PRIVACY POLICY

Effective Date: February 17, 2010

INTRODUCTION TO PRIVACY POLICY

It is PHG and/or affiliated facilities (the Facility) policy to comply with its obligations arising under federal and state laws that relate to the security and privacy of individually identifiable health information, including applicable requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the HITECH Act HIPAA privacy rule amendments, the California Confidentiality of Medical Information Act (COMIA), where applicable, and regulations of the U.S. Department of Health and Human Services lawfully promulgated thereunder.

POLICY APPLICATION

1. Application. The policies and procedures relating to patient health information under HIPAA and state law are intended to govern the use and disclosure by the Facility of patient medical information that may be received, transmitted, stored or created by the Facility.

2. Conflicts. Unless otherwise determined by the Privacy Officer, in the event of any conflict between any provision of these policies and procedures with HIPAA (or more stringent state law), HIPAA and/or the state law shall supersede and control.

3. Records Not Included. Any policies and procedures adopted pursuant to HIPAA and related state law only pertains to the access, use and disclosure of the facility's patient medical information.

4. Employee Records. Any policies and procedures adopted pursuant to HIPAA and related state law do not apply to health information obtained by the facility in its role as an employer, such as medical leave files, leave requests, physician fit-for-duty reports, drug screening and exposure testing results, occupational injury files, sick leave requests and justifications, and disability insurance eligibility. Any health information obtained by the facility in its role as a facility (including information about employees) will be protected under any policies and procedures adopted pursuant to HIPAA and will not be used to make any employment determinations (e.g., firing, demotion, etc.). See Attachment E (Employee Disclosure Form that will allow the Facility to provide employees with necessary on the job medical treatment and testing).

5. Complaints. If an employee has any concerns or complaints about the facility's HIPAA and state law compliance, the employee is encouraged to talk to his/her supervisor, the Facility Privacy Designee or the Privacy Officer and/or to complete the Complaint Form.

6. Training. All workforce members will be trained regarding all facility policies and procedures that are necessary for the workforce member to understand and fulfill his or her duties, including the medical information policies and procedures. All new workforce members will be trained within 30 days of hire and annually thereafter. In addition, workforce members will be trained/retrained regarding verified complaints and changes to the facility's polices and procedures as they occur. The facility will maintain a log of workforce member trainings. Failure to comply with training requirements will be cause for disciplinary action against a workforce member, including termination. See Attachments C (Training Program) and D (Employee, Volunteer, and Student Confidentiality Agreement).

7. Mitigation. In the event of any unauthorized or unlawful access, uses or disclosures of protected health information, the Facility Privacy Designee in collaboration with the Privacy Officer will immediately determine a plan of action to mitigate the harmful effects of such unauthorized use or disclosure. Upon detecting any unlawful or unauthorized access to, or use or disclosure of, a patient's medical information, the Privacy Officer shall report such incidents to the relevant state authorities, and also to the affected patient or the patient's representative, as soon as possible and in accordance with applicable state and federal reporting requirements (e.g., within 5 days of detection).

8. Violations. Violations of these policies will be handled in accordance with the Sanctions Policy and other applicable policies and procedures. A violation of these policies may result in disciplinary actions against the employee or contractor, including dismissal.

9. Monitoring Compliance. The Facility Privacy Designee in collaboration with the Privacy Officer will maintain and enforce a system of monitoring compliance with these policies and procedures, in accordance with any policies and procedures adopted by the Facility, including a comprehensive compliance program, and applicable laws.

DEFINITIONS

Unless the context expressly indicates otherwise, the following terms used in these policies and procedures (whether capitalized or lower case) will have the meanings ascribed to them in the CMS Regulations. The following definitions are provided only for convenience and will be amended and updated according to the CMS Regulations. Within the policies and procedures defined terms may be capitalized or written in lower case.

1. "The facility" includes PHG and all affiliated facilities.

2. "CFR" means the U.S. Code of Federal Regulations.

3. "CMS" means the Centers for Medicare and Medicaid Services (formerly known as "HCFA").

4. "CMS Regulations" means the regulations promulgated by CMS under HIPAA, including the Privacy Regulations, the Security Regulations and the Transaction Regulations.

5. "Common Rule" means 45 CFR Part 46 and is the rule for protection of human subjects in research promulgated by DHHS, and adopted by at least 17 federal government agencies, including the National Institutes of Health, for research funded in whole or in part by those agencies.

6. "Covered entity" means a health care provider, a health plan or a health care clearinghouse.

7. "Designated record set" means: a group of records maintained by or for a covered entity that is: (i) the medical records and billing records about individuals maintained by or for a covered health care provider; (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) used, in whole or in part, by or for the covered entity to make care or payment decisions about patients. For purposes of defining a "designated record set," the term "record" means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.

8. "DHHS" means the U.S. Department of Health and Human Services.

9. "Health care operations" means any of the following PHG's activities:

    a. Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

    b. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, 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, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;

c. Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of 45 C.F.R.§ 164.514(g) are met, if applicable;

d. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

e. Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies;

f. Business management and general administrative activities of the entity, including, but not limited to: (i) management activities relating to implementation of and compliance with the requirements of HIPAA; (ii) customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer; (iii) resolution of internal grievances; (iv) the sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; (v) consistency with the applicable requirements of 45 C.F.R.§ 164.514, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity; (vi) due diligence in connection with the sale or transfer of assets to a potential successor in interest, if the potential successor in interest is a covered entity or, following completion of the sale or transfer, will become a covered entity; and (vii) the creation of de-identified health information.

10. "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, and any successor provisions.

11. "Individual" means a patient, an employee, an enrollee or any of their representatives, as applicable in the context of the specific policy.

12. "Limited data set" means protected health information that excludes the following direct identifiers of the patient or of relatives, employers, or household members of the patient: (i) names; (ii) postal address information, other than town or city, state, and zip code; (iii) telephone numbers; (iv) fax numbers; (v) electronic mail addresses; (vi) social security numbers; (vii) medical record numbers; (viii) health plan beneficiary numbers; (ix) account numbers; (x) certificate/license numbers; (xi) vehicle identifiers and serial numbers, including license plate numbers; (xii) device identifiers and serial numbers; (xiii) web universal resource locators

(URLs); (xiv) internet protocol (IP) address numbers; (xv) biometric identifiers, including finger and voice prints; and (xvi) full face photographic images and any comparable images.

a. For the purpose of describing the entities participating in a health care provider network or health plan network, or for the purpose of describing if and the extent to which a product or service (or payment for such product or service) is provided by a covered entity or included in a plan of benefits; or

b. That are tailored to the circumstances of a particular individual and the communications are: (A) Made by a health care provider to an individual as part of the treatment of the individual, and for the purpose of furthering the treatment of that individual; or (B) Made by a health care provider or health plan to an individual in the course of managing the treatment of that individual, or for the purpose of directing or recommending to that individual alternative treatments, therapies, health care providers, or settings of care.

13. "Marketing" does not include a communication about a product or service a purpose of which is to encourage recipients of the communication to purchase or use the product or service if: (i) The communication is made orally; or (ii) The communication is in writing and the covered entity does not receive direct or indirect remuneration from a third party for making the communication.

14. "Privacy Officer" refers to PHG's Privacy Officer.

15. "Facility Privacy Designee" refers to the employee at the facility appointed by the administrator to manage compliance with the facilities Privacy Policies.

16. "Privacy Regulations" means the standards for the privacy of individually identifiable health information, within the meaning of the final regulations at 45 C.F.R. Parts 160 and 164, and any successor provisions.

17. "Security Regulations" means the standards for electronic signatures and the security of individually identifiable health information, within the meaning of the proposed regulations at 45 C.F.R. Part 142, and any successor provisions.

18. "Transactions Regulations" means the standards for administrative simplification, including the standards for electronic transactions, the national standard health care provider identifier, and the national standard employer identifier, within the meaning of the final regulations at 45 C.F.R. Parts 160 and 162, and any successor provisions.

19. "Protected Health Information" or "PHI" includes demographic information collected from an individual and:

a. Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

b. 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

i. That identifies the individual; or

ii. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

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

21. "Medical Information" includes protected health information that is individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, or contractor regarding a patient's medical history, mental or physical condition, or treatment. "Individually identifiable" means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity.

22. "Unauthorized or unlawful access" means the inappropriate review or viewing of patient medical information without a direct need for diagnosis, treatment or other lawful use as permitted by HIPAA, the California Confidentiality of Medical Information Act ("COMIA") (Part 2.6 (commencing with Section 56) of the Division 1 of the California Civil Code), or by other statutes or regulations governing the lawful access, use or disclosure of medical information.