

NOTICE OF PRIVACY PRACTICES FOR PROTECTED HEALTH INFORMATION

Federal law [45 CFR Parts 160 and 164] the Health Insurance Portability and Accessibility Act (HIPAA) effective April 14, 2003, requires most health care providers including Executive Health Exams International, to establish policies and procedures to protect the privacy of health information.

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

I. Your Privacy Rights. Executive Health Exams International (EHE) is permitted to use and disclose your protected health information [PHI] (i.e. individually identifiable health information – your medical records) for the purpose of treatment, payment, and health care operations. You are not required to sign a consent for EHE to use your medical information for these purposes.

Treatment is defined here as providing, coordinating, managing health care or related services as well as consultation between health care providers related to your condition and care or referral for health care. For example: Health care providers at EHE may refer to and disclose your PHI to:

- (1) Perform laboratory tests, screening tests, take medical histories and perform physical examinations;
- (2) Arrange for appropriate referrals for diagnosis and treatment as well as answer your questions about your treatment or test findings;
- (3) Consult with a specialist about your care.

Payment is defined as those activities necessary to obtain payment or be reimbursed for health care services provided. Under the privacy law your medical record (PHI) may be reviewed or disclosed to conduct payment activities such as:

- (1) Billing and collection activities;
- (2) Reviewing health care services for medical necessity, coverage, justification of charges;
- (3) Making disclosures to consumer reporting agencies (limited to specified identifying information about the individual, his or her payment history, and identifying information about EHE).

Health care operations are certain administrative, financial, legal, quality improvement and activities required by federal, state, and local law that are necessary to run EHE's business and to support the core functions of treatment and payment.

- (1) Medical records may be reviewed and disclosed when performing the following activities:
 - a. Conducting quality improvement activities to improve our patient's health care services and reduce health care costs.
 - b. Reviewing the competence or qualifications of health care professionals, evaluating our health care providers performance, training of health care and non-health care professionals, accreditation, certification, licensing, or credentialing activities;
 - c. Conducting or arranging for medical review, risk management, legal, and auditing services, including fraud and abuse detection and reporting in response to law enforcement and public health compliance programs;
 - d. Business planning and development, such as conducting cost-management and planning analyses related to managing and operating EHE.
 - e. Business management and general administrative activities, customer service, resolution of internal grievances, sale or transfer of assets, creating de-identified health information.

- (2) Executive Health Exams may contact you to provide appointment reminders or information about treatment that is permissible under the Privacy Rule.

II. Access of Individuals to Protected Health Information. You have the right to inspect and obtain a copy of your medical record available at EHE for as long as the medical record is maintained by EHE, provided the request is in writing and signed by you or your legal representative. There are exceptions. The law does not allow you to access certain records including but not limited to the following categories:

Psychotherapy notes, correctional institution records, information gathered for or in anticipation of a civil, criminal, or administrative proceeding, Certain lab reports subject to the federal Clinical Laboratory Improvements Amendments of 1988 (CLIA), and research to which the individual has consented.

- (1) Executive Health Exams, specifically your examining physician or another EHE licensed health care professional, may deny you access to your medical record.
- (2) You have the right to appeal a denial and have such denials reviewed by a licensed health care professional designated by EHE who did not participate in the original review. Appeals can be made to the EHE Medical Records Department by calling (212-332-3700).

III. Amendments and Corrections. You have the right to have EHE amend or correct your medical record for as long as EHE maintains the medical record, if the amendment or correction is made in writing and provides a reason to support the request.

- (1) Executive Health Exams, specifically your examining physician or another EHE licensed health care professional, may deny your request for an amendment or correction if he or she determines that the medical record is accurate and complete.
- (2) Executive Health Exams must provide you with a timely written denial in plain language stating the basis for the denial.
- (3) You have the right to appeal a decision denying amendments or corrections. Requests to appeal denials of amendments or corrections can be made to the EHE Medical Records Department by calling (212-332-3700).

IV. Accounting of Disclosures. You have a right to receive a written accounting of disclosures of protected health information made by EHE up to six years prior to the date on which the accounting is requested, except for the following:

- (1.) Disclosures to carry out treatment; payment and health care operations;
- (2.) Disclosures permitted by this regulation;
- (3.) Disclosures authorized by the individual; and
- (4.) Disclosures that occurred prior to April 14, 2003.

V. Receipt of Notice. You have the right to receive notice of EHE's privacy information practices. On the first day of service beginning April 14, 2003, EHE will provide each patient with a written statement of the HIPAA required privacy practices unless you are seen for emergency treatment, thereafter any revisions of the law, will be posted in a clear and prominent location in EHE's facilities.

VI. Minimum Necessary. Executive Health Exams has developed policies and procedures that reasonably limit its disclosures of, and requests for, protected health information. Executive Health Exams has also developed policies and procedures that limit which members of its workforce may have access to protected health information for treatment, payment, and health care operations, based on those who need access to the information to do their jobs. However, EHE is not required to apply the minimum necessary standard to disclosures to or requests by a health care provider for treatment purposes.

VII. Incidental Uses and Disclosures. Because of the nature of providing clinical services, the Privacy Rule permits certain incidental uses and disclosures of your health information to occur. For example, common practices, such as: overhearing a health care provider's confidential conversation with another provider or a patient; the use of sign-in sheets; placing medical charts outside exam rooms; and calling out names in waiting rooms will not violate the Rule, so long as the information disclosed is appropriately limited and EHE has used reasonable safeguards.

The Privacy Rule permits health care providers to communicate with patients regarding their health care. This includes communication with patients at their homes, whether through the mail or by phone or in some other manner. Health care providers can leave messages for patients on their answering machines if care is taken to limit the amount of information disclosed.

Health care providers can disclose limited information to family members, friends, or other persons regarding an individual's care, *unless you specifically restrict such communications*. Such disclosures can be made even when the individual is not present if professional judgment is used to assure such disclosures are in the best interest of the patient and limited information is disclosed. *The law does not expect EHE to guarantee the privacy of protected health information from any and all potential risks*. Some of the practices EHE uses to protect the privacy of medical information include:

- (1) Avoiding the use of patients' names in public hallways and elevators;
- (2) Requiring that medical records be stored in areas that can be locked or that have limited access by personnel;
- (3) Providing additional security, such as passwords on computers maintaining personal information;
- (4) Making reasonable efforts to isolate interview and examination rooms to protect confidential conversations;
- (5) Locating the x-ray viewing room away from the general patient areas;
- (6) Destroying drafts of protected health information by shredding;
- (7) Maintaining written policies and procedures that implement safeguards reasonably designed to protect medical records from unnecessary access, use, and disclosure.

VIII. Authorization Requirements. An authorization is required for uses and disclosures of protected health information, not otherwise allowed by the Rule. Examples of when an authorization is required are:

- (1) To disclose protected health information to a third party (i.e. a doctor, medical center, therapist) specified by the individual;
- (2) For marketing and for research studies where protected health information is used or disclosed.

An authorization must specify the following:

- a. A description of the protected health information to be disclosed;
- b. The person or organization authorized to make the disclosure;
- c. The person/s to whom EHE may make the disclosure;
- d. The purpose for which the information may be disclosed;
- e. Your signature or the signature of your legal representative and the date of signing;
- f. An acknowledgment of the right of revocation;
- g. A statement that once the information is disclosed it may not be protected by the authorized recipient.

IX. Business Associates Agreements. EHE must obtain a signed agreement from all business associates who may have access to medical records as part of their business relationship with EHE. Such business associates may include auditors, computer consultants assisting with patient data programs, and medical record storage companies. The agreement must state that the business associate will only use protected health information for the purpose of their business relationship with EHE. Business associates are prohibited from using EHE's protected health information for other independent purposes and are required by the law to safeguard the information from misuses.

X. Your Right to Request Privacy Protection. You have the right to request restrictions on how EHE will use and disclose your medical records for treatment, payment, and health care operations. Executive Health Exams is not required to agree to your request, but is bound by any restrictions to which EHE agrees. For example, you may request to receive confidential communications at alternative locations or by alternative means (i.e. a call to your office rather than to your home). Executive Health Exams must accommodate your reasonable requests for such confidential communications.

XI. Right to file a Complaint. If you believe EHE has not complied with the Privacy Rule, you may file a complaint with EHE's Privacy Officer who can be contacted by telephone at 212 332-3700. If you are not satisfied that your concerns have been resolved, you may file a written complaint with the Secretary of Health and Human Services, by writing to:

United States Department of Health and Human Services Secretary
200 Independence Avenue, SW
Washington, DC 20201
202.690.0257 / www.hhs.gov

The complaint must name EHE and describe the acts or omissions you believe to be in violation of the Rule. The complaint must be filed within 180 days of when you knew or should have known that the suspected violation took place. The Secretary may conduct compliance reviews to determine whether EHE is complying with the Privacy Rule.

Please note that under HIPAA other current applicable state laws may be more restrictive than the federal privacy law.