respond to requests for disclosure of PHI pertaining to deceased individuals.

POLICY:

General rule. The security, privacy and confidentiality of protected health information (PHI) of former Plan members, who are now deceased, will be protected according to the same policies that apply to the PHI of all Plan members. This applies to all permitted and prohibited uses and disclosures of PHI.

Personal representatives. An executor, administrator, or other person who has authority to act on behalf of a deceased individual, or on behalf of the individual's estate, must be treated as the individual's personal representative. (See DISCLOSURE OF PROTECTED HEALTH INFORMATION TO PERSONAL REPRESENTATIVES policy.) However, this only applies to PHI needed by the personal representative in connection with the administration of the estate or other affairs of the decedent.

Exceptions. There are certain exceptions to this general policy that permit additional disclosures of the PHI of decedents. In the following instances, PHI that pertains to deceased individuals may be disclosed without authorization from the decedent's personal representative.

1. Disclosure to a law enforcement official. Notification of the individual's death will be made to a law official if there is reason to believe that the death may have resulted from criminal conduct.

2. Disclosure to coroner or medical examiner. PHI may be disclosed to a coroner or medical examiner for identification of the individual, determination of the cause of death, or as needed by the coroner or medical examiner to perform other duties as authorized by law.

Each of these disclosures may be considered "reportable" if an accounting of PHI disclosures is requested by the decedent's personal representative. See the ACCOUNTING OF DISCLOSURES OF PROTECTED HEALTH INFORMATION policy.

1. All regular and recurring disclosures of PHI of deceased individuals will be managed in the same way as all other regular and recurring disclosures of PHI.

2. All other requests for disclosure of PHI of deceased individuals, that is, requests that are not regular and recurring in nature, will be reviewed by the Privacy Official. Such disclosures will be made only in accordance with this and other applicable the Plan policies.

3. When a request for PHI is from the executor, administrator, or other person who has authority to act on behalf of a deceased individual or of the individual's estate, only PHI that is necessary to allow the requestor to fulfill the responsibilities of such personal representation (such as administration of the estate or the affairs of the decedent) may be disclosed.

SECTION FOUR: WORKFORCE POLICIES

The policies in this section relate to how members of the workforce are trained and disciplined to achieve compliance with the organization's privacy and security policies.

Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for the organization, is under the direct control of the organization, whether or not the organization pays them.

Generally, employees of a TPA that administers an employee health benefit plan will not be considered to be members of the workforce of the health benefit plan. Their use and disclosure of protected health information is governed by the terms of the Business Associate Contract between the TPA and the plan sponsor.

TRAINING PROGRAM: USES, DISCLOSURES, AND SAFEGUARDING PROTECTED HEALTH INFORMATION

.

RESPONSIBILITY: Privacy Official, Director of Human Resources,

BACKGROUND:

The Health Benefits Plan for State and Local Employees (Plan) has instituted a number of policies, procedures and practices intended to improve the privacy of protected health information (PHI), in accordance with federal and state law and regulations.

Employee training is necessary to achieve compliance with these policies, procedures, and practices, and with the related laws and regulations.

POLICY:

All members of the Plan's workforce, including temporary staff, students, and volunteers, will receive training in the policies and procedures that apply to their jobs, including maintenance of the privacy and security of protected health information.

New members of the workforce will receive training as part of orientation to their jobs, and to the Plan, within a reasonable time of joining the workforce.

All members of the workforce will receive additional training as policies and procedures are changed, to the extent that the changes affect their jobs.

Attendance at training sessions will be documented to demonstrate that each member of the workforce has received training in accordance with this policy. The documentation must be retained for six years.

Business associates will also receive privacy and security training as appropriate to their level of access to protected health information.

Content of Training

Training sessions will include the following:

1. Awareness training: threats to the privacy and security of protected health information, how failure to protect against these threats can harm members, and the importance of each employee of the workforce in the privacy and security posture of the Plan.

2. Details of applicable policies and procedures: how privacy and security policies affect the job of each member of the workforce, and how they define what is expected of each of these workers.

3. Periodic reminders.

4. Timely information about changes in policies and procedures.

5. Information about sanctions: how members of the workforce may be sanctioned under the employer's policy, and under state and federal law, for breaches of privacy and security policies.

6. Testing: to measure comprehension and retention of the material.

PROCEDURE:

1. The Privacy Official, and the Associate Director of Policy and Instruction, Office of Health Benefits will develop and maintain a privacy and security-training program for members of the workforce.

The program will include members of the workforce at all Plan offices, and will include business associates, as necessary and appropriate to their duties and access to PHI.

2. The training program will include procedures to document the training given each workforce member in that member's personnel record. Documentation of business associate training will be filed with the business associate's contract.

3. The program will include follow-up procedures to assure that all members of the workforce have been included in training.

4. The Privacy Official will notify the Associate Director of Policy and Instruction, Office of Health Benefits whenever a material change in policies and procedures occurs, and they will develop new training materials that incorporate the change.

5. All affected members of the workforce will be trained in material changes to policies and procedures related to privacy and security of PHI prior to the effective date of the change. If this is not possible, the training will take place within a reasonable period of time after the change takes effect. Training in changed policies and procedures will be documented.

The Privacy Official will retain all training materials for six years after the date they are superceded by revised materials.

6. The Privacy Official will retain documentation of training for each member of the workforce who receives training in accordance with this policy, for six years.

SANCTIONS FOR VIOLATING PRIVACY AND SECURITY POLICIES AND PROCEDURES

RESPONSIBILITY: Privacy Official, Director of Compensation

BACKGROUND:

Federal HIPAA privacy regulations require covered entities to establish and apply sanctions against members of the workforce who violate the entity's privacy policies, and applicable state and federal law that relates to the privacy of protected health information.

POLICY:

1. Members of the State Health Benefits Plan for State and Local Employees' (Plan) workforce are subject to disciplinary action for violation of policies and procedures. Violations that jeopardize the privacy or security of protected health information are particularly serious. This seriousness will be reflected in the nature of the disciplinary action, up to and including termination of employment.

2. All members of the workforce will be treated fairly and equitably in the imposition of sanctions for privacy and security violations.

3. Sanctions will be integrated into the Plan's overall employee discipline policy. This policy will be in writing.

4. Sanctions applicable to business associates will be incorporated into business associate contracts.

5. Disciplinary actions due to breaches of privacy or security of PHI will be documented, and the documentation must be retained for six years. Disclosure of PHI in violation of policy is reportable under the ACCOUNTING OF DISCLOSURES OF PROTECTED HEALTH INFORMATION policy.

6. No member of the workforce, and no business associate, will be subject to sanctions for a disclosure of PHI made in good faith in accordance with the following policies:

   6.1. DISCLOSURE OF PROTECTED HEALTH INFORMATION BY "WHISTLEBLOWERS"

   6.2. DISCLOSURES OF PROTECTED HEALTH INFORMATION BY WORKFORCE MEMBERS WHO ARE THE VICTIMS OF A CRIME

PROCEDURE:

The Privacy Official, and Director of Compensation will periodically review the Plan's discipline policies to assure that breaches of security and privacy of PHI are dealt with adequately and fairly.

The Director of Human Resources will document disciplinary actions, and will retain the documentation for at least six years.

DISCLOSURE OF PROTECTED HEALTH INFORMATION BY "WHISTLEBLOWERS"

RESPONSIBILITY: General Counsel

BACKGROUND:

Federal law recognizes that employees or others associated with health care organizations may feel compelled by professional standards or personal ethics to come forward when they believe, in good faith, that the organization is in violation of law, professional standards, safety standards, or ethics. They may believe that they need to disclose certain protected health information to substantiate their allegations. If they make the disclosure in good faith, and if the disclosure is made to an appropriate party, as set forth in this policy, this disclosure will not be treated as a breach of the State Health Benefits Plan for State and Local Employees' (Plan) security, privacy and confidentiality policies.

POLICY:

1. A member of the workforce or business associate of the Plan is not in violation of the requirements of the Plan's policies regarding uses and disclosures of protected health information:

   1.1. When the workforce member or business associate believes, in good faith, that the Plan has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the Plan potentially endanger one or more members, workers, or the public; and,

   1.2. When protected health information is disclosed to a health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the Plan, or to an appropriate health care accreditation organization, for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the Plan.

2. The protected health information may also be disclosed by the workforce member or business associate to an attorney who is retained for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct described above.

PROCEDURE:

Any disclosure of protected health information that is made by a member of the workforce under this policy must also follow the provisions of other applicable policies and programs of the Plan regarding compliance with federal and state laws, or reporting suspected fraud and abuse.

A disclosure made under this policy must be recorded for inclusion in any accounting of disclosures, to the extent that the Plan is aware of the disclosure.

DISCLOSURES OF PROTECTED HEALTH INFORMATION BY WORKFORCE MEMBERS WHO ARE THE VICTIMS OF CRIME

BACKGROUND:

This policy is self-explanatory, and requires no responsible party or procedures.

POLICY:

A State Health Benefits Plan for State and Local Employees (Plan) workforce member who is the victim of a criminal act may disclose protected health information to a law enforcement official without violating the Plan's policies regarding the use and disclosure of PHI, provided that:

1. The protected health information that is disclosed pertains to the suspected perpetrator of the criminal act; and

2. The protected health information that is disclosed is limited to the following information:
   - 2.1. Name and address;
   - 2.2. Date and place of birth;
   - 2.3. Social security number;
   - 2.4. ABO blood type and rh factor;
   - 2.5. Type of injury;
   - 2.6. Date and time of treatment;
   - 2.7. Date and time of death, if applicable; and
   - 2.8. A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

3. Other than the information listed in number 2, above, no protected health information related to the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue may be disclosed.

A disclosure made under this policy must be recorded for inclusion in any accounting of disclosures, to the extent that the Plan is aware

SECTION FIVE: ORGANIZATIONAL MATTERS

This section contains a number of administrative policies that deal with various aspects of the federal HIPAA privacy regulations, and how an organization complies with them.

DESIGNATION OF RECORD SETS

RESPONSIBILITY: Privacy Official

BACKGROUND:

The Health Benefits Plan for State and Local Employees' (the Plan) policies, in compliance with federal and state privacy regulations, permit members to have access to their protected health information (PHI), to receive copies of it, and to request that certain information be amended. However, this applies only to information that is stored in designated record sets. Designated record sets are records that contain PHI and that are used to make decisions about individual members. This policy designates the record sets.

POLICY:

The following are the Plan's designated record sets:

1. Operations records
    - 1.1. Claims
    - 1.2. Adjudication records
    - 1.3. Claim payment records
    - 1.4. Grievances and appeals relating to claim payment, eligibility for benefits, or enrollment decisions about individual members
    - 1.5. Enrollment and eligibility forms and records
    - 1.6. Underwriting and risk-rating records that are used to set premiums or co-insurance payments for individuals
    - 1.7. Records maintained by collection agencies acting as business associates on behalf of the Plan, pertaining to collection of accounts from individual members
    - 1.8. Customer service records
2. Medical management records
    - 2.1. Utilization management records
    - 2.2. Care coordination records
    - 2.3. Case management records
    - 2.4. Disease management records

Designation of Additional Record Sets:

The Privacy Official shall designate additional record sets, based on the following criteria:

1. The record set contains protected health information of individual members

2. The record set is used to make decisions about the members whose PHI it contains.

Record retention

This record set designation will be retained by the Privacy Official for as long as it is in force, and for at least six years after it has been superceded.

Federal HIPAA privacy regulations require covered entities to provide access to PHI in designated record sets, and to respond to requests to amend information in designated record sets. Also, users should note that the requirement to account for disclosures of PHI is not limited to disclosures of PHI stored in designated record sets.

DESIGNATION OF PRIVACY OFFICIAL AND CONTACT FOR COMPLAINTS AND REQUESTS RELATED TO PRIVACY

BACKGROUND:

Federal HIPAA privacy regulations require the official designation of the people or offices responsible for the functions listed in this policy.

POLICY:

Privacy Official

The Health Benefits Plan for State and Local Employees' (Plan) Privacy Official will be designated by the Director of the Office of Health Benefits (OHB) for purposes of the Plan's policies and procedures and federal privacy regulations [45 CFR § 164.530(a)(1)].

Contact office for complaints

The Employee Services Department of OHB is designated as the contact office to receive complaints regarding the privacy of protected health information.

Contact office to receive requests for access to PHI, to amend PHI, or for an accounting of disclosures of PHI

The Employee Services Department of OHB is designated as the contact office to receive requests for access to PHI, to amend PHI, or for an accounting for disclosures of PHI.

Contact office to provide additional information about matters covered in the NOTICE OF PRIVACY PRACTICES

The Employee Services Department of OHB is designated as the contact office to receive requests for additional information about matters covered in the NOTICE OF PRIVACY PRACTICES.

Retention period

This record of designations will be retained for as long as the designations are in effect, and for a period of six years after it is superceded by a subsequent designation.

DUTY TO REPORT SECURITY OR PRIVACY BREACH AND MITIGATE THE EFFECT

RESPONSIBILITY: Privacy Officials; Office of Health Benefits, Plan's Third Party Administrators

BACKGROUND:

A breach of the Health Benefits Plan for State and Local Employees' (Plan) privacy or security policies may result in harm to the person who is the victim of the breach. It may also erode trust in an organization, and impair its ability to provide medical care. It is important to respond quickly to any alleged breach, to determine what occurred, to prevent a recurrence of any violation of policy or law, and to take steps to mitigate any harm.

POLICY:

It is the duty of all members of the workforce to report any breach of the Plan's privacy and security policies. The Plan will promptly investigate any alleged breach of the privacy or security of protected health information (PHI). The Plan will attempt to mitigate, to the extent practicable, any harmful effect resulting from a use or disclosure of protected health information in violation of its policies and procedures, or resulting from the theft or unauthorized alteration of PHI. When warranted, the Plan will change policies and procedures, and provide appropriate training, to reduce the likelihood of a recurrence of any breach.

PROCEDURE:

1. Members of the workforce will report any breach of the Plan's privacy and security policies at once to their immediate supervisors.

2. Supervisors who receive reports of a breach of privacy or security are required to act to stop the breach as soon as possible. This may include immediate suspension of access privileges to PHI of anyone suspected of breaching privacy or security policies.

3. Supervisors will report a breach of privacy or security, and any actions they have taken, to the Privacy Official.

4. Supervisors will apply the Plan's SANCTIONS FOR VIOLATING PRIVACY AND SECURITY POLICIES AND PROCEDURES policy as appropriate.

5. Any allegation of harm that is a result of a breach of security or privacy of protected health information will be referred immediately to the Office of the Attorney General.

6. The Privacy Official will investigate the breach to develop a plan to mitigate the harm, to the extent that this is practicable.

7. The Office of the Attorney General will decide whether it is necessary to notify the victim of the breach in order to mitigate effectively the alleged harm.

8. The Privacy Official will prepare changes to policies and procedures, and/or provide necessary training, to reduce the likelihood of a similar breach in the future.

The allegation, the mitigation plan, mitigation actions taken, results, record of disciplinary actions (if any), and supporting information will be documented by the Privacy Official, and the documentation will be retained for at least six years.

MAINTENANCE OF PRIVACY AND SECURITY POLICIES

RESPONSIBILITY: Privacy Official,

POLICY:

1. It is the policy of the Health Benefits Plan for State and Local Employee (Plan) to implement policies and procedures designed to comply with applicable federal and state laws that relate to the privacy of protected health information.

2. Policies and procedures will be changed whenever necessary to comply with changes in applicable laws.

3. The Plan will include in its NOTICE OF PRIVACY PRACTICES a statement that it reserves the right to change the terms of its notice and to make the new notice provisions effective for all protected health information that it maintains. Accordingly, all changes to privacy policies, procedures and practices will apply equally to PHI created or obtained prior to and subsequent to the effective date of the change.

4. All policies and procedures that relate to the privacy or security of protected health information must be retained for six years from the date when they are no longer in force.

5. No policy or procedure that relates to the privacy or security of protected health information may take effect until it has been documented, in paper or electronic form, approved, and reflected in the NOTICE OF PRIVACY PRACTICES (to the extent that the change has a material effect on that notice).

PROCEDURE:

1. The Privacy Official will review annually, changes in federal and state laws that relate to the privacy, security and confidentiality of protected health information, and members' rights of access to that information, and make conforming changes to the Plan's policies and procedures. They are responsible for processing the changes to obtain necessary approval of the amended policies and procedures.

2. The Privacy Official will ensure that any such changes, if they are material, are reflected in a new NOTICE OF PRIVACY PRACTICES.

3. The Privacy Official will assure that the changes are reflected in training materials.

4. The Privacy Official will periodically monitor compliance with the Plan's policies and procedures, and implement corrective steps as necessary to maintain compliance.

5. The Privacy Official will assure that policy and procedure documents that relate to the privacy of protected health information are retained in accordance with this policy.

DOCUMENT RETENTION PERIOD: DOCUMENTS RELATING TO THE PRIVACY OF PROTECTED HEALTH INFORMATION

RESPONSIBILITY: Privacy Official

POLICY:

1. The Privacy Official is responsible to develop and maintain systems to retain documentation that relates to compliance with federal privacy regulations.

2. Federal privacy regulations require that the following documents be retained for as long as they are in effect, plus six years:

   2.1. Designation of the components of a single affiliated covered entity.

   2.2. Signed authorizations, and documents that terminate authorizations.

   2.3. Copies of the Plan notices of privacy practices.

   2.4. Acknowledgements signed by members upon receipt of the notice of privacy practices.

   2.5. Documentation of any agreement to restrict the use or disclosure of protected health information, and documentation of any modification or cancellation of the restriction by either the member or by the Plan.

   2.6. Documentation of designation of record sets.

   2.7. Documentation of the designation of titles of persons or offices to receive and process requests for access to protected health information in designated record sets.

   2.8. Documentation of the designation of titles of persons or offices to receive and process requests to amend protected health information in designated record sets. The information that is required for an accounting of disclosures, for each accountable disclosure.

   2.9. Copies of written accountings of disclosures prepared at members' request.

   2.10. Documentation of the designation of titles of persons or offices to receive and process requests for an accounting of disclosures.

   2.11. Written requests for access to protected health information, and responses to these requests, including correspondence relating to any appeal of a denial of access.

   2.12. Written requests to amend protected health information, responses to these requests, and documentation of statements of disagreement and rebuttals.

   2.13. Written requests for accountings of disclosures.

   2.14. Policies and procedures adopted or modified to comply with federal HIPAA privacy regulations.

2.15. Documentation of training in the Plan's privacy policies.

2.16. Documentation of designation of the privacy official.

2.17. Documentation of designation of the person or office to receive complaints and to provide information about privacy practices and members' privacy rights.

2.18. Documentation of complaints regarding privacy practices, and the disposition of these complaints.

2.19. Records of sanctions applied to members of the workforce who violate the Plan's privacy policies.

2.20. Fundraising communications, demonstrating the inclusion of instructions for opting out of receiving future such communications.

2.21. Plan documents, in respect to a group health plan established by the Plan.

2.22. Business associate contracts.

2.23. All documentation related to approved waivers and alterations of authorizations, for PHI that is used or disclosed in connection with a research study.

2.24. Any other action, activity, designation or communication which must be documented under federal HIPAA privacy regulations.

3. Other records that demonstrate the Plan's compliance with these HIPAA regulations will also be retained for at least six years past the date when the document is no longer in effect, as stated in the Plan policies.

PROCEDURE:

1. The Privacy Official will develop a list of all of the types of documentation which must be retained under this policy, and where the documentation will be retained.

2. The list will define when the six-year retention period begins for each item. (For instance, for a request to amend PHI, the six years begin when the request has reached its final disposition. For a policy, the six years begin when the policy is superceded by a revision.)

3. The Privacy Official will assure that the six-year retention requirement is met for these documents, regardless of where they are stored.

SECTION SIX: SAFEGUARDS

The policies in this section relate to an organization's physical, administrative, and technical safeguards to secure protected health information.

These policies are intended to address the requirement in the HIPAA privacy regulations to provide such safeguards. These policies will not be sufficient, by themselves, to comply with the anticipated federal HIPAA security regulations

GENERAL GUIDELINES TO SAFEGUARD PROTECTED HEALTH INFORMATION

RESPONSIBILITY: Privacy Official, all members of the Health Benefits Plan for State and Local Employees workforce

BACKGROUND:

Most members of the Health Benefits Plan for State and Local Employees' (Plan) workforce use protected health information every day in the completion of their duties. This policy establishes guidelines to help safeguard this information from being seen by those who are not authorized to see it.

POLICY:

The Plan will reasonably safeguard protected health information to limit incidental uses or disclosures. An incidental use or disclosure is a secondary use disclosure that cannot reasonably be prevented, is limited in nature, and that occurs as a by-product of an otherwise permitted use or disclosure. For example: a conversation that is overheard despite attempts by the speakers to avoid being heard.

All members of the Plan workforce will follow these guidelines in handling protected health information (PHI) to limit incidental uses and disclosures.

GUIDELINES TO SAFEGUARD PROTECTED HEALTH INFORMATION

Bulletin boards:

- Bulletin boards may not contain any documents with PHI of members, unless the member has authorized the display in accordance with the AUTHORIZATION TO USE OR DISCLOSE PROTECTED HEALTH INFORMATION policy. This includes:
  - Baby pictures (even without a name or other identifying information)
  - Cards and notes of appreciation

Cleaning personnel:

- Cleaning personnel do not need PHI to accomplish their work. Whenever reasonably possible, PHI will be placed in locked containers, cabinets, or rooms before cleaning personnel enter an area.
- When it is not reasonably possible to lock up PHI, it must be removed from sight before cleaning personnel enter an area, and a supervisor must be present.
- Cleaning personnel, whether members of the workforce or contractors, will receive training in the Plan's privacy and security policies, and in the penalties for violating these policies, before they are permitted in areas where PHI is stored or used.

Computer Screens:

- Computer screens at each workstation must be positioned so that only authorized users at that workstation can read the display. When screens cannot be relocated, filters, hoods, or other devices may be employed.
- Computer displays will be configured to go blank, or to display a screen saver, when left unattended for more than a brief period of time. The period of time will be determined by the Privacy Official. Wherever practicable, reverting from the screen saver to the display of data will require a password.
- Computer screens left unattended for longer periods of time must be locked and require a password for re-entry.

Conversations:

- Conversations concerning members' claims or other PHI must be conducted in a way that reduces the likelihood of being overheard by others.
- Wherever reasonably possible, barriers will be used to reduce the opportunity for conversations to be overheard.

Copying claims and other PHI

- When PHI is copied, only the information that is necessary to accomplish the purpose for which the copy is being made, may be copied. This may require that part of a page be masked.

Desks and countertops

- Claims and other documents that contain PHI must be placed face down on counters, desks, and other places where others can see them.
- Documents containing PHI will not be left on desks and countertops after business hours. Supervisors will take reasonable steps to provide all work areas where PHI is used in paper form with lockable storage bins, lockable desk drawers, or other means to secure PHI during periods when the area is left unattended.
- In areas where locked storage after hours cannot reasonably be accomplished, PHI must be kept out of sight. A supervisor must be present whenever someone who is not authorized to have access to that data is in the area.

Disposal of paper with PHI:

- Paper documents containing PHI must be shredded when no longer needed. If retained for a commercial shredder, they must be kept in a locked bin.

Home office

- Any member of the workforce who is authorized to work from a home office must assure that the home office complies with all applicable policies and procedures regarding the security and privacy of PHI, including these guidelines.

Information carried from one building to another:

- When a member of the workforce is transporting PHI from one building to another, it may not be left unattended unless it is in a locked vehicle, in an opaque, locked container. Locking the vehicle alone is not sufficient.

Key policy

- Keys must be surrendered upon termination of employment.
- The Privacy Official will act to change locks whenever there is evidence that a key is no longer under the control of an authorized member of the workforce, and its loss presents a security threat that justifies the expense.

Personal digital assistants (PDAs)

- The Plan privacy and security policies apply to any PHI that is stored on a PDA.
- Users of PDAs are responsible for assuring that the PHI on their devices is kept secure and private.
- Any loss or theft of a PDA thought to contain PHI must be reported to the Security Official immediately.
- Users of PDAs who store PHI on their devices will receive special training in the risks of this practice, and measures that they can take to reduce the risks (such as use of passwords).

Printers and Fax Machines:

- Printers and fax machines must be located in secure areas, where only authorized members of the workforce can have access to documents being printed. (See FACSIMILE MACHINES AND PROTECTED HEALTH INFORMATION.)

Record Storage:

- Areas where claim records and other documents that contain PHI are stored must be secure.
    - Wherever reasonably possible, the PHI will be stored in locking cabinets.

Where locking cabinets are not available, the storage area must be locked when no member of the workforce is present to observe who enters and leaves, and no unauthorized personnel may be left alone in such areas without supervision.

TERMINATION OR MODIFICATION OF ACCESS TO PROTECTED HEALTH INFORMATION: ELECTRONIC SYSTEMS

RESPONSIBILITY: Director of Information Systems, Agency and Local Employer Human Resources Directors

BACKGROUND:

When an employee ends his/her employment, or when an internal or external information systems user's access to certain types of data is withdrawn, appropriate security measures must be taken to minimize the possibility of unauthorized access to secure data by those who are no longer authorized to have access to that information. This may include business associates, such as systems maintenance contractors, as well as employees and other members of the workforce. Examples of procedures that may be appropriate upon the termination of access privileges include:

- Changing locks
- Removal from access lists
- Removal of user account(s)
- Turning in keys, tokens, or cards that allow access

POLICY:

The Health Benefits Plan for State and Local Employees (Plan) will terminate access to information systems and other sources of protected health information (PHI), including access to rooms or buildings where PHI is located, when a Plan employee, agent or contractor ends his/her employment or engagement. The Plan will terminate access to specific types of PHI when the status of any business associate or member of the workforce no longer requires access to those types of information.

1.1. Retrieving Keys, Tokens, or Cards that Allow Access: Human Resources department must assure that all materials allowing access to the Plan properties, buildings, or equipment are retrieved from a terminated employee, agent, or contractor, prior to his/her final exiting of the premises. Similarly, keys, tokens and cards that allow access to types of information that an individual is no longer authorized to use must be retrieved when the change in access status becomes effective.

1.2. Changing Locks: The Director of the Office of Health Benefits will determine if the combinations on any locks used to secure an area should be changed when a person knowledgeable of the existing combinations is no longer authorized to have access to the area.

1.3. Removal from or Modification to Access Lists: The Director of the Office of Health Benefits will coordinate with the Director of Information Systems to assure the removal of a member of the workforce or business associate from lists of those with authorized access to applicable types of information as required by termination or modification of access.

1.4. Removal or Modification of User Accounts: The Director of the Office of Health Benefits will coordinate with the Director of Information Systems to assure the deletion of an individual's access privileges to the information, systems, services, e-mail and resources for which they either no longer require authorization.

POLICIES AND GUIDELINES ON WORK STATION USE AND LOCATION

RESPONSIBILITY: Information Systems, Privacy Official, and all Associate Directors

BACKGROUND:

Members of the State Health Benefits Plan for State and Local Employees' (Plan) workforce must have ready access to the computerized information sources for which they have access authorization, in order to carry out the requirements of their jobs. With this in mind, workstations containing a computer terminal need to be designed and constructed for efficient operations, yet they must be shielded from public scrutiny or possible unauthorized access. All computer terminals with access to sensitive information need to have their screens shielded or turned from public viewing.

POLICY:

The Plan will provide secure workstations containing computer terminals with physical safeguards to minimize the possibility of unauthorized observation or access to protected health information (PHI). Areas where sensitive information is regularly entered or utilized will be secured using barriers to prevent public viewing of PHI during normal working hours. Wherever feasible, based on an analysis of risks and cost, these areas will be locked when not in use. Printers and fax machines will be located in the most secure areas available, and will not be located in or near areas frequented by members or the public.

PROCEDURE:

1. Supervisory and management personnel will periodically review the location and placement of all computer displays, printers, and facsimile machines in their areas of responsibility, and make changes as necessary to assure compliance with the requirements of this policy. Any such changes will be documented.
2. Any risk and cost analysis undertaken to determine whether physical changes are needed to improve security, such as the construction of walls, relocation of equipment and wiring, or installation of locking doors, will be documented.
3. Documentation produced in compliance with procedures above will be retained for six years.

FACSIMILE MACHINES AND PROTECTED HEALTH INFORMATION

RESPONSIBILITY: Privacy Official, Senior administrative person at each location where a fax machine is located

BACKGROUND:

Facsimile ("fax") machines are a convenient way to transmit small amounts of data from one location to another. However, the use of fax machines to transmit protected health information raises concerns regarding the confidentiality of that information. For instance, a dialing error may direct the information to the wrong fax machine. Or a fax that is received by a machine located in an unsecured area may be read by someone who does not need to know the information. Both of these situations would be a breach of the Health Benefits Plan for State and Local Employees' (Plan) policy.

POLICY:

1. Protected health information (PHI) may be transmitted by facsimile machine ("fax"), provided all other Plan policies and procedures regarding the disclosure of PHI are observed.

2. In order to reduce the potential for misdirected faxes, frequently used destination numbers will be pre-programmed into fax machines and tested before being used to transmit PHI.

3. To further reduce the possibility of misdirected faxes, each fax machine will display a key that identifies the destination for each pre-programmed fax number.

4. When PHI is faxed to a destination number that is not pre-programmed, the fax machine operator will double check the accuracy of the number in the machine's display before sending the fax.

5. All fax messages will include a cover sheet with the following statement:
   "Confidentiality Statement: The documents accompanying this transmission may contain confidential health information that is legally privileged. This information is intended only for the use of the individuals or entities listed above. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or action taken in reliance on the contents of these documents is strictly prohibited. If you have received this information in error, please notify the sender immediately and arrange for the return or destruction of these documents."

6. Fax machines that are used to transmit or receive PHI shall be placed in secure locations. Whenever possible, fax machines used to receive PHI will not be used regularly for other purposes.

7. Transmittal sheets will be checked immediately after each transmission of PHI, to assure that the information was sent to the correct number. If an error is detected, the sender must immediately act to correct the error, and report the error to the Plan's Privacy Official.

8. Transmittal sheets will be filed with the PHI that was transmitted, to document the recipient.

9. Use of fax machines with carbon roles will be discontinued wherever reasonably possible. Carbon roles will be disposed of in a way that makes it impossible to read the image on the film.

PROCEDURE:

1. The Plan Privacy Official is responsible for approving a standard facsimile cover sheet to be used with any fax transmission of protected health information.

2. Anyone sending PHI by fax must use the standard cover sheet.

3. At each location at which a fax machine is used to send or receive PHI, the senior administrative person will assure that the fax machine is located in a secure area, where only authorized workers have access to it.

4. Anyone sending a fax that contains PHI will double check the accuracy of the destination number in the fax machine's LCD or other display before sending the fax.

5. Transmittal records for each fax that contains PHI must be checked immediately after the transmittal to assure that the information was sent to the correct number.

6. Anyone who sends PHI by fax must attach the transmittal record to the information that was faxed.

7. Whenever possible, separate fax machines will be installed to receive PHI and administrative information.

8. Prior to distribution of a fax message received at a Plan location, the message must be reviewed to make sure that all pages that belong to that message have been received and are together, and that pages that belong to other messages are not included inadvertently. The cover sheet received with the message, if any, will be placed on top of the message.

9. At each location at which a fax machine is used to send PHI, the senior administrative person will preprogram and test frequently used fax numbers.

10. If it is discovered that PHI has been sent to the wrong fax number, the sender must immediately send a second fax to the number that was contacted in error, reiterating the confidentiality message, above, and asking the recipient to telephone the sender immediately to arrange proper disposition of the information.

11. Any instance of transmitting PHI to the wrong destination number must be reported to the Plan Privacy Official immediately. The report must include the date, time, the wrong number, the correct number, the intended recipient, the identity of the member, and a brief description of the information that was transmitted in error. **Transmission of PHI by Fax to a wrong number must be included in an accounting of disclosures of PHI**. See the ACCOUNTING OF DISCLOSURES OF PROTECTED HEALTH INFORMATION policy.

12. At each location at which a fax machine is used to send PHI, the senior administrative person will assure that used carbon rolls from fax machines are incinerated or otherwise rendered unreadable.

E-MAIL AND PROTECTED HEALTH INFORMATION

RESPONSIBILITY: Agency and Local Employer Benefit Administrators; All users of Office of Health Benefits' e-mail systems and/or Internet e-mail

BACKGROUND:

E-mail is a powerful communication tool. However, the very features that make it useful create security concerns when an e-mail message contains confidential information, such as protected health information (PHI). For example:

- E-mail can be intercepted by someone who is not an intended recipient.
- The identity of the sender can be changed.
- The content of the message can be changed.
- The message can be forwarded to someone who does not have a right to receive the information it contains.
- E-mail can easily be broadcast to a large number of unauthorized recipients.
- E-mail can transport computer viruses.
- E-mail is not necessarily indexed by a member identifier, making it difficult to account for any e-mail disclosure of protected health information for a specific member.

POLICY:

Protected health information may not be transmitted by e-mail unless the sender is using a secure e-mail system.

A secure e-mail system has the following features:

1. The message cannot be intercepted. If the message is sent over an open network (e.g. the Internet) it must be encrypted, using an encryption standard approved by the Director of Information Services.
2. The recipient of the message will know that the content has not been altered during transmission.
3. The recipient of the message will know the true identity of the sender.
4. There are safeguards to lessen the possibility of sending the message to someone who is not authorized to receive it.
5. There are safeguards to reduce the likelihood that the message will be forwarded to someone who is not an intended recipient.
6. The e-mail will be linked to the member's record in some way, either as a paper copy or an electronic file.

7. The system has been approved by the Director of Information Systems as secure, in accordance with this policy.

E-mail will not be used to transmit a message to more than one member at one time. This is to avoid the potential for inadvertent disclosure of e-mail addresses, linking e-mail addresses with clinical information in the message, or violating prohibitions against using member-specific information for certain types of marketing.

"Instant Message" programs are inherently not secure and may not be used to transmit protected health information.

All e-mails messages will include the following statement:

"Confidentiality Statement: The documents accompanying this transmission may contain confidential health information that is legally privileged. This information is intended only for the use of the individuals or entities listed above. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or action taken in reliance on the contents of these documents is strictly prohibited. If you have received this information in error, please notify the sender immediately and arrange for the return or destruction of these documents."

PROCEDURE:

The Director of Information Systems and others with expertise in secure e-mail systems, as necessary, will develop modifications to the Plan's e-mail policy to incorporate the above requirements.

The modifications will address internal communications among members of the workforce, communications with members, communications with insurance companies, and other e-mail uses that involve the use of protected health information.

REFERENCE

The reference section contains definitions

DEFINITIONS

Most of the following definitions are taken from federal privacy and security regulations, and their preambles. In order to apply properly the Health Benefits Plan for State and Local Employees (Plan)' privacy policies and procedures, it is necessary to understand these definitions.

When the following terms are used in the Plan's policies and procedures, they are to be given the definitions listed here.

Access refers to the ability or the means necessary to create, read, write, modify, delete, or communicate data/information or otherwise make use of any system resource.

Authorization means an individual's written permission to use or disclose protected health information.

Business associate means a person or organization that performs a function or activity involving the use or disclosure of protected health information, on behalf of the Plan. A person or organization who only assists in the performance of the function or activity is also a business associate. This includes a person or organization that receives PHI from the Plan, and one who obtains PHI for the Plan. This includes, for example: data analysis, processing or administration; web site hosting; utilization review; quality assurance; billing; collections; benefit management; practice management; legal services; actuarial services; accounting and auditing; consulting; management and administrative services; accreditation; financial services; or any other service in which the person or organization obtains PHI from or for the Plan. Members of the workforce are not considered business associates. The exchange of protected health information between providers of health care, for purposes of providing treatment to a member, does not create a business associate relationship.

Clearinghouse. See health care clearinghouse.

Covered entity means an entity that is required to comply with the requirements of HIPAA administrative simplification regulations. Covered entities are: health plans, health care clearinghouses, and health care providers that transmit any health information in electronic form in connection with a standard transaction.

Data aggregation means the combining of the Plan protected health information with the protected health information of other organizations, to permit data analyses that relate to the health care operations of the respective organizations.

De-identification means the removal of data elements that could be used alone, or in combination with other available data, to identify the individual to whom a record of health information pertains.

DHHS means the federal Department of Health and Human Services.

Disclosure means the release, transfer, provision of access to, or divulging in any other manner of information outside the Plan. See also "use."

Electronic media means the mode of electronic transmission. It includes the Internet (wide-open), Extranet (using Internet technology to link a business with information only accessible to collaborating parties), leased lines, dial-up lines, private networks, and those transmissions that are physically moved from one location to another using magnetic tape, disk, or compact disk media.

Encryption, or encipherment, refers to a method of transforming confidential plaintext into ciphertext to protect it. An encryption algorithm combines plain text with other values called keys, or ciphers, so the data becomes unintelligible. Once encrypted, data can be stored or transmitted over unsecured lines. Decrypting data reverses the encryption algorithm process and makes the plain text available for further processing.

Entity authentication refers to the corroboration that an entity is the one claimed. It should include a unique user identifier, at least one means of verification (biometrics, password, personal identification number, token, or telephone callback procedure.)

Group health plan means an employee welfare benefit plan as defined in the federal Employee Retirement Income Security Act (ERISA), to the extent that the plan provides or pays for medical care.

Health care clearinghouse means a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and ''value-added'' networks and switches, that does either of the following functions:

(1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.

(2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Health care operations is a term defined in federal regulations that govern the privacy of protected health information [45 CFR 164.501]. The following is a general summary of the definition.

Health care operations include the following:
(1) Quality assessment and improvement activities
(2) Outcomes evaluation
(3) Development of clinical guidelines

(4) Population-based activities relating to improving health or reducing health care costs
(5) Protocol development
(6) Case management and care coordination
(7) Contacting health care providers and members with information about treatment alternatives
(8) Reviewing the competence or qualifications of health care professionals
(9) Evaluating practitioner and provider performance
(10) Evaluating health plan performance
(11) Conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers
(12) Training of non-health care professionals
(13) Accreditation, certification, licensing, or credentialing activities
(14) Underwriting, premium rating, and other activities relating to obtaining or renewing health insurance or reinsurance
(15) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs
(16) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity
(17) Formulary development and administration
(18) Development or improvement of methods of payment or coverage policies
(19) Business management and general administrative activities
(20) Management activities relating to implementation of and compliance with federal and state requirements regarding the privacy and security of PHI
(21) Customer service, including data analysis, provided that protected health information is not disclosed in such analyses.
(22) Resolution of internal grievances
(23) Due diligence in connection with the sale or transfer of assets to another covered entity
(24) The sale, transfer, merger, or consolidation of all or part of the Plan with another covered entity, or an entity that following such activity will become a covered entity
(25) Creating de-identified health information consistent with the applicable the Plan policies
(26) Creating a limited data set
(27) Fundraising and marketing consistent with the applicable the Plan policies

Health care provider. See Provider of health care.

Health insurance company means any health insurance issuer, including an insurance company, insurance service, or insurance organization (including an HMO) that is licensed to engage in the business of insurance in a state and is subject to state law that regulates insurance.

Health maintenance organization (or HMO) means a federally qualified HMO, an organization recognized as an HMO under State law, or a similar organization regulated for solvency under State law in the same manner and to the same extent as such an HMO. [In some states, HMOs are licensed as insurance companies. In other states, HMOs operate under a license or certificate of authority that is unique to HMOs. In either care, an HMO is considered a "health plan."]

Health plan. Brief definition: "Health plan" means an individual or group plan that provides, or pays the cost of, medical care. See the definition of "medical care," below.

Detailed definition: Health plans include all of the following:

(1) A group health plan, which is the same as an employee welfare benefit plan as defined in the federal Employee Retirement Income Security Act (ERISA), to the extent that the plan provides or pays for medical care.

(2) A health insurance issuer, which means an insurance company, insurance service, or insurance organization (including an HMO) that is licensed to engage in the business of insurance in a state and is subject to state law that regulates insurance.

(3) An HMO, which means a federally qualified HMO, an organization recognized as an HMO under State law, or a similar organization regulated for solvency under State law in the same manner and to the same extent as such an HMO. [In some states, HMOs are licensed as insurance companies. In other states, HMOs operate under a license or certificate of authority that is unique to HMOs. In either care, an HMO is considered a "health plan."]

(4) Medicare, which means Part A or Part B of title XVIII of the U. S. Social Security Act.

(5) Medicaid, which means title XIX of the U. S. Social Security Act.

(6) A company that issues Medicare supplemental policies, even if it is not otherwise a health insurance issuer or HMO.

(7) A company that issues long-term care policies, even if it is not otherwise a health insurance issuer or HMO. Exception: if the company only issues nursing home fixed-indemnity policies, and does not otherwise meet the terms of this definition, it is not considered a "health plan."

(8) A Multi-Employer Welfare Arrangement (MEWA) or any other employee welfare benefit plan or other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers.

(9) The health care program for active military personnel under title 10 of the United States Code.

(10) The veterans' health care program under title 38 chapter 17 of the United States Code.

(11) CHAMPUS(TRICARE): The Civilian Health and Medical Program of the Uniformed Services.

(12) The Indian Health Service program under the Indian Health Care Improvement Act.

(13) The Federal Employees Health Benefits Program (FEHBP)

(14) An approved State child health plan under title XXI of the U. S. Social Security Act.

(15) The Medicare+Choice program under Part C of title XVIII of the U. S. Social Security Act.

(16) A high risk pool established under state law to provide health insurance coverage or comparable coverage to eligible individuals.

(17) Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care.

The following are NOT "health plans" for purposes of federal privacy regulations:

1. Policies that provide coverage only for accident, and/or disability income insurance.
2. Coverage issued as a supplement to liability insurance.
3. Liability insurance, including general liability insurance and automobile liability insurance.
4. Workers' compensation or similar insurance.
5. Automobile medical payment insurance.
6. Credit-only insurance.
7. Coverage for on-site medical clinics.
8. Other similar insurance coverage under which benefits for medical care are secondary or incidental to other insurance benefits.
9. A government-funded program that does not meet any of the definitions above, and
   (a) whose principal purpose is other than providing, or paying the cost of, health care; or
   (b) whose principal activity is:
      i. The direct provision of health care to persons; or
      ii. The making of grants to fund the direct provision of health care to persons.

HIPAA means the federal Health Insurance Portability and Accountability Act of 1996.

HMO. See health maintenance organization.

Marketing means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service. It is not considered marketing to communicate treatment options to a member. [NOTE: The definition of marketing in federal HIPAA privacy regulations is more involved. In these templates, the various qualifications attached to this definition in HIPAA, are included in the policy template instead. The HIPAA definition follows:

> Marketing means:
>
> > (1) To make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service, unless the communication is made:
> >
> > > (i) To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits.
> > >
> > > (ii) For treatment of the individual; or
> > >
> > > (iii) For case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual.
> >
> > (2) An arrangement between a covered entity and any other entity whereby the covered entity discloses protected health information to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service.]

Medical care means the diagnosis, cure, mitigation, treatment, or prevention of disease, or amounts paid for the purpose of affecting any body structure or function of the body; amounts paid for transportation primarily for and essential to these items; and amounts paid for insurance covering the items and the transportation specified in this definition.

Member means any individual about whom the Plan has created or received individually identifiable health information.

Minimum necessary is the least amount of protected health information that is required to achieve the purpose for which it is intended.

Organized health care arrangement means:

(1) A clinically integrated care setting in which individuals typically receive health care from more than one health care provider (Example: hospital and its medical staff, when treating members at the hospital);
(2) An organized system of health care in which more than one covered entity participates, and in which the participating covered entities:
    (i) Hold themselves out to the public as participating in a joint arrangement; and
    (ii) Participate in joint activities that include at least one of the following:
        (A) Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;
        (B) Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or
        (C) Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.

    (Example: an individual practice association, or "IPA.")
(3) A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to protected health information created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan;
(4) A group health plan and one or more other group health plans each of which are maintained by the same plan sponsor; or
(5) The group health plans described in paragraph (4) of this definition and health insurance issuers or HMOs with respect to such group health plans, but only with respect to protected health information created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such group health plans.

Payment means:
(1) The activities undertaken by the Plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan
(2) The activities undertaken by the Plan to obtain or provide reimbursement for the provision of health care

(3) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts)
(4) Adjudication or subrogation of health benefit claims;
(5) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;
(6) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
(7) Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and
(8) Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement:
    (A) Name and address;
    (B) Date of birth;
    (C) Social security number;
    (D) Payment history;
    (E) Account number; and
    (F) Name and address of the health care provider and/or health plan.

Personal representative means a person who, under applicable law, has authority to act on behalf of another individual in making decisions related to health care.

PHI. See Protected health information.

Plan administration means the administration functions performed by the plan sponsor of a group health plan on behalf of the group health plan, and excludes functions performed by the plan sponsor in connection with any other benefit or benefit plan of the plan sponsor.

Plan sponsor means (i) the employer in the case of an employee benefit plan established or maintained by a single employer, (ii) the employee organization in the case of a plan established or maintained by an employee organization, or (iii) in the case of a plan established or maintained by two or more employers or jointly by one or more employers and one or more employee organizations, the association, committee, joint board of trustees, or other similar group of representatives of the parties who establish or maintain the plan.

Protected health information (abbreviated PHI) means information, including demographic information, whether oral or recorded in any form or medium, that relates the individual's health, health care services, or payment for services and which identifies the individual. (This includes information that 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 includes information that could reasonably be used to identify the individual, such as social security number or driver's license number, even if the name is not included). Protected health information does not include the following:

1. Records covered by the Family Educational Right and Privacy Act
2. Employment records held by the Plan in its role as employer.

Provider of health care means any person or organization, which furnishes, bills, or is paid for health care services in the normal course of business.

Research means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to knowledge that is generally applicable.

Summary health information means information about individual participants in a group health plan that summarizes the claims history, claims expenses, or type of claims experienced by those participants; and which has been de-identified in accordance with the Plan's DE-IDENTIFIED INFORMATION policy, except that the information may be aggregated by 5-digit zip code instead of 3-digit zip code.

Treatment means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a member; or the referral of a member for health care from one health care provider to another.

Use means, with respect to protected health information, the sharing, employment, application, utilization, examination, or analysis of such information within the Plan. See also "disclosure."

Worker means a member of the Plan workforce.

Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for the Plan, is under the direct control of the Plan, whether or not the Plan pays them. Generally, for an employee health benefit plan, the workforce will include individuals directly employed by the health benefit plan, if any, and employees of the plan sponsor who are assigned to perform plan administration duties.

REFERENCE: 45 CFR §§ 142.304, 160.103, 160.202, 162.103, 164.501; 65 FR 82546