Cobb County Government

HIPAA PRIVACY POLICY AND PROCEDURES

This Policy is intended to comply with the Health Insurance Portability and Accountability Act of 1996. It applies to the following employee benefits (the "Plan") that are sponsored by the Employer:

Medical
Health flexible spending account
Dental

GENERAL INFORMATION

Effective Date
This Privacy Policy is effective as of January 1, 2012 (the "Effective Date").

General Policy
It is the policy of the Plan to maintain and protect the privacy of the protected health information ("PHI") of its plan participants and to give its participants specific rights with respect to their PHI.

Purpose
This policy is intended to promote awareness of the confidential nature of the medical information that is collected, maintained and disseminated by the Plan. This policy and these procedures reflect the commitment of the Employer to protecting the confidentiality of the private health information of its employees and their dependents.

Responsibility
This Privacy Policy shall be overseen by the Privacy Officer. The Privacy Officer shall have authority and responsibility for implementation and operation of this Policy and Procedures.

POLICIES AND PROCEDURES

Policy #1: Collection and Receipt of Protected Health Information

Policy
The Plan will collect only the minimum necessary PHI that is needed for the particular purpose for which it is collected. The designated record set of the Plan includes all enrollment and disenrollment information, along with any claim forms, explanations of benefits, and any other information that the Plan receives as part of the operations and payment functions of the Plan.

Procedures
1. When collecting or receiving PHI, employees will request only the minimum necessary information. Prior to making such a request and at the time this policy first becomes effective, employees who collect or receive PHI will evaluate the information that is requested or received to determine that he or she is receiving or requesting the minimum necessary. The Privacy Officer will make the final determination (when necessary) as to what information can be requested and received.

2. When collecting or discussing PHI, employees will comply with the following privacy guidelines, along with any additional procedures established from time to time:
   - PHI should not be discussed in any open area;
   - Documents containing PHI should be kept in locked files and should not be left in any open area or area where the general public has access;
   - Documents containing PHI should be de-identified wherever possible; and
   - Documents containing PHI should be shredded when they are no longer needed.

3. PHI will be discussed and shared with an employee only to the extent that the individual has a need to know the PHI as part of the performance of his or her job duties.

4. The information in the designated record set will be kept in a file separate from an employee's employment file.

Policy #2: Uses and Disclosures of Protected Health Information

Policy

1. The Plan will use and disclose the PHI it creates, collects and/or maintains for the following: to enroll and disenroll individuals in or from the Plan; to evaluate renewal proposals or new health plan vendors, insurance companies or administrators; to assist in claims resolution; and to conduct due diligence in connection with the sale or transfer of assets to a potential successor.

2. All PHI collected by the Plan will be disclosed only to the following "valid recipients" or in the following situations: (1) to the plan participant; (2) if the plan participant is a minor, to the plan participant's parent or legal guardian (a Personal Representative); (3) to a Personal Representative of an individual who is incapable of making health care decisions and/or has appointed another individual to make these decisions on his or her behalf; (4) to an insurance company, reinsurance company, third party administrator or a business associate of the Plan, (5) to the plan participant's representative, agent, or any other person with a signed authorization from the plan participant; (6) in response to legal process; (7) to investigate possible insurance fraud; (8) to help settle a claim dispute for benefits under a medical benefit plan or insurance policy; or (9) to the Plan Sponsor, but only if the plan documents have been amended in accordance with the provisions of HIPAA.

Procedures

1. To the extent reasonably possible, PHI that is requested or disclosed by the Plan will be received or distributed after it has been de-identified. The Privacy Officer will oversee the de-identification process.

2. Where it is not possible or practicable to de-identify PHI that is disclosed, employees will disclose only the minimum necessary information. The Privacy Officer will help, upon request, to determine that the minimum necessary information is disclosed. Minimum necessary standards will be created and followed for all routine disclosures of PHI.

3. In any situation where PHI is requested from the Plan, an employee will verify the identity of the person requesting the information and the authority of the person to have access to PHI (unless the identity and authority is already known).

4. PHI will be disclosed to a Valid Recipient as described above through the telephone, only after the identity and authority of the person who is on the other end of the call is verified.

5. PHI will be sent to a Valid Recipient by facsimile only if the employee who is sending the information can determine that the intended recipient will be the receiver of the facsimile, or that he or she is expecting the confidential facsimile at that time.

6. All fax cover sheets utilized by employees will contain a standard confidentiality statement.

Policy #3: Access to Protected Health Information by Plan Participants

Policy

The Plan will provide plan participants with the right to access their own PHI that has been collected and is maintained by the Plan and is part of the designated record set. This right of access does not apply to information compiled in anticipation of a civil legal action.

Procedures

1. A plan participant (or his or her Personal Representative, including the parent or legal guardian of a minor) may request a copy of his or her PHI, as long as the request is in writing and is dated and signed by the plan participant on a form approved by the Plan. All such requests will be given to the Privacy Officer for response.

2. Within 30 days of receipt of the written request (or 60 days for information that is not maintained on-site), the Privacy Officer will inform the plan participant of the acceptance of the request, will provide a written denial, or will direct the plan participant to the entity that maintains the requested information.

3. The Privacy Officer will provide the plan participant either with the ability to inspect the plan participant's file or will provide a copy of the file, as requested by the plan participant. The Plan may charge a reasonable fee for all copying requests. This fee will include supplies, labor and postage.

4. The Privacy Officer will provide the file in the format requested by the plan participant, unless it is not readily producible in that format.

5. The Privacy Officer may provide the plan participant with a summary of the PHI or an explanation of the PHI, if the plan participant requests such a summary or explanation.

Policy #4: Amendment of Protected Health Information

Policy

The Plan will allow plan participants to request amendment of their PHI that is part of the designated record set. PHI that was not created by the Plan or that is accurate and complete, as determined by the Privacy Officer, is not subject to amendment.

Procedures

1. A request for amendment of PHI must be made on a form approved by the Plan. The request must be made by the plan participant or the plan participant's personal representative, parent (for a minor) or guardian (collectively referred to as "plan participant"). The request must reference the information for which amendment is requested and the reason for the requested amendment.

2. When a plan participant first contacts the Plan to request an amendment, the employee who receives the request will notify the plan participant of the requirements for requesting the change.

3. All written requests for amendment will be forwarded to the Privacy Officer for response.

4. Within 60 days after receipt of the request for amendment, the Privacy Officer will either accept or deny the amendment request. The Privacy Officer will make this determination. If the amendment request is accepted, the Privacy Officer will notify the plan participant and request the agreement of the plan participant to notify business associates or other persons who have received the incorrect PHI about the plan participant from the Plan. If the amendment request is denied, the Privacy Officer will notify the plan participant of the basis for the denial, the right of the plan participant to submit a written statement of disagreement or to request that the amendment and the denial be included in any future disclosures, and a description of how the plan participant may file a complaint.

5. If the plan participant files a statement of disagreement, the Privacy Officer may prepare a written rebuttal, which must be given to the plan participant. All future disclosures of PHI for this plan participant must include both the statement of disagreement and the rebuttal, if any, and a link between these documents and the PHI that is subject to dispute.

Policy #5: Accounting of Disclosures of PHI

Policy

It is the Policy of the Plan to provide plan participants with an accounting of disclosures of PHI that were made for purposes other than the payment and healthcare operations of the Plan.

Procedures

All disclosures of PHI, other than those conducted in the course of payment or healthcare operations of the Plan, will be reported to the Privacy Officer. When requested by a plan participant in writing, the Privacy Officer will prepare an accounting of all disclosures that were not part of the health care operations of the Plan. The accounting will include all disclosures made by the Plan that occurred in the past six years (or shorter period as requested by the plan participant), but excluding any disclosures made prior to April 14, 2004, and will comply with all applicable laws and regulations. The accounting will be provided within 60 days of the request. No charge will be imposed for the first accounting requested during any 12-month period.

Policy #6: Restriction on Disclosures of PHI

Policy

It is the Policy of the Plan to allow plan participants to request a restriction on the uses and disclosures of the plan participant's PHI made by the Plan.

Procedures

1. A request for restriction on the uses and disclosures of PHI must be made on a form approved by the Plan. The request must be made by the plan participant or the plan participant's personal representative, parent (for a minor) or guardian (collectively referred to as "plan participant"). The request must reference the particular type of restriction that is requested and the reason for the requested restriction.

2. When a plan participant first contacts the Plan to request a restriction, the employee who receives the request will notify the plan participant of the requirements for requesting the change.

3. All written requests for restriction will be forwarded to the Privacy Officer for response.

4. Within a reasonable period of time after receipt of the request for restriction, the Privacy Officer will either accept or deny the restriction request. The Privacy Officer will make this determination. If the restriction request is accepted, the Privacy Officer will notify the plan participant and will document the agreed upon restriction. If the restriction request is denied, the Privacy Officer will notify the plan participant of the basis for the denial.

Policy #7: Notice of Privacy Practices

Policy

It is the Policy of the Plan to create and, as required by law, to provide all employees with a Notice of Privacy Practices that describes the Plan's required and permitted uses and disclosures of PHI and the rights of plan participants with respect to their PHI.

Procedures

1. The employer will deliver the Notice of Privacy Practices to each employee as soon as possible after the Effective Date or upon enrollment in the Plan, if later. If an employee has requested that benefit, enrollment or other employment information be delivered by e-mail, the notice may be given by e-mail. Otherwise, the Notice will either be hand delivered or sent by interoffice or U.S. mail.

2. If the employer maintains an employee benefits related website, the employer will also post of copy of the Notice of Privacy Practices prominently on its website.

3. Every three years from the date of the initial delivery of the Notice, the Privacy Officer will be responsible for notifying employees that the Notice is available and that they can receive a copy of it on request.

4. A revised Privacy Notice will be delivered to each employee within 60 days after a material change is made, based on a change in the law or regulations or a change in internal procedures.

Policy #8: Notice in case of Breach of Unsecured PHI

Policy

It is the Policy of the Plan to secure PHI in accordance with its Security Policy (if the employer maintains any PHI in an electronic format on behalf of the plan) and to notify individuals, the media and the Department of Health and Human Services in the event of a breach of unsecured PHI, in accordance with the HITECH Act.

Procedures

1. The employer will follow any Security Policy that it has adopted to comply with the HIPAA Security Rules and will secure any electronic PHI that it maintains in accordance with the HITECH Act.

2. For any breach of unsecured PHI (as both breach and unsecured are defined in the HITECH Act, the employer will provide written notice or a substitute notice (if the last known contact address is insufficient) to each affected individual within 60 days following discovery of any breach of Unsecured PHI. The notice will include:
    - A brief description of what happened including the date of the breach and the date of discovery, if known;
    - A description of the types of unsecured PHI that were involved in the breach;
    - Any steps the individual should take to protect him/herself from potential harm resulting from the breach;
    - A brief description of what the employer is doing to investigate the breach in accordance with HIPAA breach notification requirements;
    - Contact procedures for individuals to ask questions or learn additional information

3. If a breach of unsecured PHI involves more than 500 residents of a state, the employer will provide notice to local media outlets serving the state within 60 days of discovering the breach.

4. If a breach of unsecured PHI involves more than 500 covered persons, the employer will provide notice to the DHHS not later than 60 days after the end of the calendar year in with the breach occurred.

Policy #9: Training

Policy
The Privacy Officer will train or oversee training of all new employees and current staff who have access to PHI. Training will include general information about HIPAA and will focus on the requirements of this HIPAA Privacy Policy.

Procedures

1. The Privacy Officer will conduct or oversee the training for all employees who have or may have access to PHI no later than the date that this Policy becomes effective. New staff will receive training on the Privacy Policy within 3 months of the start of their employment, or within 3 months of the assignment to a position in which they deal with PHI as part of their job requirements.
2. The Privacy Officer will conduct training on any material changes made to the Privacy Policy within 60 days after the changes become effective.
3. Additional training sessions may be conducted by the Privacy Officer as needed.
4. All training will be documented by the Privacy Officer, or other employee as requested by the Privacy Officer.

Policy #10: Complaints

Policy
The Plan will accept and respond to complaints relating to the Privacy Policy, procedures, and compliance efforts relating to the privacy of PHI.

Procedures
1. Complaints regarding this Privacy Policy will be forwarded to the Privacy Officer for review and response.
2. The Privacy Officer will review all complaints, will discuss them (as needed) with the Controller and/or other employees, will review relevant documents and will respond to the plan participant who has filed the complaint.
3. All complaints will be logged by the Privacy Officer. The log will include the complaint and a brief description of the resolution of the complaint.

Policy #11: Recordkeeping

Policy
The Plan will retain all documentation related to this Privacy Policy for a minimum of six (6) years from the date the documentation was created or the date that it was last in effect, whichever is later.

Procedures
1. The following documents will be maintained in the files of the Privacy Officer or other secured location:
    - This Privacy Policy
    - Notice of Privacy Practices (all versions)
    - All signed authorizations
    - PHI Disclosure Log
    - Record Request Log
    - Record Requests
    - Complaint Log, along with copies of any written complaints
    - Records of any sanctions imposed on employees
    - Employee training manuals and procedures
    - Business associate contracts
    - Plan document amendments
    - Plan sponsor certification

2. Every year on or about January 1, the Privacy Officer will determine which records, if any, have been held for the minimum period required and should be destroyed.

Policy #12: Sanctions

Policy
The Plan Sponsor, on behalf of the Plan, will appropriately discipline any staff member who fails to comply with this Privacy Policy.

Procedures
For any failure to comply with this Privacy Policy, an employee will be subject to sanctions up to and including removal of access by the employee to PHI and termination of employment.

Policy #13: Miscellaneous

Mitigation of Wrongful Disclosures
The Plan will attempt to mitigate any disclosures of PHI that are in violation of this Privacy Policy by, for example, requesting return of any written PHI that was improperly disclosed, or by admonishing the recipients of any wrongly-disclosed PHI of their obligation not to further disclose the PHI.

Refraining from Intimidating or Retaliatory Acts
It is the policy of the Plan to prohibit any intimidation, threats, coercion, discrimination or other retaliatory acts against any person for the exercise of his or her rights under this Privacy Policy, for filing a complaint with the DHHS, or for assisting in an investigation of any act made unlawful by the Health Insurance Portability and Accountability Act.

This Privacy Policy is effective as of the Effective Date shown above.

Signature:_____

Name (print or type):_____

Title:_____

Date Signed:_____