

ELKIN & ASSOCIATES, LLC

HIPAA Privacy Policy and Procedures

INTRODUCTION

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations restrict a Covered Entity's ability to use and disclose Protected Health Information (PHI). It is the policy of Elkin & Associates, LLC (the "Company") in Business Associate relationships with Covered Entities (clients) to comply fully with HIPAA's requirements. To that end, all members of the Company's workforce who have access to PHI must comply with this Privacy Policy and Procedures.

For purpose of this Policy, the workforce includes individuals who would be considered part of the workforce under HIPAA such as employees, volunteers, trainees, temporary workers, and other persons whose work performance is under the direct control of the Company whether or not they are paid by the Company.

No third party rights (including but not limited to rights of Plan participants, beneficiaries, covered dependents or business associates) are intended to be created by this Policy. The Company reserves the right to amend or change this Policy at any time (even retroactively) without notice. To the extent this Policy establishes requirements and obligations above and beyond those required by HIPAA, the Policy shall be aspirational and shall not be binding upon the Company. This Policy does not address requirements under other federal laws or under state laws.

RESPONSIBILITIES AS A BUSINESS ASSOCIATE OF A COVERED ENTITY

- I. **Privacy Officer and Contact Person:** Emily E. Lemel will be the Privacy Officer. The Privacy Officer is responsible for the development and implementation of policies and procedures relating to privacy. The Privacy Officer will also serve as the contact person for participants who have questions, concerns or complaints about the privacy of their PHI.
- II. **Workforce Training:** It is the Company's policy to train all members of its workforce on its privacy policies and procedures. The Privacy Officer is charged with developing training schedules and programs.
- III. **Technical and Physical Safeguards and Firewall:** The Company will establish appropriate technical and physical safeguards to prevent PHI from intentionally or unintentionally being used or disclosed. Technical safeguards including limiting access to information by creating computer firewalls. Physical safeguards including locking doors or filing cabinets. Firewalls will ensure that only authorized employees will have access to PHI, that they will have access to only

the minimum amount of PHI necessary for administrative functions, and they will not further use or disclose PHI in violation of HIPAA.

- IV. **Privacy Notice:** The Privacy Officer is responsible for developing and maintaining a notice of the Company's privacy practices. The privacy notice will inform participants that the Company will have access to PHI in connection with its administrative functions. The notice will also provide a description of the complaint procedures including the name and telephone number of the contact person and the date of the notice. The notice of privacy practices will be individually delivered to all participants:
 - a. no later than April 14, 2004,
 - b. on an ongoing basis, at the time of an individual's enrollment in the Plan
 - c. within 60 days after a material change to the notice
 - d. notice of availability of the privacy notice
- V. **Complaints:** The Privacy Officer, Emily E. Lemel, will be the contact person for receiving complaints. A copy of the complaint procedure shall be provided to any participant upon request.
- VI. **Sanctions for Violations of Privacy Policy:** Sanctions for using or disclosing PHI in violation of this policy will be imposed in accordance with the Company's disciplinary policy up to and including termination.
- VII. **Mitigation of Inadvertent Disclosures of Protected Health Information:** The Company shall mitigate, to the extent possible, any harmful effects that become known to it as a result of a use or disclosure of an individual's PHI in violation of this policy. As a result, if an employee becomes aware of a disclosure of PHI, either by an employee or an outside consultant/contractor, that is not in compliance with this Policy, immediately contact the Privacy Officer so that the appropriate steps to mitigate the harm to the participant can be taken.
- VIII. **No Intimidating or Retaliatory Acts: No Waiver of HIPAA Privacy:** No employee may intimidate, threaten, coerce, discriminate against or take other retaliatory action against individuals for exercising their rights, filing a complaint, participating in an investigation, or opposing any improper practice under HIPAA. No individual shall be required to waive his or her privacy rights under HIPAA as a condition of treatment, payment, enrollment or eligibility.
- IX. **Documentation:** The Company's privacy policies and procedures shall be documented and maintained for at least six (6) years. Policies and procedures must be changed as necessary or appropriate to comply with changes in the law, standards, requirements and implementation specifications. Any changes to policies or procedures must be promptly documented. If a change in law impacts the privacy notice, the privacy policy must promptly be revised and made available. Such change is effective only with respect to PHI created or received after the effective date of the notice. The Company shall document certain events and actions (including authorizations, requests for information, sanctions and complaints) related to an individual's privacy rights. The documentation of any policies, procedures, actions, activities and designations may be maintained in either written or electronic format.

POLICIES ON USE AND DISCLOSURE OF PHI

- I. **Use and Disclosure Defined:** The Company will use and disclose PHI only as permitted under HIPAA.
 - a. *Use:* The sharing, employment, application, utilization, examination or analysis of individually identifiable health information by any person working for or under the direction of the Company.
 - b. *Disclosure:* Any release, transfer, provision of access to or divulging in any other manner of individually identifiable health information to persons not employed by or working under the direction of the Company.
- II. **Workforce Must Comply with Company's Policy and Procedures:** All members of the Company's workforce (described at the beginning of this Policy and referred to herein as "employees") must comply with this Policy.
- III. **Access to PHI is Limited to Certain Employees:** Any employees of the Company who adjudicate claims or provide customer service for participants shall have access to PHI on behalf of the Covered Entity. These employees may use and disclose PHI for administrative functions and they may disclose PHI to other employees with access for administrative functions; however the PHI disclosed is limited to the minimum amount necessary to perform the administrative function. Employees with access may not disclose PHI to other employees unless an authorization is in place or the disclosure otherwise is in compliance with this Policy.
- IV. **Permitted Uses and Disclosures:** PHI may be disclosed for payment purposes and for purposes of health care operations.
 - a. *Payment:* Payment includes activities undertaken to obtain contributions or to determine or fulfill the responsibility for benefits or to obtain or provide reimbursement for health care. Payment also includes: eligibility and coverage determinations including coordination of benefits and adjudication or subrogation of health benefit claims; risk adjusting based on enrollee status and demographic characteristics; billing claims management, collection activities, and related health care data processing.
 - b. *Health Care Operations:* Health care operations may include any of the following activities to the extent that they are related to the administrative functions: conducting quality assessment and improvement activities; reviewing health plan performance, underwriting and premium rating, conducting or arranging for medical review, legal services and auditing functions (e.g., health care fraud and abuse detection programs); business planning and development; and business management and general administrative activities.
- V. **No Disclosure of PHI for Non-Health Plan Purposes:** PHI may not be used or discussed for the payment or operation of the non-health benefits such as disability, workers' compensation, life insurance, etc. unless the participant has provided an authorization for such use or disclosure or such use or disclosure is required by applicable state law and particular requirements under HIPAA are met.

- VI. **Mandatory Disclosure of PHI:** to the Individual and The Department of Health & Human Services (HHS): A participant's PHI must be disclosed as required by HIPAA in two situations:
- a. The disclosure is to the individual who is the subject of the information;
 - b. The disclosure is made to HHS for purposes of enforcing HIPAA.
- VII. **Permissive Disclosure of PHI:** for Legal and Public Policy Purposes: PHI may be disclosed in the following situations with a participant's authorization, when specific requirements are satisfied. The Company's more detailed procedures describe specific requirements that must be met before these types of disclosures may be made. The requirements include prior approval of the Company's Privacy Officer. Permitted are disclosures:
- a. about victims of abuse, neglect or domestic violence;
 - b. for law enforcement purposes;
 - c. for public health activities
 - d. for health oversight activities;
 - e. about decedents;
 - f. to avert a serious threat to health or safety;
 - g. for specialized government functions; and
 - h. that relate to worker's compensation programs.
- VIII. **Disclosure of PHI Pursuant to an Authorization:** PHI may be disclosed for any purpose if an authorization that satisfies all of HIPAA's requirements for a valid authorization is provided by the participant. All uses and disclosures made pursuant to a signed authorization must be consistent with the terms and conditions of the authorization.
- IX. **Complying With the "Minimum-Necessary" Standard:** HIPAA requires that when PHI is used or disclosed, the amount disclosed generally must be limited to the "minimum necessary" to accomplish the purpose of the use or disclosure. The minimum necessary standard does not apply to any of the following uses or disclosures made: to the individual, pursuant to a valid authorization, to HHS, required by law or required to comply with HIPAA. All other disclosure must be reviewed on an individual bases with the Privacy Officer.
- X. **Disclosure of PHI to Business Associates:** Employees may disclose PHI to business associates and allow other business associates to create or receive PHI. However, prior to doing so, assurances must be obtained from the business associate that it will appropriately safeguard the information. Before sharing PHI with outside consultants or contractor who meet the definition of a business associate, employees must contact the Privacy Officer and verify that a business associate contract is in place.
- XI. **Disclosures of De-Identified Information:** The Company may freely use and disclose de-identified information. De-identified information is health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual.

POLICIES ON INDIVIDUAL RIGHTS

- I. **Access to Protected Health Information and Requests for Amendment:** HIPAA gives participants the right to access and obtain copies of their PHI that the business associate maintains in designated record sets. HIPAA also provides that participants may request to have their PHI amended. The Company will provide access to PHI and it will consider requests for amendment that are submitted in writing by participants. Designated Record Set is a group of records maintained by or for the Company that includes the payment and claims adjudication records of an individual or other PHI used in whole or in part by or for the Covered Entity to make coverage decisions about an individual.
- II. **Accounting:** An individual has the right to obtain an accounting of certain disclosures of his or her own PHI. This right to an accounting extends to disclosures made in the last six years. The Company shall respond to an accounting request within 60 days. If the Company is unable to provide the accounting within 60 days it may extend the period by 30 days, provided that it gives the participant notice (including the reason for the delay and the date the information will be provided) within the original 60 day period. The accounting must include the date of the disclosure, the name of the receiving party, a brief description of the information disclosed and a brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure (or a copy of the written request for disclosure, if any). If a brief purpose statement is included in the accounting, it must be sufficient to reasonably inform the individual of the basis of the disclosure. The first accounting in any 12 month period shall be provided free of charge. The Privacy Officer may impose reasonable production and mailing costs for subsequent accountings.
- III. **Requests for Alternative Communication Means or Locations:** Participants may request to receive communications regarding their PHI by alternative means or at alternative locations. The Company may grant such requests if they are reasonable and the participant assures that confidentiality will not be compromised.
- IV. **Requests for Restrictions on Uses and Disclosures of Protected Health Information:** A participant may request restrictions on the use and disclosure of the participant's PHI. It is the Company's policy to attempt to honor such requests if, in the sole discretion of the Company, the requests are reasonable.

DETAILED HIPAA PRIVACY PROCEDURES

- I. **Reimbursement Claim Forms**
Hard copies of all reimbursement claim forms are stored in a secure area while in the Elkin & Associates office. Copies will be shredded after digitally imaged into the Elkin & Associates system.
- II. **Phone Conversation with Participant**
To ensure that potential Protected Health Information is not divulged to an improper party, Elkin & Associates will confirm the participant's social security number and mailing address to recognize a participant or participant representative.
- III. **Phone Conversation with Third Parties regarding Participant**
No third party entity will be allowed access to a participant's Personal Health Information without explicit written authorization by the participant. All authorizations must be submitted to the Elkin & Associates HIPAA Privacy Officer for review and acceptance prior to the release of any information.
- IV. **Changes in mailing address will not be accepted via phone conversation.**
Participant must request a mailing address change in writing via faxed or mailed form or an email to Elkin and Associates.
- V. **Phone Conversations with Service Providers**
Telephone calls to service providers will be limited to requests for information at the request of the participant and/or a signed release form.
- VI. **Phone Conversations with Clients**
Telephone calls to clients will be limited to requests for the information which is considered enrollment information and is used for plan administration purposes only and not protected health information.
- VII. **E-mail Correspondence**
Notification emails sent to participants throughout the claim process do not include identifiable health information. Any additional email correspondence from Elkin & Associates to a participant shall not include identifiable health information. Elkin & Associates will not, however, be responsible for any transfer of confidential information via email originating from the participant.
- VIII. **Participant Activity Statements**
Elkin & Associates will only disclose financial activity statements to client companies. Any statements containing protected health information will be limited to participant requests only.
- IX. **Rejection Letters/Mailed Correspondence**
Any correspondence originating from Elkin & Associates is mailed to the participant's home address. Prior to mailing, each correspondence is audited to ensure correct identification of enclosures.

- X. **Rejection Responses/Participant Correspondence**
Hard copies of any employee correspondence are held in a secure area while in the Elkin & Associates office. All documents will be shredded after digitally imaged into the Elkin & Associates system.
- XI. **Reimbursement Checks and Direct Deposit Vouchers**
All checks and vouchers contain protected health information in the form of participant or dependent name, identifiable services, and service dates. In order to protect this information, Elkin & Associates maintains the following in-house check procedures:
- Checks and vouchers mailed directly to participant homes are sealed prior to mailing.
- Checks and vouchers sent to clients instead of participant home addresses are sealed prior to mailing.
- Voided checks and returned vouchers are manually shredded in the Elkin & Associates office.
- XII. **Internet Security**
Participants can access their own account information via the encrypted interactive website (www.elkinassociates.com). In order to access his/her personal information, the participant is required to set-up the online account upon first entering the website by selecting a personalized user name and password. Employees at Elkin & Associates do not have access to any individual employee's user name or password.
- XIII. **Electronic Data Transfer Compliance**
Standard format for Electronic Data Interchange between clients and Elkin & Associates is not required. All data transferred between clients and Elkin & Associates is considered employment record and is not subject to standardized formatting. However, Elkin & Associates encourage all clients to submit electronic data in a secure manner. All correspondence originating from Elkin & Associates is protected with a randomly assigned password.