



Cardiovascular Associates of the Delaware Valley, P.A.

*Diagnostic and Interventional Cardiology
Diplomates of the American Board of Internal Medicine & Cardiology*

Section 1. OVERVIEW

1.1 Background and Effective Date.

1.1.1 The Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (“HIPAA”), required that regulations be developed to protect the privacy and security of individually identifiable health care information.

1.1.2 The final privacy regulations promulgated under HIPAA are entitled *Standards for Privacy of Individually Identifiable Health Information*, and are codified at 45 C.F.R. Parts 160 and 164 (the “HIPAA Privacy Rules”).

1.1.3 These Health Privacy Policies and Procedures will apply to operations of THE HEART HOUSE-CADV (“Provider”) to the extent that Provider is a “covered entity” pursuant to 45 C.F.R § 160.102 and § 160.103.

1.2 Purpose.

1.2.1 These Health Privacy Policies and Procedures govern the use and disclosure of individually identifiable health information by Provider and each member of its workforce. They have been issued by THE HEART HOUSE-CADV’s Board of Directors.

1.2.2 By issuing these Health Privacy Policies and Procedures, Provider intends to: (A) reinforce Provider’s long-standing commitment to the privacy and security of personally identified health information that comes into the possession of Provider; (B) establish a framework for compliance with the requirements of the privacy obligations under HIPAA; (C) require all members of Provider’s workforce who come into contact with personally identifiable health information as part of their duties to comply with federal and New Jersey law and to conduct themselves in accordance with all of Provider’s privacy policies; (D) assure that members of Provider’s workforce remain in full compliance with all applicable laws and standards relating to Privacy; and (D) foster an environment to encourage and require reporting of any instances of non-compliance with the HIPAA Privacy Rules and these Health Privacy Policies and Procedures.

1.2.3 All members of Provider’s workforce who have access to individually identifiable health information are expected to read and to be familiar with these Health Privacy Policies and Procedures and should use their best judgment to act in a manner consistent with these Health Privacy Policies and Procedures. If any member of Provider’s workforce is unclear as to his/her rights and obligations with respect to these Health Privacy Policies and Procedures, he or she should review such questions with the Privacy Officer appointed by the Compliance Committee under Section 3.1.

1.3 Amendment.



Cardiovascular Associates of the Delaware Valley, P.A.

*Diagnostic and Interventional Cardiology
Diplomates of the American Board of Internal Medicine & Cardiology*

1.3.1 These Health Privacy Policies and Procedures include any Exhibits and Forms attached to these Health Privacy Policies and Procedures and are subject to change from time to time by the Compliance Committee.

1.4 Definitions. The HIPAA Privacy Rules introduce new terms and redefine other terms. In these Health Privacy Policies and Procedures, definitions of terms may be found in Section 18 and defined terms are shown with Initial Capital Letters. Please consult the Privacy Officer if you do not understand a term used in these Health Privacy Policies and Procedures.

1.5 Application to THE HEART HOUSE-CADV.

1.5.1 The HIPAA Privacy Rules apply only to covered entities, such as health care providers and health care plans. Provider provides health care and thus is covered under the HIPAA Privacy Rules.

1.6 Protected Health Information.

1.6.1 HIPAA protects information that (A) relates to the physical or mental health of an individual; the provision of health care to an individual; or the payment for the provision of health care to an individual; and (B) identifies the individual, or reasonably could be used to identify the individual.

1.6.2 This information is called “Protected Health Information” or “PHI,” and includes:

- name
- any geographic subdivision smaller than a state, including zip codes
- dates related to the individual (birth date, admission date, treatment date, discharge date, death date)
- age if the person is over 89
- telephone number
- fax number
- e-mail address
- social security number
- medical record number, health plan beneficiary number, account number
- certificate and license number, vehicle identification and serial number
- device identifier and serial number
- URL, IP address
- biometric identifier (finger and voice prints)
- full face photographs and comparable images
- any other unique identifier

1.7 Restrictions on Use and Disclosure.

1.7.1 Generally, the HIPAA Privacy Rules prohibit disclosure of Protected Health Information except in accordance with the regulations. These define and limit the



Cardiovascular Associates of the Delaware Valley, P.A.

*Diagnostic and Interventional Cardiology
Diplomates of the American Board of Internal Medicine & Cardiology*

circumstances under which covered entities may use or disclose Protected Health Information to others. Permissible uses under the HIPAA Privacy Rules generally include three categories:

- (A) Use and disclosure for treatment, payment, and health care operations.
- (B) Use and disclosure with individual authorization.
- (C) Use and disclosure without authorization for specified purposes, including certain government and law enforcement activities.

1.7.2 All of these terms will be further discussed in these Health Privacy Policies and Procedures.

1.8 Summary of Required Administrative Actions. The HIPAA Privacy Rule requires Provider to take certain actions, each of which is described in these Health Privacy Policies and Procedures. In particular, Provider must; (A) appoint a privacy officer who is responsible for HIPAA compliance for Provider; (B) develop and disseminate a privacy notice; (C) develop minimum necessary policies, including appropriate procedures to obtain authorization for releases of Protected Health Information; (D) develop a system for tracking disclosures; (E) develop a procedure to request alternative means of communication; (F) develop a procedure to request a restriction on the use or disclosure of PHI; (G) develop a complaint procedure; (H) develop a procedure to request an amendment of records containing PHI; (I) develop an access, inspection, and copying procedure; (J) develop an anti-retaliation policy; (K) train the workforce; and (L) enter into or amend “business associate” contracts.

Section 2. SCOPE

2.1 Applicability. These Health Privacy Policies and Procedures apply to the collection, use, storage and disclosure of Protected Health Information, as defined by the HIPAA Privacy Rules, by any member of the workforce of Provider. These Health Privacy Policies and Procedures govern Protected Health Information in any format, including electronic, paper and verbal.

2.2 Information Not Within Scope. The following types of information are not considered Protected Health Information, and so are not included within the scope of these Health Privacy Policies and Procedures: (A) Student records covered by the Family Educational Right and Privacy Act (“FERPA”); (B) Employment records held by Provider in its role as an employer (except that records used to administer Provider’s employee health benefit plans are covered); (C) Workers compensation records; and (D) Disability and life insurance policies.

2.3 De-Identified Information.

2.3.1 Health information that does not identify an individual, and where there is no “reasonable basis” to believe that the information could be used to identify the individual, is not subject to these Health Privacy Policies and Procedures (i.e. is “de-identified information”).



Cardiovascular Associates of the Delaware Valley, P.A.

*Diagnostic and Interventional Cardiology
Diplomates of the American Board of Internal Medicine & Cardiology*

2.3.2 There are two mechanisms to de-identify health information so that it is not covered by these Health Privacy Policies and Procedures: (A) A person with appropriate knowledge and experience, applying generally accepted statistical and scientific principles and methods for rendering information not individually identifiable, determines and documents that the risk is “very small” that the information (either alone or in combination with other reasonably available information) could be used to identify an individual; or (B) eighteen (18) specific identifiers are removed regarding the individual, and the individual’s relatives, employers, or household members.¹

2.4 Marketing and Research Activities Prohibited. Protected Health Information entrusted to Provider shall not be used for Marketing or Research activities without the prior written approval of the Privacy Officer.

Section 3. PROVIDER PERSONNEL AND ADMINISTRATIVE MATTERS

3.1 Privacy Officer.

3.1.1 Purpose. The HIPAA Privacy Rules require covered entities, including Provider, to designate a privacy officer who is responsible for the development and implementation of privacy policies and procedures. 45 CFR § 164.530(a)(1).

3.1.2 Policy.

(A) Provider’s Compliance Committee will appoint a Privacy Officer for Provider. The same individual who serves as the Provider’s Compliance Officer will serve as the Provider’s Privacy Officer. The current Privacy Officer is Dr. Kartik Giri.

(B) The Privacy Officer will oversee all ongoing activities related to the development, implementation, maintenance of, and adherence to these Health Privacy Policies and Procedures by Provider.

3.1.3 Privacy Officer Responsibilities. The role of the Privacy Officer is to:

¹ (1) Names; (2) all geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code and equivalent geocodes, except for the initial three digits of a zip code if, according to current Census data, the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; (3) the initial three digits of a zip code for all geographic units containing 20,000 or fewer people is changed to 000; (4) all elements of dates (except year) for dates directly related to an individual including birth date, admission date, discharge date, date of death, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older; (5) telephone numbers; (6) fax numbers; (7) electronic mail addresses; (8) Social Security numbers; (9) medical records numbers; (10) health plan beneficiary numbers; (11) account numbers; (12) certificate/license numbers; (13) vehicle identifiers and serial numbers, including license plate numbers; (14) device identifiers and serial numbers; (15) Web Universal Resource Locator (URL); (16) internet protocol (IP) address number; (17) biometric identifiers, including finger or voice prints; (18) full face photographic images and any comparable images; (19) any other unique identifying number, characteristic or code.



Cardiovascular Associates of the Delaware Valley, P.A.

*Diagnostic and Interventional Cardiology
Diplomates of the American Board of Internal Medicine & Cardiology*

(A) Provide guidance and assist in the implementation and maintenance of these Health Privacy Policies and Procedures.

(B) Serve in a leadership role for privacy activities.

(C) Ensure compliance with these Health Privacy Policies and Procedures, and consistent application of sanctions for failure to comply with these Health Privacy Policies and Procedures policies for all individuals in Provider's workforce using Protected Health Information on behalf of Provider.

(D) Ensure that Provider has and maintains copies of Provider's HIPAA forms and materials reflecting current policies and procedures.

(E) Oversee delivery of privacy training to all Provider personnel who may have access to PHI information on behalf of Provider.

(F) Oversee delivery of guidance to contractors, business associates, and other appropriate third parties.

(G) Oversee response of Provider to requests for access, amendment, accounting of disclosures, complaints, restrictions on use, disclosures, and communication to alternative location, and ensure such responses are consistent with these Health Privacy Policies and Procedures.

(H) Initiate, facilitate and promote activities to foster information privacy awareness within Provider and with Business Associates.

(I) Serve as a liaison to Business Associates, where necessary, and participate in implementation of Business Association Agreements with Business Associates.

(J) Review information security plans to ensure alignment between security and privacy practices.

(K) Work with personnel involved in release of Protected Health Information, to ensure full coordination and cooperation under these Health Privacy Policies and Procedures.

3.2 Incident Response Plan. State and federal laws require that individuals be notified of Privacy Incidents concerning their Protected Health Information. As a result, the Provider must identify and investigate all incidents involving Protected Health Information to determine if there has been a breach and if a notice obligation is triggered. It is imperative that Privacy Incidents be identified and reported immediately upon the Provider's becoming aware of them.

3.2.1 A Privacy Incident is a security breach involving Protected Health Information.



Cardiovascular Associates of the Delaware Valley, P.A.

*Diagnostic and Interventional Cardiology
Diplomates of the American Board of Internal Medicine & Cardiology*

3.2.2 Policy. Any personnel who become aware of facts or circumstances that may involve the improper, unauthorized, accidental or unlawful collection, access, use, alteration, loss or disclosure of Protected Health Information should immediately report them to the Privacy Officer. The Privacy Incident must thereafter be reported to the Compliance Committee or its designee within twenty-four hours.

(A) The Compliance Committee or its designee will then determine and/or verify:

- Whose Protected Health Information and which elements of that Protected Health Information were disclosed or affected;
- To whom the information was disclosed, or the possible parties who might have access to the information;
- The nature of the incident (e.g., accidental loss, unauthorized access, etc.);
- The date and time the incident took place;
- Whether the current use and processing of the Protected Health Information must be stopped immediately; and
- Whether the breach involved an event which resulted in contacting law enforcement, or should have resulted in contacting law enforcement.

(B) Upon completion of its initial determination, the Compliance Committee or its designee will:

- Contact Counsel, who will advise as to the proper course of immediate action to limit the scope of the incident;
- If necessary, conduct a follow-up investigation, including interviews and retrieval of copies where appropriate;
- Determine what steps are required as a result of the incident and, if necessary, a timeline in which to complete the investigation and take any actions required by law, the Plan, or any Business Associate Agreement in place; and
- Determine if it is necessary or appropriate to notify the patient about the Privacy Incident involving his or her Protected Health Information.



Cardiovascular Associates of the Delaware Valley, P.A.

*Diagnostic and Interventional Cardiology
Diplomates of the American Board of Internal Medicine & Cardiology*

(C) Any questions regarding this Incident Response Plan should be brought to the attention of the Privacy Officer.

3.3 Prohibition Against Retaliatory Acts.

3.3.1 Purpose. Provider is committed to preventing retaliation against individuals for exercising their rights under HIPAA, and other applicable federal and New Jersey laws and regulations.

3.3.2 Policy. Provider and members of Provider's workforce will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual who: (A) exercises any right under these Health Privacy Policies and Procedures or Provider's Notice of Privacy Practices, including the filing of a complaint; (B) testifies, assists or participates in an investigation, compliance review, proceeding or hearing related to Provider's privacy practices; or (C) opposes any act or practice that is illegal under the HIPAA Privacy Rules, provided that the individual has a good faith belief that the challenged practice is unlawful, and the manner of challenge is reasonable and does not involve a disclosure of Protected Health Information.

3.3.3 Procedure. If a member of Provider's workforce becomes aware of a violation of the policy set forth in Section 3.3.2, the member of Provider's workforce shall report that information to the Privacy Officer, and Provider shall take appropriate action to ensure compliance with the policy set forth in Section 3.3.2.

3.4 Discipline. Each member of Provider's workforce must strictly adhere to these Health Privacy Policies and Procedures. Provider views any violation of these Health Privacy Policies and Procedures as a serious matter. Provider will apply appropriate discipline, up to and including dismissal, against members of its workforce who fail to comply with these Health Privacy Policies and Procedures.

3.5 Training and Education.

3.5.1 Purpose. The HIPAA Privacy Rules require that a covered entity train all members of its workforce, who have access to Protected Health Information, concerning the requirements of the HIPAA Privacy Rules, as necessary and appropriate for the members of the workforce to carry out their job functions. This policy is designed to give guidance and ensure compliance with the training requirement.

3.5.2 Policy. Provider will provide training to its workforce in accordance with the HIPAA Privacy Rules. 45 CFR § 164.530.

3.5.3 Procedure.

(A) All members of Provider's workforce who have access to or use Protected Health Information shall receive training regarding the requirements of the HIPAA Privacy Rules and these Health Privacy Policies and Procedures.

(B) Training will be provided:



Cardiovascular Associates of the Delaware Valley, P.A.

*Diagnostic and Interventional Cardiology
Diplomates of the American Board of Internal Medicine & Cardiology*

(1) Immediately to all individuals who are members of Provider's workforce on the date these Health Privacy Policies and Procedures are issued and who have access to Protected Health Information.

(2) To each new member of the workforce with access to Protected Health Information within a reasonable period of time after the person joins the workforce.

(3) To each member of the workforce whose functions are affected by a material change in these policies or procedures required, within a reasonable period of time after the material change becomes effective.

(C) Attendance at training sessions must be documented by the Privacy Officer to demonstrate that each member of the workforce with access to Protected Health Information has received training in accordance with this policy. Records of such training must be retained for at least six (6) years.

Section 4. NOTICE OF PRIVACY PRACTICES

4.1 Purpose. The HIPAA Privacy Rules require that notice be given to individuals concerning the use and disclosure of Protected Health Information, as well as the individual's rights and a covered entity's legal duties with respect to Protected Health Information. This policy is designed to give guidance and to ensure compliance with the Notice of Privacy Practices requirements. 45 CFR § 164.520.

4.2 Policy.

4.2.1 Provider will give adequate notice to individuals regarding the use and/or disclosure of their Protected Health Information, their rights with respect to such use and/or disclosure, and Provider's legal duties pursuant to the HIPAA Privacy Rules. 45 CFR § 164.520.

4.2.2 The content of the notice regarding the use and disclosure of Protected Health Information shall comply with the requirements of the HIPAA Privacy Rules. 45 CFR § 164.520.

4.2.3 The Notice will be provided in accordance with the HIPAA Privacy Rules. 45 CFR § 164.520.

4.3 Procedure – Content of Notice; Revisions.

4.3.1 Provider shall use the form of Notice of Privacy Practices attached to these Health Privacy Policies and Procedures and titled "Notice of Privacy Practices for Protected Health Information" and numbered HIPAA Form 1.

4.3.2 Provider shall revise the Notice whenever there is a material change in its uses and/or disclosures of Protected Health Information, individuals' rights, Provider's legal duties, or other privacy practices stated in the Notice. If the Notice of Privacy Practices is



Cardiovascular Associates of the Delaware Valley, P.A.

*Diagnostic and Interventional Cardiology
Diplomates of the American Board of Internal Medicine & Cardiology*

revised, the Privacy Officer will ensure that the form of Notice is updated and distributed appropriately.

4.4 Procedures – Distribution.

4.4.1 The Notice will be provided to individuals with whom Provider has a direct treatment relationship as follows:

(A) No later than the date of the first service delivery, including service delivered electronically, to such individual after April 14, 2003.

(B) Upon request.

(C) On or after the effective date of a revision.

(D) Promptly, at the service delivery site for individuals to request and to take with them.

(E) By posting in a clear and prominent location where it is reasonable to expect individuals seeking services from Provider will be able to read the Notice.

4.4.2 Provider will make a good faith effort to obtain a written acknowledgment that the Notice has been offered to each patient. If the patient's acknowledgement cannot be obtained, Provider shall document what efforts were taken to obtain such acknowledgment and the reason why the acknowledgment was not obtained. See Provider's form of Acknowledgement attached to these Health Privacy Policies and Procedures, titled "Acknowledgment of Receipt of Notice of Privacy Practices" and numbered HIPAA Form 2.

4.4.3 Provider will prominently post its notice on any Web site that it maintains that provides information about its services or benefits, and will make the notice available electronically through the Web site.

4.4.4 Provider will document compliance with this policy by retaining a copy of its form of notice for a period of at least six years from the date of its creation or from the date when it was last in effect, whichever is later, and by keeping a copy of all Acknowledgement forms for a period of six years from completion of the form.

Section 5. MINIMUM NECESSARY STANDARD

5.1 Purpose. Section 6 of this Privacy Policy explains under what circumstances Provider may use and disclose an individual's protected health information. If a use or disclosure is permitted by Section 6 of this Privacy Policy, the member of Provider's workforce must still limit the amount of protected health information used or disclosed to the minimum necessary amount. In essence, the Privacy Rule establishes a "need to know" limitation. This rule does not apply to uses or disclosures for treatment purposes. 45 CFR § 164.502(b).



Cardiovascular Associates of the Delaware Valley, P.A.

*Diagnostic and Interventional Cardiology
Diplomates of the American Board of Internal Medicine & Cardiology*

5.2 Policy.

5.2.1 The Compliance Committee will determine THE HEART HOUSE-CADV personnel's electronic and manual access to Protected Health Information on an individual basis guided by the scope and responsibilities of each individual's position.

5.2.2 Routine disclosures of Protected Health Information will be limited to the minimum necessary to meet the purpose of the disclosure. While the HIPAA Privacy Rules have a number of exceptions to the "minimum necessary" standard, in all cases members of Provider's workforce should consider what Protected Health Information is necessary to accomplish their task and only use the information they determine to be required.

5.3 Entire Record. Members of Provider's workforce may not use, disclose, or request a patient's entire record unless such use, disclosure or request is specifically justified as the amount of patient information that is reasonably necessary to accomplish the purpose of the use, disclosure or request.

5.4 Requests from Others. In the following instances, Provider may rely on a request from another entity for Protected Health Information as representing the minimum necessary for the stated purpose, if such reliance is reasonable under the circumstances:

5.4.1 The request is from a public official, such as a representative of a government regulatory agency or a law enforcement official.

5.4.2 The information is requested by another HIPAA covered entity; or

5.4.3 The information is requested by a professional (i.e., a lawyer or an accountant) who is a business associate of Provider; and

(A) The purpose is to provide professional services to Provider; and

(B) The professional represents that the information requested is the minimum necessary for the stated purpose.

5.5 Exceptions to the Minimum Necessary Standard.

5.5.1 There are a number of exceptions to the "minimum necessary" standard. For the following types of uses and disclosures, the minimum necessary rule does not apply:

(A) Disclosures to or requests by a health care provider for treatment.

(B) Disclosures made to the individual who is the subject of the information.

(C) Disclosures to third parties that are requested by the individual using an authorization.



Cardiovascular Associates of the Delaware Valley, P.A.

*Diagnostic and Interventional Cardiology
Diplomates of the American Board of Internal Medicine & Cardiology*

(D) Disclosures made to the Secretary of the U.S. Department of Health and Human Services that are related to compliance with and enforcement of HIPAA.

(E) Uses and disclosures that are required by law, so long as any restrictions provided by law are complied with.

5.6 Procedure.

5.6.1 For each use and disclosure of Protected Health Information, members of Provider's workforce will determine whether a use or disclosure is limited to the amount of Protected Health Information necessary to achieve the purpose of the use or disclosure.

- Where a use or disclosure is routine or recurring, personnel shall consult with the Privacy Officer, who will develop guidelines that limit the amount of Protected Health Information to that which is necessary to achieve the purpose of the use or disclosure.

Section 6. USE AND DISCLOSURE

6.1 Purpose. The HIPAA Privacy Rules prescribe when a covered entity, including Provider, may use or disclose Protected Health Information. 45 CFR §§ 164.506, 164.508, 164.510 and 164.512.

6.2 Policy. Provider may use and disclose Protected Health Information for treatment, payment, health care operations, and certain activities that are in the public interest, without permission from the individual. In addition, for disclosures to close family and friends that are directly involved in the individual's care, and for disclosures of a patient's location in a facility directory, written authorization is not required, but the individual must have an opportunity to object, either orally or in writing. For all other uses and disclosures, Provider must obtain specific permission from the individual in the form of a HIPAA-compliant authorization.

6.3 Permitted Uses and Disclosures. Provider may use and disclose Protected Health Information in the following circumstances without any permission from the individual:

6.3.1 For treatment, payment, and Provider's health care operations.

6.3.2 For certain activities that are in the public interest that are listed in Section 6.4.

6.3.3 To a relative or close friend that is directly involved with the patient's care where the individual has had an opportunity to object to this disclosure, either orally or in writing, and has not objected. An opportunity to object is not necessary if the situation is an emergency or the individual lacks the capacity to object.

6.3.4 When Protected Health Information is requested by the Secretary of HHS to investigate or determine the covered entity's compliance with the Privacy Rule.



Cardiovascular Associates of the Delaware Valley, P.A.

*Diagnostic and Interventional Cardiology
Diplomates of the American Board of Internal Medicine & Cardiology*

6.3.5 Although probably not relevant to Provider's operations, for a facility directory (if any) if the individual has had an opportunity to object to this disclosure, either orally or in writing, and has not objected.

6.4 Uses and Disclosures in the Public Interest.

6.4.1 For each of the types of uses and disclosures described in this Section 6.4, special rules may apply. Therefore, the Privacy Officer should be consulted before disclosing Protected Health Information under any of these exceptions. In addition, these types of disclosures must be tracked as described in Section 7, so that an accounting of these disclosures may be made to the individual upon request.

6.4.2 The following uses and disclosures are permitted without patient authorization:

(A) Uses and disclosures as required by law.

(B) Disclosures to a public health authority to collect information for the purpose of preventing or controlling disease, injury, or disability, including the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions.

(C) Disclosures to a public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect.

(D) Disclosures about victims of abuse, neglect, or domestic violence, to specified authorities in abuse situations other than those involving child abuse or neglect, such as spousal abuse or abuse of elderly residents of a nursing home.

(E) Disclosures to another person who may have been exposed to a communicable disease, if Provider is authorized by law to notify that person in conducting a public health intervention or investigation.

(F) Disclosures to a health oversight agency for health oversight activities that are authorized by law, such as an audit, an investigation, and activities to determine compliance with program standards.

(G) Disclosures in judicial and administrative proceedings. Special rules apply where a subpoena or discovery request is not accompanied by a court order (see Section 18 of this Privacy Policy).

(H) Disclosures to a law enforcement official for various law enforcement purposes if certain conditions are met.

(I) Uses and disclosures about decedents to coroners, medical examiners and funeral directors.



Cardiovascular Associates of the Delaware Valley, P.A.

*Diagnostic and Interventional Cardiology
Diplomates of the American Board of Internal Medicine & Cardiology*

- (J) Uses and disclosures for cadaveric organ, eye or tissue donation.
- (K) Uses and disclosures to avert a serious and imminent threat to health or safety.
- (L) Uses and disclosures for specialized government functions, including military and veterans activities.
- (M) Disclosures to the extent necessary to comply with laws relating to workers' compensation.
- (N) Disclosure of Protected Health Information in disaster situations.
- (O) Disclosures to correctional institutions or law enforcement officials with lawful custody of an inmate, where the correctional institution or law enforcement official has represented to Provider that the information is necessary to provide health care to the individual, for the health and safety of such individual, other inmates, employees or others at the correctional institution, and for the administration and maintenance of the safety and security of the institution.
- (P) Disclosures to another government agency administering a program providing public benefits, if the sharing of the information or the maintenance of the information in a single or combined data system accessible to both government agencies is authorized by law, or if sharing information among agencies is necessary to improve the function of the program.

6.5 Authorization to Use or Disclose Protected Health Information.

6.5.1 Policy.

- (A) A written authorization, signed by the patient, or the patient's personal representative, is required to permit Provider personnel to use or disclose that the patient's Protected Health Information in any circumstance that is not identified in Section 6.3 and 6.4.
- (B) In addition, authorization is specifically required:
 - (1) For most uses and disclosures of psychotherapy notes; and
 - (2) For any marketing (but see Section 2.4 concerning prohibition on marketing activities).

6.5.2 Provider Authorization Form.

- (A) The written authorization should be in the form prescribed by Provider. See Provider's form of Authorization attached to these Health Privacy Policies and



Cardiovascular Associates of the Delaware Valley, P.A.

*Diagnostic and Interventional Cardiology
Diplomates of the American Board of Internal Medicine & Cardiology*

Procedures, titled “Authorization to Use and/or Disclose Health Information” and numbered HIPAA Form 11.

(B) Provider personnel should not accept forms of Authorizations other than Provider’s Authorization form (HIPAA Form 11) without prior review and approval by the Privacy Officer.

6.5.3 HIPAA Authorization Checklist. If an authorization other than Provider’s Authorization form is to be used, in order to be a valid Authorization under the HIPAA Privacy Rules, an Authorization must:

- (A) Be written in plain language.
- (B) Be signed and dated by the patient or a legally authorized representative (e.g. a parent, guardian, person with power or attorney).
- (C) Contain a specific and meaningful description of the Protected Health Information to be used or disclosed.
- (D) List the name or specific identification of the persons or types of persons who are authorized to use or disclose the protected health information under the authorization.
- (E) List the name or specific identification of the persons or types of persons to whom the protected health information may be disclosed.
- (F) Contains a description of each purpose of the requested use or disclosure. The statement “at the request of the individual” is a sufficient description of the purpose when the patient initiates the authorization and does not, or elects not to, provide a statement of the purpose.
- (G) Contains a statement of when the authorization will expire (either a date or an event) that relates to the individual or the purpose of the use or disclosure.
- (H) Contains a statement that the patient may revoke the Authorization in writing at any time, including instructions on how to exercise this right.
- (I) Lists any exceptions to the patient’s right to revoke the authorization.
- (J) Contains a statement of the consequences, if any, of not signing the authorization.
- (K) Contains a statement that a decision not to sign the authorization or to revoke the authorization after it is signed will not affect the patient’s access to treatment, payment, enrollment or eligibility for benefits, or other legal rights to which he is otherwise entitled.



Cardiovascular Associates of the Delaware Valley, P.A.

*Diagnostic and Interventional Cardiology
Diplomates of the American Board of Internal Medicine & Cardiology*

(L) Contains a statement that once the protected health information is disclosed under the authorization, it may no longer be protected by HIPAA.

6.5.4 When is an Authorization invalid? An Authorization is invalid if:

(A) It does not comply in all respects with Provider's Authorization form; or

(B) One or more required elements is not completed or does not clearly express the patient's desires (See Authorization checklist in Section 6.5.3); or

(C) It has been revoked by the patient to whom the Protected Health Information pertains, or by a personal representative authorized to act on the patient's behalf; or

(D) It has expired, based on the expiration date or event; or

(E) Any material information contained in it is known by Provider to be false.

6.5.5 Authorizations Must Be In Writing; Faxed Authorization Acceptable.

Provider may accept a fax or other paper copy of an authorization that otherwise meets the requirements of this Section 6.5. An authorization that has been e-mailed or is otherwise in electronic form is not acceptable. In addition, oral authorization from a patient is not acceptable. All authorizations must be in writing.

6.5.6 Disclosure pursuant to an Authorization.

Any use or disclosure under the terms of an authorization must be consistent with the provisions of that authorization.

6.5.7 Records of Authorizations.

Each Authorization must be in writing and will be filed with the patient's record. Authorizations must be retained for at least six years after the date they cease to be in effect (either because they expired or were revoked.)

6.5.8 Revocation of Authorizations.

A patient may revoke an Authorization at any time, except to the extent that Provider has taken action in reliance on the Authorization. The revocation must be in writing, and must be specific enough to permit identification of the authorization that is being revoked.

6.5.9 Authorization as Precondition to Treatment.

Provider will not require an Authorization as a precondition to treatment except in the following circumstances as described in this paragraph. If the treatment is research-related, provision of treatment may be conditioned on receipt of an authorization to use and disclose PHI related to the treatment as necessary for the research. Also, if the purpose of the treatment is to create Protected Health Information for disclosure to a third party (e.g., for a fitness for duty determination at the request of the employer), provision of the treatment may be conditioned on receipt of an authorization to disclose the PHI to that third party.



Cardiovascular Associates of the Delaware Valley, P.A.

*Diagnostic and Interventional Cardiology
Diplomates of the American Board of Internal Medicine & Cardiology*

6.5.10 The Minimum Necessary Rule does not limit the amount of information which may be used or disclosed under an authorization.

6.5.11 Procedure.

(A) Requests for uses and disclosures of Protected Health Information without written Authorization (except as otherwise provided in these Health Privacy Policies and Procedures) will be directed to the Privacy Officer. The Privacy Officer will review such requests in accordance with applicable Provider policies, and respond with a determination as to whether the requested use or disclosure is permitted under Provider policy and federal and state law without authorization from the individual, or whether a written authorization from the patient is required. If the Privacy Officer determines that an authorization is required prior to the requested use or disclosure, an authorization that complies with this policy must be obtained.

(B) When a written authorization to use or disclose PHI is presented by or on behalf of a patient, the authorization document will be reviewed using the checklist attached for compliance with Provider policy regarding the content of authorization forms. This includes determining whether the correct form has been used and whether all required elements have been completed.

(C) If the authorization document does not comply, it is not valid and will be returned to the person from whom it was received, with a cover letter explaining the reason it was rejected, and inviting the patient to submit the authorization in the form approved by Provider (HIPAA Form 11). A copy of Provider's Authorization form will be included with the letter. A copy of the returned form and the cover letter will be filed in the patient's record and retained for at least six years.

(D) If the authorization document does comply, the requested information will be released in accordance with the provisions of the authorization form, using Provider's current policies regarding the copying and mailing of patient records. The original authorization form will be filed in the patient's record and retained for at least six years. A notation will be made in the patient's record to identify which information was disclosed, the date, the recipient, and the reason.

(E) Any patient who wishes to revoke an authorization to use or disclose PHI will be instructed to submit a request in writing to the Privacy Officer and that the request must be specific enough to permit identification of the authorization that is being revoked. The Privacy Officer will notify the appropriate personnel that it has been revoked, and will determine the extent to which action has been taken in reliance upon the authorization. The Privacy Officer will prepare directions regarding how the patient's PHI is to be handled following the revocation. This may include no further action pursuant to the authorization, or action to the extent that it is permitted because Provider has already relied upon the authorization.



Cardiovascular Associates of the Delaware Valley, P.A.

*Diagnostic and Interventional Cardiology
Diplomates of the American Board of Internal Medicine & Cardiology*

6.6 Verification Requirements.

6.6.1 Policy. Prior to any disclosure of Protected Health Information, Provider will take reasonable steps to verify the identity of the person requesting Protected Health Information and the authority of that person to have access to the Protected Health Information.

6.6.2 Procedures.

(A) Verify Identities. Members of Provider workforce who authorize the disclosure of PHI shall take reasonable steps to:

(1) Verify the identity of the person to whom the PHI is disclosed; and

(2) Verify the person's authority to receive the PHI.

(B) Reasonable Steps. Reasonable steps include the following, depending on the circumstance:

(1) If the worker knows the identity and authority of the recipient of the PHI, no further documentation is necessary.

(2) If the person does not, the following steps should be taken:

(a) If the person requesting the information is requesting their own information, confirm their address and social security number from information in the file; or

(b) If the person whose PHI is at issue is present or otherwise available prior to disclosure, the patient must be given the opportunity to agree or object to the disclosure. If the person is requesting the information is a third person, you need to:

(i) Ascertain the authority of that person to obtain the information. If you are unclear as to their authority, ask the requesting party to contact the individual whose health information is to be disclosed to call you to authorize the release;

(ii) Confirm the identity of the recipient by address, social security number or other identifying information from the file.

(3) If the person requesting Protected Health Information is a public official, Provider may rely upon the following to verify their identity:

(a) Presentation of an agency identification badge, credentials, or other proof of status.



Cardiovascular Associates of the Delaware Valley, P.A.

*Diagnostic and Interventional Cardiology
Diplomates of the American Board of Internal Medicine & Cardiology*

(b) Requests made on appropriate governmental letterhead.

(c) A written statement of the legal authority (or, if impracticable, an oral statement) under which the information is requested.

(d) If a request is made pursuant to a warrant, subpoena, court order, or other legal process, it is presumed to constitute legal authority.

(C) These verification requirements are met if Provider relies on the exercise of professional judgment in making a use or disclosure, or acts on a good faith belief in making a disclosure regarding serious threats to health or safety.

Section 7. ACCOUNTING OF DISCLOSURES

7.1 Purpose.

Under the HIPAA Privacy Rules, individuals have a right to receive an accounting of certain types of disclosures of their Protected Health Information. Provider has developed general policies and procedures to address the accounting of instances when Protected Health Information has been used or disclosed for purposes other than treatment, payment, health care operations, or pursuant to an individual authorization. 45 CFR § 164.528.

7.2 Policy.

7.2.1 Provider will keep an accounting of all disclosures by Provider for any of the purposes set forth in Section 6.4, and provide such accounting to individuals upon written request.

7.2.2 Provider will not track the following types of disclosures:

- (A) To carry out treatment, payment and health care operations.
- (B) To the individual of his or her own Protected Health Information.
- (C) Pursuant to an authorization from the individual.
- (D) To notify relatives and close friends who are involved in the individual's care, including the individual's personal representative.
- (E) For national security or intelligence purposes.
- (F) To correctional institutions or law enforcement officials regarding inmates or individuals in custody.
- (G) To disaster relief agencies as directed by the Privacy Officer.
- (H) That occurred prior to April 14, 2003.



Cardiovascular Associates of the Delaware Valley, P.A.

*Diagnostic and Interventional Cardiology
Diplomates of the American Board of Internal Medicine & Cardiology*

7.2.3 If requested by a regulatory agency or law enforcement official, Provider may temporarily suspend an individual's right to an accounting of disclosures made to such regulatory agency or law enforcement official, so long as:

(A) The regulatory agency or law enforcement official provides Provider with a written statement that notifying the patient of a disclosure to the agency/official would be reasonably likely to impede the activities of the agency or official. The statement must specify the time period during which the patient is not to be informed of the disclosure.

(B) If the agency is not able to produce a written statement immediately, Provider may act upon an oral statement for a period of no more than 30 days. The oral statement, including the identity of the agency and/or official making the request, must be documented.

(C) The suspension of the patient's right to an accounting of the disclosure of Protected Health Information to the agency is only temporary, lasting only for the period of time requested in the written statement (or for no more than 30 days if no written statement is produced by the agency).

7.3 Procedure.

7.3.1 Tracking Disclosures.

(A) Provider will track disclosures for the purposes set forth in Section 7.2.2 using the tracking form attached to these Health Privacy Policies and Procedures, titled "Internal Accounting of Disclosures of Protected Health Information," and numbered HIPAA Form 3.

(B) Whenever a disclosure is made for one of the purposes set forth in Section 7.2.2, the member of Provider workforce who makes the disclosure will document the disclosure on the "Internal Accounting of Disclosures of Protected Health Information" form (HIPAA Form 3) and insert the completed copy of the form in the patient's record.

(C) The tracking form will account for the following:

- (1) the date of the disclosure;
- (2) the name of the entity or person who received the PHI, and, if known, the address of that entity or person;
- (3) a brief description of the PHI disclosed; and
- (4) a brief statement of the purpose of the disclosure.

(D) Where Provider makes multiple disclosures to the same person, company or agency for the same purpose over time, and where the Privacy Officer deems such



Cardiovascular Associates of the Delaware Valley, P.A.

*Diagnostic and Interventional Cardiology
Diplomates of the American Board of Internal Medicine & Cardiology*

course of conduct to be reasonable, Provider may track only the following information, instead of tracking each disclosure as outlined in paragraphs 1-3 above:

- (1) the information in paragraph 1.3 above for the first disclosure during the accounting period;
- (2) the frequency of disclosures made during the accounting period; and
- (3) the date of the last disclosure during the accounting period.

7.4 Responding to a Request for an Accounting.

7.4.1 Any request for an accounting of disclosures of Protected Health Information must be in writing using the form attached to these Health Privacy Policies and Procedures, titled "Request for Accounting of Uses and Disclosures of Protected Health Information," and numbered HIPAA Form 4. The request must be dated and specify the time period for which the accounting applies, which may not be for more than a period of six (6) years.

7.4.2 All requests for accounting of disclosures should be forwarded to the Privacy Officer.

7.4.3 The Privacy Officer will then identify what disclosures must be accounted for, using the tracking mechanisms identified in Section 7.3.1.

7.4.4 Each accounting of disclosures will be in writing and include the following:

- (A) The date of disclosure.
- (B) The name of the entity or person who received the protected health information and, if known, the address of such entity or person.
- (C) A brief description of the Protected Health Information disclosed.
- (D) 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 request for disclosure.

7.4.5 Provider will act on the individual's request for an accounting not later than 60 days after receipt of the request by:

- (A) Providing the individual with the accounting requested; or
- (B) Extending the time to provide the accounting by no more than 30 days.



Cardiovascular Associates of the Delaware Valley, P.A.

*Diagnostic and Interventional Cardiology
Diplomates of the American Board of Internal Medicine & Cardiology*

7.4.6 In the event that Provider extends the time to provide the accounting, within 60 days after receipt of the request, it will provide the individual with a written statement of the reasons for the delay and the date by which the covered entity will provide the accounting.

7.4.7 If appropriate, Provider may impose a reasonable cost-based fee for providing an accounting. If a fee is imposed, Provider will inform the individual in advance of the fee and provide the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

7.4.8 Provider will document and retain the following for a period of at least six years from the date of its creation:

- (A) The information required to be included in an accounting; and
- (B) The written accounting that is provided to the individual.

Section 8. ALTERNATIVE MEANS OF COMMUNICATION

8.1 Purpose.

Under the HIPAA Privacy Rules, individuals may request to receive communications regarding their Protected Health Information by an alternative means (e.g., by mail rather than by telephone) or at an alternative location (e.g., at work rather than at home). 45 CFR § 164.522(b)(1).

8.2 Policy.

Provider will accommodate all reasonable requests by individuals to receive confidential communications of Protected Health Information by alternatives means or at an alternative location.

8.3 Procedure.

8.3.1 Requests for confidential communications must be made in writing using the form attached to these Health Privacy Policies and Procedures, titled "Request for Alternative Means of Communication," and numbered HIPAA Form 5.

8.3.2 All requests for confidential communications should be forwarded to the Privacy Officer.

8.3.3 An alternative means or location that is satisfactory to Provider and the individual will be designated on a case by case basis before a communication of Protected Health Information is made.

8.3.4 Provider shall respond to the individual notifying him or her in writing that the request has been received and whether Provider will comply with the request.



Cardiovascular Associates of the Delaware Valley, P.A.

*Diagnostic and Interventional Cardiology
Diplomates of the American Board of Internal Medicine & Cardiology*

8.3.5 Provider shall retain a copy of all requests for confidential communications in the patient's record, along with a written indication of whether the request was granted, so that personnel know whether to communicate with such patient in accordance with such request.

Section 9. REQUESTING RESTRICTIONS ON USES AND DISCLOSURES

9.1 Purpose.

The HIPAA Privacy Rules provide an individual with the right to request a restriction on the use and disclosure of his/her Protected Health Information. An example of a restriction might be where an individual's neighbor is an employee or independent contractor of Provider, and that individual requests that his or her neighbor not have access to his/her Protected Health Information. If Provider agrees to the requested restriction, it may not use or make a disclosure in a manner that is inconsistent with that restriction, unless such use or disclosure is mandated by law. 45 CFR § 164.522(a).

9.2 Policy.

Provider will allow an individual to request that uses and disclosures of their Protected Health Information be restricted. Provider will agree to reasonable and feasible restrictions. This provision does not apply to using and disclosing Protected Health Information to provide health care to an individual on an emergency basis.

9.3 Procedure.

9.3.1 Provider will allow an individual to request restrictions on the use and disclosure of Protected Health Information. Any such request must be in writing using the form attached to these Health Privacy Policies and Procedures, titled "Request for Restriction on Use and Disclosure of Protected Health Information," and numbered HIPAA Form 6.

9.3.2 All requests for restrictions should be forwarded to the Privacy Officer. The Privacy Officer will determine whether the request is reasonable and feasible, and will decide whether to grant or deny the request.

9.3.3 Whether the request has been accepted or denied should be indicated on the request form, and the form should be filed in the patient's record. Provider shall respond to the patient, notifying him or her in writing that the request has been received and whether Provider will comply with the restriction.

9.3.4 Upon agreeing to such a restriction, Provider will comply with the restriction, unless specified below.

9.3.5 Provider is not required to honor an individual's request in the following situation(s):



Cardiovascular Associates of the Delaware Valley, P.A.

*Diagnostic and Interventional Cardiology
Diplomates of the American Board of Internal Medicine & Cardiology*

(A) When the individual who requested the restriction is in need of emergency treatment and the restricted Protected Health Information is needed to provide the emergency treatment.

(B) If restricted Protected Health Information is disclosed to a health care provider for emergency treatment, Provider will request that such health care provider not further use or disclose the information.

9.3.6 If Provider agrees to an individual's requested restriction, the restriction nevertheless will not apply to the following types of uses and disclosures:

(A) To an individual accessing his or her own Protected Health Information.

(B) To an individual requesting an accounting of his or her own Protected Health Information.

(C) Uses and disclosures for judicial and administrative purposes; health oversight; research; law enforcement; public health, to avert a serious threat to health and safety; cadaveric organ, eye, or tissue donation; to coroner/medical examiner or funeral director; Worker's Compensation; reporting of abuse, neglect or domestic violence; specialized government functions or other instances required by law.

9.3.7 Provider may terminate its agreement to a restriction in the following situations:

(A) The individual agrees to or requests the termination in writing.

(B) The individual orally agrees to the termination and the oral agreement is documented in the patient record.

(C) Provider informs the individual that it is terminating its agreement to a restriction. Such termination is only effective with respect to Protected Health Information created or received after informing the individual of the termination.

9.3.8 Documentation of the request for restriction and Provider's response must be maintained in the patient record for at least six years from the date of its creation or the date when it last was in effect, whichever is later.

9.3.9 The termination should be documented on the same form in the patient record that documents the initial request and restriction.



Cardiovascular Associates of the Delaware Valley, P.A.

*Diagnostic and Interventional Cardiology
Diplomates of the American Board of Internal Medicine & Cardiology*

Section 10. SECURITY OF PROTECTED HEALTH INFORMATION

10.1 Purpose.

10.1.1 Under the HIPAA Privacy Rules, Provider is required to have in place appropriate administrative, technical, and physical safeguards to protect the privacy of Protected Health Information. 45 CFR § 164.530(c).

10.2 Policy.

10.2.1 Access. Each member of Provider's workforce is only permitted access to that Protected Health Information that he or she is required to have to do his/her job. No member of Provider's workforce shall attempt to access Protected Health Information in paper files or on computers where he or she does not have the authority to do so.

10.2.2 Paper Files. Members of Provider's workforce who maintain or use Protected Health Information in paper files must take care to return such files to their proper files and cabinets when not in use to help prevent access to Protected Health Information by others who may not have proper authorization to view such information. Files containing Protected Health Information should not be left on desks overnight, but should be returned to their proper cabinets.

10.2.3 Electronic Files. Electronic files and programs containing Protected Health Information must be closed when not in use. All workstations shall have a screen saver and password protection mechanism, with the screen saver set to appear whenever the workstation has not been in use for five minutes or more. Passwords should not be written on notes kept near the workstation. Protected Health Information may only be removed from Provider by electronic media (i.e., on a diskette, CD-Rom, or laptop computer) with specific authorization from the Privacy Officer.

10.2.4 Printers. Documents containing Protected Health Information should be removed from printers located in common areas immediately after such documents are printed. If an employee notes that a document containing Protected Health Information has been sitting on a printer in a common area for longer than an hour, the employee should either bring the document to the person who printed the document (if known) or destroy the document.

10.2.5 Use of E-mail. E-mail is a written means of communication. Employees should not transmit anything in an e-mail message that they are not comfortable writing in a memo. Further, sending an e-mail containing Protected Health Information to a third party is considered a disclosure under HIPAA, and must be done consistent with the requirements for uses and disclosures of Protected Health Information under Section 1.7 of this Policy. Protected Health Information should not be sent outside of the Provider's network unless it is in encrypted form and password protected. Deleting an e-mail message from a screen does not guarantee that it has been deleted from the system, because back-up copies of the e-mail may exist. All members of Provider's workforce should be aware that e-mail must not be used in any way which would result in the compromising of Protected Health Information.



Cardiovascular Associates of the Delaware Valley, P.A.

*Diagnostic and Interventional Cardiology
Diplomates of the American Board of Internal Medicine & Cardiology*

10.2.6 Use of Foreign Disks or Programs. Members of Provider's workforce are required to scan foreign computer diskettes to prevent viruses from invading Provider's computer system if such anti-virus software exists on the employee or independent contractor's work station computer system. If such anti-virus scanning software does not exist on the employee or independent contractor's work station computer, that individual must contact the Privacy Officer prior to using the foreign diskettes. Installation of software onto any Provider computer system that is not licensed to Provider or approved by the Privacy Officer is strictly prohibited.

Section 11. HEALTH INFORMATION AMENDMENT PROCEDURES

11.1 Policy.

Under the HIPAA Privacy Rules, individuals who believe the Protected Health Information in their record is incorrect or incomplete may request an amendment of the information. 45 C.F.R. § 164.526.

11.2 Procedures.

11.2.1 A request by a patient for amendment of his/her Protected Health Information must be made in writing using the form attached to these Health Privacy Policies and Procedures titled "Request for Amendment of Protected Health Information," and numbered HIPAA Form 7.

11.2.2 All Requests for Amendment forms should be forwarded to the Privacy Officer.

11.2.3 Provider will act on the request no later than thirty (30) days after receipt of the request for amendment.

11.2.4 Provided Provider gives the individual written notice of a delay and the reason for the delay, Provider may have a thirty (30) day extension to process the request.

11.2.5 The Privacy Officer, or his/her designee, will evaluate the request upon receipt, and will determine whether it is reasonable to make the requested amendment.

11.2.6 The request may be denied if the Protected Health Information was not created by Provider or is reasonably accurate and complete.

11.2.7 If the request for amendment is granted, this should be indicated on the request form. Provider will make a notation at the site of the information that is being corrected or amended indicating "See amendment form" and will sign and date that notation. The amendment form will be attached to the amended entry and the individual informed that the amendment is accepted. For changes on a computer system, the amendment must be noted via alert, case narrative, or other appropriate mechanism, and the amendment form will be filed in the paper file for the patient.



Cardiovascular Associates of the Delaware Valley, P.A.

*Diagnostic and Interventional Cardiology
Diplomates of the American Board of Internal Medicine & Cardiology*

11.2.8 Copies of the amendment/correction form will be provided by Provider to all business associates or others who have access to the information subject to amendment and who may have relied or might rely on that information to the detriment of the individual.

11.2.9 Notations will be made on the amendment form indicating to whom the amendment form was sent, the date and the staff member who sent the amendment form.

11.2.10 Whenever a copy of the amended entry is disclosed, a copy of the amendment form will accompany the disclosure.

11.2.11 If Provider denies the requested amendment, Provider shall provide the individual with a timely denial that contains the basis of the denial. The denial must also explain the individual's right to (A) file a complaint in accordance with Provider's HIPAA complaint procedures, (B) submit a statement of disagreement to Provider; and (C) request that the amendment request and denial be provided with all future disclosures of the information at issue.

11.2.12 A patient whose request to amend PHI has been denied (in whole or in part) may appeal the denial by submitting a statement of disagreement. This is a statement of the reasons why the patient disagrees with the denial.

11.2.13 If Provider decides to make a requested amendment on the basis of a statement of disagreement, the amendment will be made in accordance with this policy, and the patient will be so notified.

11.2.14 If Provider does not accept the reasoning of the statement of disagreement, it will send the patient a written rebuttal, stating why it is still not accepting the requested amendment.

11.2.15 If the amendment is denied, Provider will identify the information to which the denied request applied, and, where such information is located in the patient record, provide a reference or link to a copy of the patient's request for amendment, the denial letter, any statement of disagreement, and any rebuttal. This applies to both paper and electronic records.

Section 12. RIGHT OF INDIVIDUALS TO ACCESS, INSPECT AND OBTAIN A COPY OF PROTECTED HEALTH INFORMATION

12.1 Purpose.

12.1.1 Under the HIPAA Privacy Rules, an individual has the right to access, inspect and obtain a copy of Protected Health Information in a "designated record set" (i.e., health and billing records that are used to make decisions about an individual) for as long as the information is maintained in the designated record set. 45 C.F.R. § 164.524.



Cardiovascular Associates of the Delaware Valley, P.A.

*Diagnostic and Interventional Cardiology
Diplomates of the American Board of Internal Medicine & Cardiology*

12.2 Policy.

12.2.1 Provider will take necessary steps to address requests from individuals to access, inspect, and/or obtain a copy of their Protected Health Information that is maintained in a designated record set in a timely and professional manner.

12.2.2 In instances where the Protected Health Information is in more than one record set, or at more than one location, Provider will only produce the Protected Health Information in response to a request for access, unless the individual specifies that the information is at more than one location.

12.2.3 An individual does not have the right to access the following types of information:

(A) Psychotherapy notes.

(B) Information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding.

(C) PHI that is not stored in “designated record sets,” such as information contained in files containing peer review or quality assurance information.

12.3 Procedure.

12.3.1 To request access, inspection, or a copy of Protected Health Information, Provider requires that an individual complete the form attached to these Health Privacy Policies and Procedures, titled “Request for Access to Inspect or Copy Protected Health Information,” and numbered HIPAA Form 8.

12.3.2 The individual will be informed that a request for access is required to be in writing.

12.3.3 Upon receipt of a fully completed HIPAA Form 8, the Privacy Officer will act on the request by:

(A) Informing the individual of the acceptance and providing the access requested; or

(B) Providing the individual with a written denial. See Section 12.4, (relating to Denying Access to Inspect and Obtain a Copy of Protected Health Information).

12.3.4 Action on the request must be taken:

(A) No later than 30 days after the request is made; or,

(B) If the request is for Protected Health Information that is not maintained or accessible on-site, no later than 60 days after the request is made.



Cardiovascular Associates of the Delaware Valley, P.A.

*Diagnostic and Interventional Cardiology
Diplomates of the American Board of Internal Medicine & Cardiology*

12.3.5 If Provider cannot take action on a request for access within the relevant time periods, Provider may extend the time required by 30 days.

12.3.6 The individual will be allowed access, inspection, and/or copies of the requested Protected Health Information in a secure and confidential manner, such that the information cannot be accessed by other persons who do not have proper authority to access the information.

12.3.7 Provider will provide the individual with access to the Protected Health Information in the form or format requested by the individual, if it is readily producible in such form or format.

12.3.8 If the requested format is not readily producible, Provider will provide the individual with access to the Protected Health Information in a readable hard copy form or such other form that is readily producible.

12.3.9 If requested by the individual, Provider will arrange with the individual for a convenient time and place to inspect or obtain a copy of the Protected Health Information, or to mail the Protected Health Information.

12.3.10 Appropriate personnel will document the request and delivery of the Protected Health Information in the patient file using the completed HIPAA Form 8.

12.3.11 Provider may charge a fee for providing access under this section. Any fees imposed on the individual for a copy of the Protected Health Information will:

(A) Be collected by Provider at the time of receipt of the request and the proper completion of the request form.

(B) Be reasonable and cost-based.

(C) Be only for the cost of the following:

(1) Copying, including the cost of supplies for and labor of copying, the Protected Health Information requested by the individual.

(2) Postage, when the individual has requested that the copy be mailed.

12.4 Denying Access to Inspect and Obtain a Copy of Protected Health Information.

12.4.1 Provider may deny access in the following circumstances:

(A) The Protected Health Information:

(1) Contains psychotherapy notes;



Cardiovascular Associates of the Delaware Valley, P.A.

*Diagnostic and Interventional Cardiology
Diplomates of the American Board of Internal Medicine & Cardiology*

(2) Contains information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding;

(3) Includes information to which patients may not have access under the terms of the Clinical Laboratory Improvements Act.

(B) Provider is acting under the direction of a correctional institution upon an inmate's request for a copy of the Protected Health Information and obtaining a copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate.

(C) Access to Protected Health Information that was created or obtained by Provider in the course of a research study may be temporarily suspended for as long as the research study is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research, and has been informed that the right of access will be reinstated upon completion of the research.

(D) The individual's access to Protected Health Information that is contained in records that are subject to the Privacy Act, 5 U.S.C. §552a, may be denied, if the denial of access under the Privacy Act would meet the requirements of that law.

(E) The individual's access may be denied if the Protected Health Information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

12.4.2 Provider may also deny access in the following circumstances, but the individual has a right to request a review of such denial by an independent reviewer:

(A) A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to the individual.

(B) The Protected Health Information makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person.

(C) The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

12.5 Denial of Access.

12.5.1 The notice of denial must be in writing and contain all of the following:



Cardiovascular Associates of the Delaware Valley, P.A.

*Diagnostic and Interventional Cardiology
Diplomates of the American Board of Internal Medicine & Cardiology*

- (A) Basis for the denial.
- (B) A statement of any review rights, if applicable.
- (C) A statement of how the patient may complain to Provider or to the Secretary, Department of Health and Human Services. (This will be the same information that is contained in the Notice of Privacy Practices.)

12.5.2 If access is denied because Provider does not maintain the information, the notice of denial must include any information that Provider has regarding the location of the requested information.

12.6 Review of Denial of Access.

12.6.1 A review of denial of access will be conducted by an independent reviewer designated by Provider. The reviewer may not have participated in the original decision to deny access. The decision of the reviewer is final, and is binding on Provider. The referral for review must be prompt, and the reviewer must complete the review within a reasonable period of time. The reviewer will determine if the standards of this policy were properly applied in denying access. Provider will promptly provide written notice of the reviewer's decision to the patient.

12.6.2 The written denial and all supporting documentation should be maintained in the patient's file.

Section 13. COMPLAINT PROCEDURES

13.1 Policy.

Under the HIPAA Privacy Rules, Provider will provide a process for individuals to make complaints to Provider concerning implementation of and compliance with these Health Privacy Policies, or its compliance with the HIPAA Privacy Rule itself. Provider is also required to document all complaints received and their disposition. 45 C.F.R. § 164.530(d).

13.2 Filing a Complaint.

13.2.1 A statement informing individuals of the process to complain about violations of these Health Privacy Policies and Procedures is contained in the "Notice of Privacy Practices," which will be distributed to each individual treated by Provider, consistent with Section 4.

13.2.2 The Notice informs individuals that all complaints should be in writing using the form provided by Provider that is attached to these Health Privacy Policies and Procedures, titled "Complaint Form" and numbered HIPAA Form 9.

13.2.3 All complaints should be forwarded to the Privacy Officer.



Cardiovascular Associates of the Delaware Valley, P.A.

*Diagnostic and Interventional Cardiology
Diplomates of the American Board of Internal Medicine & Cardiology*

13.2.4 Under HIPAA, the individual also has a right to file a complaint with the United States Department of Health and Human Services, Office for Civil Rights at any time.

13.3 Additional Responsibilities.

13.3.1 Provider will assist the individual with filing the complaint, if necessary, and may not limit or interfere with the right to make a complaint in any way.

13.3.2 The Privacy Officer will respond in writing to the individual who made the complaint within five business days of receipt, to notify the individual that the complaint was received and is being evaluated.

13.3.3 The Privacy Officer will date stamp the complaint upon receipt and immediately initiate an investigation of the complaint. The Privacy Officer will gather all relevant documents, meet with or talk to the individual making the complaint, and summarize the findings of the investigation in a written report. Provider will take action under this policy and under other Provider policies and procedures regarding the response to complaints. This includes taking action to mitigate any harm done as a result of the incident that gives rise to the complaint, modifying applicable policies and procedures, and/or retraining personnel. A copy of the written report shall be sent to the Compliance Committee.

13.3.4 The Privacy Officer will make every effort to resolve the complaint by following this procedure. If resolution satisfactory to the patient is not reached, the Privacy Officer will forward the results of the investigation and an explanation of any efforts to resolve the issue to the Compliance Committee within seven (7) business days after receiving the complaint.

13.3.5 If the Privacy Officer cannot resolve the complaint to the satisfaction of the patient, the Compliance Committee or its designee will investigate the individual's complaint, make findings of fact based on the circumstances surrounding the complaint and document whether corrective steps are necessary.

13.3.6 The Compliance Committee shall reach a final disposition within 60 days of receipt of the complaint from the Privacy Officer.

13.3.7 The Compliance Committee or a designee will send a copy of the final disposition to the Privacy Officer. The Privacy Officer will send a copy of the final disposition to the individual and will keep a copy in the patient's file for at least six years.

13.3.8 The Privacy Officer will retain a copy of the final disposition and will keep a log of all complaints and their current disposition.

13.3.9 Provider is bound by the determination of the Compliance Committee.



Cardiovascular Associates of the Delaware Valley, P.A.

*Diagnostic and Interventional Cardiology
Diplomates of the American Board of Internal Medicine & Cardiology*

Section 14. PROTECTED HEALTH INFORMATION FOR DECEDENTS

14.1 Purpose.

The HIPAA Privacy rules require that a covered entity comply with use and disclosure rules for deceased persons. Use and disclosure rules for Protected Health Information of decedents are the same as for any other individual. 45 C.F.R. § 164.502(f).

14.2 Policy. Except for permitted uses where the individual has an opportunity to object, Provider must:

14.2.1 Verify the identity of the person requesting Protected Health Information of a deceased individual and the authority to have access to that information.

14.2.2 Obtain written documentation if disclosure is conditioned on representations in § 164.514 (h).

14.3 Personal Representatives.

An executor or administrator authorized by law to act on behalf of an individual's estate is a personal representative. The representative will be treated as the individual for purposes of disclosure of Protected Health Information.

14.4 Permitted Disclosures.

The following are permitted disclosures of decedent's Protected Health Information:

14.4.1 Disclosures to law enforcement official to alert if death due to criminal conduct.

14.4.2 Disclosures to coroners/medical examiners for identification, cause of death, other duties.

14.4.3 Disclosures to funeral directors as necessary to carry out their duties.

14.4.4 Disclosures to organ/tissue donation procurement agencies.

14.4.5 Disclosure for a research study using decedent's information.

14.4.6 For each of these types of disclosure, the HIPAA Privacy Rules may impose additional requirements. Therefore, the Privacy Officer should be informed prior to disclosing a decedent's Protected Health Information for any of the above purposes.



Cardiovascular Associates of the Delaware Valley, P.A.

*Diagnostic and Interventional Cardiology
Diplomates of the American Board of Internal Medicine & Cardiology*

Section 15. PERSONAL REPRESENTATIVES

15.1 Purpose.

The HIPAA Privacy Rules permit those persons authorized by state law (“Personal Representatives”) to control and access an individual’s Protected Health Information. 45 C.F.R. § 164. 502.

15.2 Policy.

15.2.1 Personal Representatives Generally. In applying these Health Privacy Policies and Procedures relating to the use or disclosure of Protected Health Information, Provider will treat the parent, guardian or other personal representative the same as the individual to whom the Protected Health Information pertains. This includes the right to examine and receive a copy of the individual’s Protected Health Information, to request an amendment of that Protected Health Information, to request an accounting for disclosures of Protected Health Information, and to authorize its disclosure to another.

15.2.2 Exceptions for Minors in Some Circumstances.

(A) When a request for Protected Health Information is from a parent, guardian, other person acting in loco parentis of an unemancipated minor, the following exceptions apply. For convenience, parents, guardians, other persons acting in loco parentis are referred to collectively as “parent,” and the word is italicized to emphasize that this is intended to be read as a collective term that includes guardians and others acting in loco parentis).

(B) If the minor may lawfully receive a given health care service without the consent of a parent (regardless of whether someone else has given consent or not), a parent of that minor will not be treated as a personal representative for purposes of Protected Health Information related to that health care service, unless the minor has requested that the parent be treated as a personal representative. This applies to the following situations:

(1) State law allows a minor to consent to receive the service;
or

(2) A minor consents to the service and state law does not require other consent; or

(3) A court or other person authorized by law (other than a parent) consents to the service on the minor’s behalf; or

(4) If the parent has agreed that PHI related to a given health care service will be kept confidential between the health care provider and the minor, that parent will not be treated as a personal representative for purposes of Protected Health Information related to that health care service.



Cardiovascular Associates of the Delaware Valley, P.A.

*Diagnostic and Interventional Cardiology
Diplomates of the American Board of Internal Medicine & Cardiology*

15.3 Procedure.

15.3.1 Provider personnel must confirm the identity and, if the person is not a parent, the authority of a personal representative.

15.3.2 The following criteria must be used to identify a personal representative.

(A) A parent will be treated as the personal representative of an unemancipated minor unless one of the exceptions listed above applies. An adult will be recognized as the parent of an unemancipated minor child if:

(1) He or she identifies himself or herself as the parent, and the adult and child share the same address; or

(2) If the child is identified on a health insurance identification card or other documentation as a dependent covered by that adult's health insurance; or

(3) If the adult is known by the workforce member to be the child's parent or guardian; or

(4) If the adult presents documentation of guardianship.

15.3.3 All others claiming to act as the Personal Representative of an individual must present written evidence of authority to act on behalf of the individual in making health care decisions.

15.3.4 A copy of the written evidence of authority must be approved by the Privacy Officer (or his or her designee) before the personal representative is to be granted access to the individual's Protected Health Information, or before a request to amend Protected Health Information, a request for an accounting of disclosures of Protected Health Information, an authorization to disclose Protected Health Information, or other request to act as a personal representative, will be honored. The Privacy Officer will determine which information the Personal Representative may have access to, in accordance with this and other Provider policies and applicable federal and state laws.

Section 16. BUSINESS ASSOCIATES

16.1 Policy.

16.1.1 Business Associates are any third parties that provide a service on behalf of Provider using Protected Health Information.

16.1.2 In order to disclose Protected Health Information to a Business Associate, Provider must receive satisfactory assurance that the Business Associate will appropriately safeguard the information. Such satisfactory assurance requires a contract or other written arrangement.



Cardiovascular Associates of the Delaware Valley, P.A.

*Diagnostic and Interventional Cardiology
Diplomates of the American Board of Internal Medicine & Cardiology*

16.2 Business Associate Agreement Requirements. A Business Associate Agreement must establish permitted and required uses and disclosures by the business associate and must also require the business associate to:

16.2.1 Appropriately safeguard the Protected Health Information.

16.2.2 Report any misuse of Protected Health Information.

16.2.3 Secure satisfactory assurances from any subcontractor.

16.2.4 Grant individuals access to and the ability to amend their Protected Health Information.

16.2.5 Maintain a mechanism to provide an accounting of disclosures to individuals.

16.2.6 Release applicable records to the Secretary of the Department of Health and Human Services, if requested.

16.2.7 Upon termination, return or destroy all Protected Health Information.

16.2.8 Authorize termination by Provider if the Business Associate violates a material term of the Agreement.

16.3 No Business Associate Agreement Required.

A Business Associate Agreement is not required for:

16.3.1 Disclosures made to a provider for treatment.

16.3.2 Disclosures made to a plan sponsor by employee group health plan.

16.3.3 Uses by and disclosures to a government agency that determines enrollment or eligibility for Medicaid or another public benefit program if such activity is authorized by law.

16.4 Procedures.

16.4.1 Provider has developed a form Business Associate Agreement, attached to these Health Privacy Policies and Procedures, titled "Provider Business Associate Agreement," and numbered HIPAA Form 10. In addition, a Business Associate addendum will be attached to relevant Provider contracts to provide appropriate provisions if such are applicable.

16.4.2 Business Associate Agreements, in the form of HIPAA Form 10, may be executed by the Privacy Officer. Business Associate Agreements that differ in any manner from HIPAA Form 10 must be submitted to the Privacy Officer for prior approval and may not be executed without that approval.



Cardiovascular Associates of the Delaware Valley, P.A.

Diagnostic and Interventional Cardiology
Diplomates of the American Board of Internal Medicine & Cardiology

16.4.3 Provider will review relationships with third parties and identify who their business associates are, what Protected Health Information they receive, and for what purpose.

Section 17. RESPONDING TO SUBPOENA REQUESTS

17.1 Purpose. The Privacy Rule permits covered entities to disclose Protected Health Information for judicial and administrative proceedings under limited circumstances. Specific rules apply to the release of information depending on the type of disclosure, as more fully discussed below.

17.2 Policy.

17.2.1 All members of Provider's workforce will refer all requests for documents and materials containing Protected Health Information pursuant to legal actions or administrative proceedings (i.e., a subpoena, discovery request, court order, or search warrant) to the Privacy Officer immediately upon receiving any such request.

17.2.2 After the Privacy Officer has been notified of the request for documents containing Protected Health Information, the Privacy Officer will take one of the following courses of action:

(A) If the request for materials containing Protected Health Information *is pursuant to a court order or order of an administrative proceeding*, the Privacy Officer will produce the requested documents only to the extent that the information is expressly authorized by the order.

17.2.3 If the request for materials containing Protected Health Information is pursuant to a subpoena, discovery request or other legal procedure that *is not accompanied by a court order or order of an administrative tribunal*, the Privacy Officer will produce the requested documents only after consultation with counsel, unless the patient has authorized the disclosure.

Section 18. DEFINITIONS

18.1 Authorization. A document signed and dated by the individual that authorizes the use and/or disclosure of Protected Health Information for reasons other than treatment, payment or health care operations. An authorization must contain a description of the Protected Health Information to be used and/or disclosed, the names or class of persons permitted to make a disclosure, the names or class of persons to whom the covered entity may disclose, an expiration date or event, an explanation of the individual's right to revoke and how to revoke, and a statement about potential redisclosures.

18.2 Business Associate. A person or entity who, on behalf of a covered entity or an organized health care arrangement uses Protected Health Information to perform or assist in the performance of: (A) a function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or (B) provides legal, actuarial, accounting, consulting, data



Cardiovascular Associates of the Delaware Valley, P.A.

*Diagnostic and Interventional Cardiology
Diplomates of the American Board of Internal Medicine & Cardiology*

aggregation, management, administrative, accreditation, or financial services for such covered entity or organized health care arrangement.

18.3 Business Associate Agreement. A contract between a covered entity and a business associate which must (A) establish the permitted and required uses and disclosures of Protected Health Information by the business associate; (B) provide that the Business Associate will use Protected Health Information only as permitted by the contract or required by law, appropriately safeguard the information, report any disclosures not permitted by the contract, ensure that agents to whom it provides Protected Health Information will abide by the same restrictions and conditions, make Protected Health Information available to the subject individual, make its records available to the Department of Health and Human Services to determine compliance with the Privacy Rule; and (C) authorize termination of the contract by Provider if Provider determines that there has been a violation of the contract. A Business Associate Agreement is usually part of a contract made in the procurement process, but can be part of a Memorandum of Understanding, Grant Agreement, contract amendment or other documents. See Provider's form of Business Associate Agreement, numbered HIPAA Form 10.

18.4 CMS. Centers for Medicare & Medicaid Services within the United States Department of Health and Human Services.

18.5 Compliance Date. The date by which a covered entity must comply with a standard, implementation specification, requirement, or modification adopted under these policies.

18.6 Covered Entity. A health plan, a health care clearinghouse, or a health care provider who transmits any Protected Health Information in electronic form in connection with a transaction covered by HIPAA.

18.7 Covered Functions. Those functions of a covered entity, the performance of which makes the entity a health plan, health care provider, or health care clearinghouse.

18.8 Designated Record Set. The medical records and billing records about individuals maintained by or for a covered health care provider; the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or medical records and billing records used by or for the covered entity to make decisions about individuals.

18.9 Disclosure. The release, transfer, provision of access to, or divulging of information outside the entity holding the information.

18.10 Health Care. Care, services, or supplies related to the health of an individual. Health care includes, but is not limited to preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care and sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

18.11 Health Care Clearinghouse. A public or private entity that does either of the following:



Cardiovascular Associates of the Delaware Valley, P.A.

*Diagnostic and Interventional Cardiology
Diplomates of the American Board of Internal Medicine & Cardiology*

18.11.1 Processes health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.

18.11.2 Receives a standard transaction from another entity and processes health information into nonstandard format or nonstandard data content for the receiving entity.

18.12 Health Care Provider. A provider of services and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

18.13 Health Information. Any information, whether oral or recorded in any form or medium, that: (A) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (B) relates to the physical or mental health or condition of an individual; the provision of health care to an individual; or payment for the provision of health care to an individual.

18.14 Health Maintenance Organization (HMO). A federally qualified HMO, and any organization recognized as an HMO under State law.

18.15 Health Plan. An individual or group plan that provides, or pays the cost of, medical care.

18.15.1 Health plan includes: (A) a group health plan (created pursuant to the Employee Retirement Income Security Act of 1974 [ERISA]); (B) a health insurance issuer; (C) an HMO; (D) Part A or Part B of the Medicare program; (E) the Medicaid program; (F) an issuer of a Medicare supplemental policy; (G) an issuer of a long-term care policy, excluding a nursing home fixed-indemnity policy; (H) an employee welfare benefit plan; (I) the health care program for active military personnel; (J) the veterans health care program; (K) the Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); (L) the Indian Health Service program under the Indian Health Care Improvement Act; (M) the Federal Employees Health Benefits Program; (N) an approved State child health plan; (O) the Medicare+Choice program; (P) a high risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible individuals; and (Q) any other individual or group plan.

18.15.2 A health plan excludes: (A) any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits that are listed in Section 2791(c)(1) of the PHS Act, 42 U.S.C. 300gg-91(c)(1); and (B) a government-funded program (other than one listed above in this definition): (1) whose principal purpose is other than providing, or paying the cost of, health care; or (2) whose principal activity is: (a) The direct provision of health care to persons; or (b) The making of grants to fund the direct provision of health care to persons.

18.16 Health Care Operations. Any of the following activities:

18.16.1 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;



Cardiovascular Associates of the Delaware Valley, P.A.

*Diagnostic and Interventional Cardiology
Diplomates of the American Board of Internal Medicine & Cardiology*

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;

18.16.2 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;

18.16.3 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);

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

18.16.5 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; and

18.16.6 Business management and general administrative activities of the entity, including, but not limited to: (A) management activities relating to implementation of and compliance with the requirements of this subchapter; (B) 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; (C) resolution of internal grievances; (D) 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; and (E) creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.

18.17 Health Oversight Agency. An agency or authority of the United States, a State or a political subdivision of a State, or a person or entity acting under a grant of authority from such public agency that is authorized by law to oversee the health care system or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

18.18 HIPAA. The Health Insurance Portability and Accountability Act of 1966, title II, subtitle F, §§ 261-264, Public Law 104-191.

18.19 HIPAA Privacy Rules. The final privacy regulations promulgated under HIPAA, 45 CFR Parts 160 and 164, which created national standards to protect medical records and other Protected Health Information.



Cardiovascular Associates of the Delaware Valley, P.A.

*Diagnostic and Interventional Cardiology
Diplomates of the American Board of Internal Medicine & Cardiology*

18.20 Indirect Treatment Relationship. A relationship between an individual and a health care provider in which:

18.20.1 The health care provider delivers health care to the individual based on the orders of another health care provider; and

18.20.2 The health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the individual.

18.21 Individual. The person who is the subject of Protected Health Information.

18.22 Inmate. A person incarcerated in, or otherwise confined to, a correctional institution.

18.23 Law Enforcement Official. An officer or employee of any agency or authority of the United States, a State, or a political subdivision of a State who is empowered by law to investigate or conduct an official inquiry into a potential violation of law, or to prosecute or otherwise conduct a criminal, civil or administrative proceeding arising from an alleged violation of law.

18.24 Marketing. To make 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.

18.24.1 Marketing does not include communications (A) to describe a health related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: (1) the entities participating in a health care provider network or health plan network; (2) replacements of, or enhancements to, a health plan; and (3) health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; (B) for treatment of the individual; or (C) for case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual.

18.24.2 Marketing specifically includes any arrangement between a covered entity and any other entity whereby the covered entity discloses Protected Health Information to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or that encourages recipients of the communication to purchase or use that product or service.

18.25 Notice of Privacy Practices. A notice to the individual of the uses and disclosures of Protected Health Information and the individual's rights and the covered entity's legal duties with respect to Protected Health Information.

18.26 Organized Health Care Arrangement. A clinically integrated care setting in which individuals typically receive health care from more than one health care provider or an organized system of health care in which more than one covered entity participates, and in which the



Cardiovascular Associates of the Delaware Valley, P.A.

*Diagnostic and Interventional Cardiology
Diplomates of the American Board of Internal Medicine & Cardiology*

participating covered entities hold themselves out to the public as participating in a joint arrangement and participate in joint activities.

18.27 Payment.

18.27.1 The activities undertaken by:

(A) A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or

(B) A health care provider or health plan to obtain or provide reimbursement for the provision of health care.

18.27.2 The activities in paragraph 18.27.2 of this definition relate to the individual to whom health care is provided and include, but are not limited to:

(A) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;

(B) Risk adjusting amounts due based on enrollee health status and demographic characteristics;

(C) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;

(D) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;

(E) Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and

(F) Disclosure to patient reporting agencies of any of the following Protected Health Information relating to collection of premiums or reimbursement: name and address; date of birth; social security number; payment history; account number; and name and address of the health care provider and/or health plan.

18.28 Personal Representative. An individual authorized by law to act on behalf of an individual is a personal representative. The representative will be treated as the individual for purposes of disclosure of Protected Health Information.

18.29 Policies and Procedures. This document, which is comprised of the policies and procedures adopted by the President of Provider, all Exhibits and Forms attached hereto, as such may be amended from time to time either by or with the approval of the President of Provider.

18.30 Privacy Incident. An event or action that:



Cardiovascular Associates of the Delaware Valley, P.A.

*Diagnostic and Interventional Cardiology
Diplomates of the American Board of Internal Medicine & Cardiology*

- (A) May have resulted from the unauthorized or unlawful access, use, alteration, disclosure, destruction or loss of Protected Health Information; or
- (B) Results in any inquiry, complaint, claim or request for inspection or audit related to the processing of Protected Health Information; or
- (C) Is a violation of the Provider's Health Privacy Policies and Procedures or any other confidentiality policy; or
- (D) Is a violation of U.S. federal or state privacy laws and regulations or of a HIPAA Business Associate Agreement to which the Provider is a party.

18.31 Privacy Rule. See HIPAA Privacy Rule.

18.32 Protected Health Information (PHI). Individually identifiable health information that is maintained or transmitted in any form or medium. Protected health information excludes individually identifiable health information in education records covered by the Family Educational Right and Privacy Act.

18.33 Psychotherapy Notes. 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.

18.34 Public Health Authority. An agency or authority of the United States, a State, a political subdivision of a State or a person or entity acting under a grant of authority from or contract with such public agency that is responsible for public health matters as part of its official mandate.

18.35 Research. A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to general knowledge.

18.36 Treatment. The provision, coordination or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to an individual or the referral of an individual for health care from one health care provider to another.

18.37 Use. With respect to individually identifiable health information, the sharing, employment, application, utilization, examination or analysis of such information within an entity that maintains such information.