g.c.g. risk management inc.
11 BEACH STREET • NEW YORK, NY 10013 • (212) 431-3000

HIPAA SAMPLE PRIVACY POLICY GUIDE – GCG 04/04

Abstract: The following is a sample Employee Medical Information Privacy Policy as per HIPAA, (Health Information Portability and Accountability Act). It tracks and reflects the definitions and procedures relayed in the required Privacy Notice (accompanying this document). Peruse the verbiage **(and customize where indicated)** to ensure your processes are in step with the intent of this policy, including, the designation of the Privacy Officer. More practically, ensure that the basic privacy practices described at the end of the policy are in place to maximize common sense and logistical privacy as much as possible within the context of your operations. A sample checklist is included for your convenience.

**Please note that workers' compensation is in fact, exempt from HIPAA, and legally, the protections and rights do not apply. However, workers' compensation is included in the text herein to maintain consistency in the handling of all health insurance information. (It is our judgment that the requirements, protections and rights are basically common sense and normative and do not present any undue or onerous burden on employers to include in this Privacy Policy.)*

(Sample Policy - GCG 06/04)

(ORGANIZATION) EMPLOYEE MEDICAL INFORMATION PRIVACY POLICY

Introduction *- We are committed to protecting employee health and medical information. We may create/receive/transmit/ maintain a record of employee medical information relating to health care, workers' compensation and disability claims submitted for adjudication (to settle) in administering these benefit plans. This Policy applies to all of the medical information about employees we receive/transmit/ maintain* ***as the employer****. Employees' personal health care providers may have different policies or notices regarding the use and disclosure of your medical information.*

Designated Privacy Officer - The Privacy Office is ***(Name)*** _____ and can be contacted at ***(Contact information including location of office)*** _____.

This Policy covers the methods we may use/disclose employee medical information. It also describes our obligations and employees' rights regarding this. We are required by law to:

- Ensure identifying employee medical information is kept private
- Give employees a Notice of our legal duties & privacy practices regarding their medical information
- Follow the terms of the notice that is currently in effect

How We May Use/Disclose Employee Medical Information: The following categories describe different ways that we use/disclose employee medical information. Each category of uses or disclosures is described. Some examples are provided. Not every use/disclosure in a category is listed. All of the ways we are permitted to use/disclose information will fall within one of these categories.

- ***For Payment.*** In administering employees' health, workers' compensation and disability benefits, our associates and we may use/disclose employee medical information to:
  - Determine eligibility for benefits under the plan.
  - Facilitate payment for treatment, goods, and services employees receive from health care providers
  - Determine benefit responsibility under the plans we serve
  - Coordinate plan coverage.

For example: We use employee medical information from their health care provider to help determine whether a particular treatment is experimental, investigational, or medically necessary. We use such information to determine whether the health plan will cover, or whether the New York State workers' compensation or disability rules call for, a service or treatment. We may also share medical information with a utilization review or pre-certification service provider. We may share medical information with another entity to assist with the adjudication or subrogation of health claims or with another health plan or insurance company to coordinate benefit payments. We may release medical information about employees for workers' compensation or similar programs. We may also disclose medical information about employees in our explanation of benefits forms describing, in general what services were performed, whether they were covered, and to what extent. These explanations of benefits forms are sent to the health care provider that billed the health care benefits plan for the services performed or goods purchased, and they are sent to the enrollee in the employee benefits plan.

- ***For Heath Care Operations.*** We may use/disclose employee medical information for other operations of the employee health care, workers' compensation and disability benefits plans. These uses/disclosures are necessary to run the plan and can include but not limited to:
  - Administer plan benefits requiring handling within our organization's internal offices and staff
  - Make business & development plans for cost/administration activities/business management
  - Implement pre-certification, case management, disability management, or disease management
  - Conduct/arrange medical review, legal services, audit services, & fraud & abuse detection programs
  - Submit claims for stop-loss (or excess loss) coverage
  - Conduct quality assessment and improvement activities
  - Provide underwriting, premium rating, and other activities relating to coverage under the plan
  - Facilitate claims payments under another entity's plan

- ***As Required by Law.*** We will disclose employee medical information when required by federal, state, or local laws, rules, or regulations. For example, we may disclose medical information in response to a: court or administrative order; subpoena; discovery request; other lawful processes; duly authorized law enforcement/regulatory/federal official for intelligence and other national security activities. We are required to abide by state privacy laws that are more stringent than HIPAA. For example, we may be required by state privacy laws to disclose medical information of minors under certain conditions.

All other uses/disclosures of employees' medical information not related to Payment, Healthcare Operations or as required by law will only be released with the employees' written authorization. Employees have the right to revoke the authorization at any time by submitting a Notice of Revocation of Authorization form to the Privacy Officer, ***(name of person if you want to be specific)*** at ***(contact information & location)***. Forms may be obtained from the Privacy Officer or your ***(HR Representative if you prefer)***.

Employees' Rights Regarding Medical Information About Them:

1. ***Right to Inspect & Copy.*** Employees have the right to inspect and obtain a copy of medical information that may be used to make decisions about their healthcare, workers' compensation and disability benefits plans. Request must be submitted in writing to the Privacy Officer, ***(name of person if you want to be specific)***, at ***(contact information & location)***. Information that is considered *"medical and exposure records"* under OSHA is provided free of charge within 15 business days of the request. A cost may be involved in other types of information and may take longer to produce. Requests may be denied in certain very limited circumstances. Employees may request a review of the denial.

2. ***Right to Amend.*** If the employee feels that the medical information is incorrect or incomplete, they may ask us to amend it. Employees have the right to request an amendment as long as the information is kept by or for the applicable employee health, workers' comp and disability benefits plans. Request must be made in writing and submitted to the Privacy Officer, ***(name of person if you want to be specific)***, ***(contact information & location)***. Employee must provide a reason to support the request. We may deny the request for an amendment if it is not in writing or does not include a reason to support it. We may deny the request if it:
   - Is not part of the medical information kept by or for the employee health/disability benefits plan;
   - Was not created by us, (unless the person/entity that created it is no longer available to amend it);
   - Is not part of the information which the employee would be permitted to inspect and copy; or
   - Is accurate and complete.

3. ***Right to an Accounting of Disclosures.*** Employees have the right to request an *"accounting of disclosures"* where such disclosure was made for any purpose other than treatment, payment, or healthcare operations. Requests must be submitted in writing to the Privacy Officer, ***(name of person if you want to be specific)*** at ***(contact information & location)***. The request must state a time period, not longer than six years and not include dates before 04/14/03. The first request list within a 12-month period is free of charge. Employee will be notified of any charges that additional lists may entail at which time they may withdraw/modify the request.

4. ***Right to Request Restrictions.*** Employees have the right to request a restriction/limitation on the medical information we use/disclose for treatment, payment or healthcare operations. Employees also have the right to request a limit on the medical information we disclose to someone who is involved in their care or the payment of their care, like a family member or friend. For example, employee could ask that we not use/disclose information about a surgery that they have had. We are not required to agree to the request. Restrictions requests must be submitted in writing to the Privacy Officer, ***(name of person if you want to be specific)*** at ***(contact information & location)***. The request must state: (1) what information to limit; (2) whether use or disclosure or both is limited; and (3) to whom the limits to apply, for example, disclosures to the spouse.

5. ***Right to Request Confidential Communications.*** Employees have the right to request that we communicate with them about medical matters in a certain way or at a certain location. For example, employee can ask that we only contact them at work or by mail to a certain address. Submit written requests for confidential communications specifying how or where employee wishes to be contacted to the Privacy Officer, ***(name of person if you want to be specific)*** at ***(contact information & location)***. We will not ask the reason for the request. We will accommodate all reasonable requests.

6. ***Right to a Paper Copy of This Notice.*** Employees have the right to a paper copy of this notice. Employees may obtain a copy at any time at ***(elsewhere including web site if you post it)*** or contact the Privacy Officer, ***(name of person if you want to be specific)*** at ***(contact information & location)***.

Changes to This Notice: We reserve the right to change this notice and to make the revised/changed notice effective for medical information we already have along with information we receive in the future. We will post a copy of the current notice at ***(locations you will post changes)***. The Effective Date will be on the top right-hand corner on the first page of the Notice.

Complaints: Employee may file a complaint with us, or the Secretary of the Dept. of Health & Human Services, if they believe their privacy rights have been violated. Complaints must be submitted in writing to the Privacy Officer, ***(name of person if you want to be specific)*** at ***(location)***. Employees will not be penalized for filing a complaint.

Other Uses of Medical Information: Other uses/disclosures of medical information not covered by this Notice or the laws that apply to us will be made only with employees' written permission. If employees provide us permission to use/disclose medical information, they may revoke that permission, in writing, at any time. If permission is revoked, we will no longer use/disclose the medical information for the reasons covered by the written authorization. Employees understand that we are unable to take back any disclosures we have already made with their permission. We are also required to retain our records of the claims submissions we have received from employees or their healthcare providers.

Basic Privacy Practices: We will make every reasonable effort to ensure the privacy of employees' medical information as they are received, collected, stored and transmitted to and from our offices. See checklist of sample procedures below.

___ 1. Medical information files are sequestered from other personnel files.

___ 2. Files containing medical information are retrieved, stored and transmitted in a secure fashion in that they are never made inadvertently available to any unauthorized users.

___ 3. Fax machines receiving and transmitting medical information are in a secure environment with restricted access to authorized employees only.

___ 4. Computer screens displaying medical information are carefully placed so as to minimize unintended disclosure to unauthorized and/or passing viewers, use of screen blinders, procedures to log out each time the user steps away, and restricted code access, are all methods considered and implemented whenever necessary and appropriate.

___ 5. All conversations involving medical information about any employee shall be held in private. Such conversations shall not be held in public areas such as elevators, bathrooms, cafeteria, waiting rooms, lobbies, large hall type rooms, etc.

___ 6. If conversations must be held in an open environment, participants in the discussion shall try to sequester themselves and speak in a low voice in order that only the appropriate listeners can hear and understand the information conveyed.