COLUMBUS EYE ASSOCIATES
COLUMBUS OPTICAL

COMPLIANCE PLAN
PROGRAM FOR THE
HIPAA PRIVACY STANDARDS

TABLE OF CONTENTS

COLUMBUS EYE ASSOCIATES
COLUMBUS OPTICAL

COMPLIANCE PLAN

FOR THE HIPAA PRIVACY STANDARDS

MARCH 1, 2003

COLUMBUS EYE ASSOCIATES & COLUMBUS OPTICAL
HIPAA PRIVACY COMPLIANCE PROGRAM

Columbus Eye Associates and Columbus Optical recognize that patient information is sensitive and, as such, must be treated carefully and responsibly. The purpose of this Compliance Program is to establish a framework to guide the Columbus Eye Associates and Columbus Optical use and disclosure of protected health information required by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Privacy Standards issued under HIPAA. It will also assist Columbus Eye Associates and Columbus Optical in responding to patients who exercise their health information rights.

The Columbus Eye Associates and Columbus Optical Compliance Program shall be applicable to all officers, directors, managers, employees, physicians and independent contractors of Columbus Eye Associates and Columbus Optical and its affiliated entities (the "Company"). The Program is divided into two distinct parts. The first part, called the Compliance Plan, gives direction on the process that will be followed to help ensure that the Privacy Standards are met. The second part, the Policies and Procedures, gives directions on the specific standards or rules to apply in various situations.

I. COMPLIANCE PLAN

A. Privacy Officer

1. The Company has appointed a Privacy Officer, Bob Moore, who is responsible for the development and implementation of privacy policies and procedures. The Privacy Officer will be responsible for:

- providing leadership to any privacy board, committee or task forces created by the Company;
- overseeing the Company's Compliance Program;
- developing and implementing the Company's training program for privacy;
- monitoring the effectiveness of the Compliance Program;
- initiating and overseeing the completion of corrective action plans for violations of the Compliance Program;
- developing and maintaining the Company's Privacy Notice, consents, authorizations, and other forms;
- serving as the contact person for individuals who have complaints about how the Company uses and discloses protected health information and about questions regarding matters covered in the Company's Privacy Notice;
- approving requests for amendment; and
- keeping abreast of developments under the Administrative Simplification provisions of HIPAA and periodically revising the Compliance Program as necessary and with the approval of the Company's management.

2. If Company personnel have a question concerning the scope, use or release of protected health information; their questions should be addressed to the Privacy Officer.

B. Complaint Process

1. The Company will provide a process for any individual to raise issues to the Company regarding the Company's policies and procedures concerning the use and disclosure of protected health information and its compliance with those policies and procedures and the requirements of HIPAA.

2. The Privacy Officer will be responsible for all reports of issues, will conduct any necessary investigation into those reports, and will attempt to resolve complaints and take corrective measures, if necessary.

3. The Privacy Officer will routinely report the outcome of investigations to the Company's management. Individuals who file a report will be notified of the disposition of their report no later than sixty (60) days after a report is filed. The Privacy Officer will document all reports received and dispositions of such reports.

C. Sanctions

1. As a condition of employment or other affiliation with the Company, all Company personnel are required to follow the Company's policies and procedures concerning the use and disclosure of protected health information. The Company shall impose appropriate disciplinary action, in accordance with the Company's disciplinary policies, upon any personnel who fail to comply with applicable laws or this Compliance Program.

2. Punishment for serious violations may subject an individual to immediate termination. The following violations are representative examples of serious violations potentially justifying termination:

- committing any act which would expose the Company to potential criminal sanctions;
- intentional or reckless conduct that violates this Compliance Program or HIPAA's Privacy Standards;
- failure to report conduct that the individual knew was a violation of this Compliance Program or HIPAA's Privacy Standards; or
- failure to correct behavior for which an individual was subject to prior disciplinary action.

3. Officers and managers are responsible for disciplining personnel in an appropriate and consistent manner. The type of disciplinary action shall be determined on a case-by-case basis, and where appropriate, in consultation with the Privacy Officer and the Company's management.

4. The range of sanctions shall include oral warnings, written warnings, oral reprimands, written reprimands, demotion, suspension, or termination.

5. Nothing in this policy shall be interpreted as granting employees of the Company any right to challenge or seek further review of the disciplinary action imposed upon them by their supervisor or by any other officer or agent of the Company. The review processes discussed here are for the sole benefit of the Company to enhance the effectiveness of its Compliance Program.

D. Mitigation

1. Whenever it comes to know of a violation of HIPAA, the Company will take all reasonable steps necessary to mitigate any harmful effect of a use or disclosure of PHI in violation of its policies and procedures or of HIPAA's Privacy Standards.

2. This requirement applies whether the harm is created by the Company or one of its business associates.

E. No Intimidation or Retaliatory Acts

1. The Company will not require individuals to waive their rights to file a complaint with the Secretary of the Department of Health and Human Services (the "Secretary") or their other rights under the HIPAA Privacy Standards as a condition to receiving treatment.

2. Company personnel are also prohibited from retaliating against any person who files a complaint with the Secretary or testifies, assists, or participates in investigations, compliance reviews, proceedings or hearings under the Administrative Simplification provisions of HIPAA.

3. All personnel are prohibited from retaliating against patients for exercising their rights granted under HIPAA or participating in any process established by the HIPAA Privacy Standards, such as the filing of a complaint against the Company.

F. Policies and Procedures as an Element of the Compliance Program

1. The Company's policies and procedures with respect to protected health information, which may be found later in this document, are reasonably designed to comply with the standards, implementation specifications, and other requirements of HIPAA's Privacy Standards, taking into account the size of the Company and the type of activities undertaken by the Company.

2. All policies and procedures aimed at compliance with the HIPAA Privacy Standards will be documented. This documentation will be maintained by the Privacy Officer for six (6) years from the date they were last in effect.

3. The Company will modify its policies and procedures as necessary to comply with changes in law, including changes to HIPAA's Privacy Standards. These changes will be promptly documented and implemented. If a change in law materially affects the content of the Company's Notice of Privacy Practices, as discussed later in this document, the Company will

promptly make appropriate changes to its Notice. The Privacy Officer shall be responsible for overseeing these changes.

G. Training Requirement

1. All members of the Company's workforce must undergo training on the Company's policies and procedures, as necessary and appropriate for the individuals to carry out their functions.

2. Initial training will occur before the compliance date, which is April 14, 2003.

3. For persons joining the workforce after the date of the initial training, training will be required within a reasonable period of time after the person joins the workforce.

4. When the Company makes a material change in its privacy policies it will retrain those affected by the change within a reasonable period of time.

5. Annual training of a minimum of one (1) hour per year will be provided to workforce members with significant access to protected health information.

6. All members of the workforce will sign an acknowledgement when they have completed required training. This documentation will be maintained by the Privacy Officer for six (6) years from the date the acknowledgement is signed.

II. POLICIES AND PROCEDURES

A. General Framework

1. The Company will use and disclose protected health information only as permitted by the HIPAA Privacy Standards and this Compliance Program. Protected health information means individually identifiable health information[1] transmitted or maintained in any format (written, electronic, or oral), whether relating to a living or a deceased individual.

2. The Company is required to disclose protected health information when an individual requests access to certain health information, in accordance with Section II(I)(4), or an accounting of disclosures, in accordance with Section II(I)(6).

3. The Company must also disclose protected health information when the Secretary requests information to determine the Company's compliance with the HIPAA Privacy Standards.

4. Any request for access or an accounting, or a request from the Secretary will be forwarded immediately to the Privacy Officer who will coordinate the Company's efforts. The Privacy Officer shall log each such request as well as the Company's follow-up to each such request.

5. The Company may use or disclose protected health information without patient permission for certain public policy-related purposes.[2]

6. The Company may also use and disclose protected health information for its own treatment, payment and health care operation purposes, without patient permission, as discussed in Section II(C), unless another law requires it.

7. In general, for all other purposes, the Company must obtain the individual's permission before it uses or discloses the individual's protected health information. There are two forms of permission under the HIPAA Privacy Standards: oral agreement and authorization.

8. The Company will obtain the patient's verbal agreement before disclosing protected health information to persons assisting in a patient's care, unless an exception to this requirement applies. The agreement does not have be in writing and may be inferred from the circumstances. See Section II(D).

9. In certain other circumstances, discussed at Section II(E), where oral agreements is not sufficient for a disclosure or use, the Company will obtain a written authorization from the individual.

10. Prior to any disclosure permitted by this Compliance Program, the Company will, except for disclosures permitted under Section II(D), take reasonable steps in an effort to verify the identity of a person requesting protected health information and the authority of any such person to have access to protected health information, if the identity or authority of the person is not known to the Company.

11. The Company will secure any documentation, statements, whether oral or written, from the person requesting protected health information, when such documentation, statement, or representation is a condition of disclosure.

B. De-identified Information

1. The Privacy Standards apply to health information that identifies or could reasonably be expected to identify an individual. They do not restrict the use or disclosure of information that has been de-identified.[3]

2. To create de-identified information, the Company may use one of two methods. First, it may remove all of the identifiers that appear in the footnote below.[4] Second, the Company may remove fewer identifiers, if a person with appropriate statistical and scientific knowledge determines that the risk of identification is very small.

3. If the information is to be used for research, public health purposes, or health care operations, the Company may create a more limited data set, that does not include directly identifiable information but in which certain identifiers, such as admission, discharge and service dates, date of death, age and five-digit zip code remain.[5]

4. The Company must condition disclosure of the limited data set upon the recipient signing a data use or similar agreement, in which the recipient agrees to limit its use of the data to the original reasons for the disclosure and to refrain from attempting to re-identify the information or use it to contact the subjects of the information.

C. Uses and Disclosures for Treatment, Payment and Health Care Operations

1. General Requirements

a. The Company may use or disclose the patient's protected health information for its own treatment, payment[6] or health care operations,[7] without permission from the patient, unless required under state or other law.[8]

b. The Company may release protected health information to another health care provider for treatment activities of the other health care provider without patient permission.

c. The Company may release protected health information to another health care provider, without regard to that provider's status as a covered entity under the Privacy Standards, without patient permission, where the recipient will use the information for payment purposes.

d. It is also permissible for the Company to disclose protected health information, without patient permission, to another covered entity for certain health care operations purposes of the receiving entity,[9] including, but not limited to, conducting quality assessment and improvement activities, carrying out population-based analyses related to improving health and reviewing the competence of health care providers and for the purposes of health care fraud and abuse detection or compliance. However, the Company will make such disclosures only to the extent that the entity receiving the protected health information has or had a relationship with the individual who is the subject of the information which is requested. Where such a relationship has ended, the Company will only disclose protected health information that relates to the past relationship.

e. The occasional incidental use or disclosure of protected health information in connection with other permissible uses or disclosures is not a violation the Privacy Standards as long as the Company complies with Section II(G) and implements reasonable safeguard to limit these kinds of uses and disclosures.

f. Where the Company has a direct treatment relationship[10] with a patient, it will make a good faith effort to obtain a patient's written acknowledgment of receipt of the Company's Notice of Privacy Practices no later than the time of first service delivery after the April 14, 2003 compliance deadline.[11]

g. Where the Company participates in an organized health care arrangement, it may disclose protected health information about an individual, without patient permission, to another covered entity for the health care operation activities of the arrangement.

2. Procedures for Implementation

a. The Company need not use a specific form for the acknowledgment of receipt of the Notice of Privacy Practices. It may have the patient initial a cover sheet to its Notice of Privacy Practices or sign a list or form. The acknowledgment may also be electronic.

b. Where a patient refuses to sign or to return the acknowledgment, the Company will document its efforts to obtain the acknowledgment and the reasons why an acknowledgment could not be obtained in the patient's record (e.g., patient received form but refused to sign acknowledgment).

c. The Company will maintain this documentation for six (6) years from the date they were created or last in effect, whichever is later.

D. Uses and Disclosures Pursuant to Individual Agreement

1. General Requirements

a. The Company will obtain an individual's agreement before it discloses protected health information to a patient's family member, relative, close personal friend or other person identified by the patient as assisting in the patient's care, unless one of the exceptions discussed below applies. Individual agreement may be oral. The Company will limit its disclosures of protected health information in this context to the information that is directly relevant to the person's involvement in the patient's care. [12]

b. The Company may use or disclose protected health information to notify, or assist in the notification of a family member a personal representative or another person responsible for the care of a patient, of the patient's location, general condition or death.

c. In the event of disaster relief activities, the Company may share information with disaster relief officials to coordinate notification of a person involved in the patient's care.[13]

2. Securing Individual Agreement

a. In order to obtain individual agreement, the Company must inform the individual in advance that it would like to disclose protected health information to a person assisting in the patient's care and provide the individual with the opportunity to agree to, prohibit or restrict the disclosure. If the individual does not express an objection, the Company may assume that the patient agrees to the proposed disclosures. If the patient expresses an objection, the Company will proceed with the disclosure only in accordance with the individual's direction.

b. Company personnel may reasonably infer agreement from the circumstances, based on the exercise of its professional judgment.[14]

3. Exceptions

a. Where an individual is not present to secure agreement or the opportunity to agree or object practicably cannot be provided because of the individual's incapacity or an emergency circumstance, the Company may forego obtaining individual permission to release protected health information.

b. Such disclosure must be, in the Company's professional judgment, in the best interests of the patient.

4. Procedures for Implementation

a. Where the Company obtains a patient's oral agreement to disclose protected health information to a patient's family members, relatives and any other person designated by the patient, it is the policy of the Company that such agreement will be noted in the patient's record with the time, date and any relevant restrictions, though this is not required by HIPAA.

b. Before making any disclosure to a family member or other person listed above, Company personnel must verify that the individual's agreement was obtained, where agreement is required. A person's identity does not have to be verified unless, in the Company's professional judgment, there is reason to believe the person is not who he/she claims.

E. Authorizations

1. General Requirements

a. The Company will obtain an authorization from an individual to use and disclose the individual's protected health information where an individual's permission is required but individual oral agreement is not appropriate.

b. In other words, the Company will obtain an authorization from an individual when it seeks to use or disclose the individual's protected health information for any purpose other than treatment, payment, health care operations; disclosures to the individual himself or herself; to make disclosures to persons assisting in an individual's care as discussed in Section II(D), or for the public policy-related purposes discussed in footnote 2.

c. Where required, the Company will obtain an authorization to use or disclose protected health information for marketing activities.[15]

d. In those situations where authorization is required, the authorization will state clearly whether the Company will receive remuneration from a third party for its efforts.

e. When the Company seeks an authorization from an individual, the Company will provide the individual with a copy of the signed authorization.

2. Effective Authorizations

a. Authorizations obtained by the Company will contain all necessary elements.[16]

b. The Company will not use or disclose protected health information as outlined in an authorization if the authorization is not appropriate to use for any reason.[17]

c. In general, Company personnel may not combine an authorization to use or disclose protected health information with another document.[18]

d. The Company will maintain an authorization for six (6) years from the date it was last in effect.

3. Conditioning Treatment on Signing an Authorization

a. The Company will not condition the provision of treatment to an individual on the individual signing an authorization to use or disclose protected health information, unless one of the following exceptions applies.

b. The Company may condition the provision of research-related treatment on the individual signing an authorization to use and disclose protected health information for such research.

c. The Company may condition treatment that is solely for the purpose of creating protected health information for disclosure to a third party on the individual signing an authorization for the disclosure of such information to the third party.[19]

4. Revocation

a. The Company will permit patients to revoke their authorizations, except to the extent that the Company has taken action in reliance on the authorization. All revocations must be in writing to be effective.

b. Notification of revocations will be disseminated to all persons, including business associates, who handle the individual's protected health information on behalf of the Company.

F. Personal Representatives

1. With limited exceptions, the Company must allow an individual's personal representative to exercise the rights given to that individual.[20]

2. If, under applicable law, a person has authority to act on behalf of an adult or an emancipated minor,[21] the Company must treat such person as the personal representative with respect to the adult's or emancipated minor's protected health information.[22]

3. If under applicable law a parent, guardian or other person acting in place of a parent has authority to act on behalf of an unemancipated minor, the Company must treat the person as a personal representative with respect to protected health information.

4. If any of the following exceptions applies, the Company must permit the minor to exercise the rights given to individuals under the Standards and to control the disclosure and access to the minor's protected health information:

- The minor consents to the health care service, no other consent is required by law, and the minor has not requested that any person be treated as a personal representative;

- The minor may lawfully obtain the health care service without consent of a parent, guardian or other person acting in loco parentis, and the minor, a court or another person authorized by law consents to the service; or

- A parent, guardian or other person acting in loco parentis assents to an agreement of confidentiality between the Company and the minor with respect to the health care service.

5. Even if one of the above-mentioned exceptions in this Section II(F)(4) applies, the Company may disclose or provide access to a minor's protected health information to a parent, guardian or other person acting in loco parentis, if state or other law permits or requires such disclosure. However, it may not disclose or provide access to such information, if state or other law prohibits such disclosure or access.

6. Even if one of the above-mentioned exceptions in this Section II(F)(4) applies, the Company may provide or deny access to a parent, guardian or other person acting in loco parentis, if (1) such person is not the personal representative of the minor, (2) there is no applicable access provision under state or other law, (3) such action is consistent with state or other applicable law, and (4) the decision to provide or deny access is made by a licensed health care professional, in the exercise of professional judgment.

7. If under applicable law, an executor, administrator, or other person has authority to act on behalf of a deceased individual or the individual's estate, the Company must treat such person as a personal representative.

G. Minimum Necessary Requirements

1. General Requirements

a. Unless an exception listed below applies, the Company will make reasonable efforts not to use, disclose or request more than the minimum amount of protected health information necessary to accomplish the intended purpose of a use, disclosure or request.

b. The Company does not need to make a minimum necessary determination in the following circumstances:

- disclosure made in a HIPAA standard transaction, meaning one of the standardized electronic communications created under HIPAA, such as electronic claims submissions;

- disclosures to or requests by a health care provider for treatment;

- disclosures of protected health information made to the Secretary to determine the Company's compliance with the Standards;

- uses and disclosures required by law;

- disclosures to individuals of their own protected health information; and

- disclosures pursuant to an authorization.

2. Uses of Protected Health Information and Procedures for Implementation

a. For uses of protected health information, the Company will identify those persons or classes of persons in its workforce who need access to the information to carry out their duties. For each such person or classes of persons, it will identify the category or categories of access they need to perform their jobs and any conditions appropriate to such access. The Company will make reasonable efforts to limit the access of protected health information in accordance with these designations.

b. The Company finds that all physicians and medical directors involved in the treatment of an individual, including nurses, technicians, and screeners, need access to the individual's entire medical record, as do billing and coding personnel.

c. Front-office personnel who receive patients into the office will have access to patient medical records, but only as necessary to pull and prepare a chart for a treating physician, check for the completion of patient forms used by the Company, organize charts or file materials for others in the chart, or to perform other delegated specific tasks.

All personnel of the Company, including physicians, will be given passwords to access medical information they need. Depending on the access rights attributed to a password, personnel will be permitted to view the fields they need to perform their functions.

The Company will keep all medical records in files marked with a numerical colored tab. At each Company office, all medical records will be maintained in one location which can be secured either by locking the file drawers that contain such records or locking the door to the room where records are kept or, if that is not possible, ensuring that the office is locked at the end of each day. Forms necessary to file health care claims will be maintained in files separately from patient medical records.

3. Routine Requests or Disclosures and Procedures for Implementation

a. For routine requests or disclosures of protected health information, the Company will establish policies and procedures to limit the amount of information requested or

disclosed to the minimum amount necessary to accomplish the purpose of the request or disclosure.

b. The Company makes the following types of routine disclosures and has determined that the following information is the minimum necessary protected health information in such circumstances:

- for disclosures to accreditation organizations - all relevant information requested consistent with the organizations' protocols and methodologies, including the entire medical record for any case studies;

- for disclosures to attorneys - all relevant information requested by the attorneys;

- for disclosures to risk managers at malpractice insurance companies - all relevant information requested by the risk managers;

- for billing, coding, or practice management consultants - all relevant information consistent with their protocols or methodologies;

- for disclosures to billing companies - all information required to file health care claims, but not the entire medical record, unless verification of billing and coding is to be provided by the billing company; and

- for disclosures to transcriptionists - all information which needs transcribing, as well as any documents useful to ensuring the accuracy of those transcriptions.

- for disclosures to collection agencies - all information required to enable the collection agency collect payments owed by patient to the Company.

c. The Company does not violate the Privacy Standards when it makes incidental uses and disclosures of PHI that cannot reasonably be prevented, that are limited in nature, and that occur as a by-product of an otherwise permitted uses or disclosures, so long as reasonable safeguards are taken to minimize the chance of incidental disclosure to others.[23]

4. Non-Routine Requests or Disclosures and Procedures for Implementation

a. For non-routine requests or disclosures, the Company will develop reasonable criteria and procedures for determining and limiting, on an individual basis, the request for or the disclosure of, protected health information to the minimum amount necessary to accomplish the purpose of the request or disclosure.

b. Some relevant criteria in making case-by-case determinations include how much information is being requested, if all the information to be provided is relevant to the stated purpose of the use or disclosure, whether the information is particularly sensitive, and whether the requesting party could accomplish its purpose with de-identified information.

c. All individual reviews of minimum necessity, for non-routine disclosures and requests, will be conducted or approved by the Privacy Officer.

5. Disclosure of an Entire Medical Record

a. Unless one of the exceptions in Section II(G)(1)(b) applies, the Company will not use, disclose or request an entire medical record, except when the entire record is specifically justified as the minimum amount necessary in its policies and procedures. A treatment purpose justifies a request for an entire medical record.

b. The Company may rely on another person's representation that it is requesting the minimum amount of information necessary, if the reliance is reasonable and where the request is made by : (1) another covered entity, (2) a professional (such as an accountant) who needs the information to provide services to the Company, (3) a public official in accordance with one of the public policy-related uses and disclosures outlined in footnote 2, or (4) an Institutional Review Board ("IRB") or privacy board for research purposes.[24]

H. Business Associates

1. The Company will not disclose protected health information to a business associate unless it has first executed a written contract with the business associate which contains all of the provisions contained in the example found at Exhibit 1. The Privacy Officer will be responsible for securing the appropriate contract from all of the Company's business associates and overseeing their duties.

2. If the Company becomes aware of a pattern of activity or practice of a business associate that constitutes a material breach or violation of the business associate's obligations under its contract, it will take reasonable steps to cure the breach or end the violation.[25]

3. The Company may continue operating under certain existing written contracts with their Business Associates until April 14, 2004 without amending the contracts to include the Business Associate contract provisions. To qualify for the extension, the contract between the Business Associate and the Company must: (1) exist before October 15, 2002 and (2) not be modified or renewed between that date and April 14, 2003 (the Privacy Standards' compliance date). By April 14, 2004, all of the Company's Business Associate arrangements must be in conformance with the Privacy Rule.[26]

I. Individual Rights

1. Notice of Privacy Practices

a. The Company will develop a Notice of Privacy Practices required by the HIPAA Privacy Standards.

b. The Company will adhere to its Notice of Privacy Practices (the "Notice"). The Privacy Officer shall be responsible for developing and maintaining the Company's Notice. The Notice currently adopted by the Company is attached as Exhibit 4.

c. The Privacy Officer will be listed on the Notice and serve as the contact person for individuals who have complaints about how the Company has used or disclosed their protected health information or who have questions about the Company's Notice.

d. Except in emergency treatment situations, a copy of the Notice shall be distributed to each patient no later than the patient's first visit after HIPAA's compliance date of April 14, 2003.[27] It shall be the responsibility of the front desk personnel to ensure that this is accomplished. Additional copies will be provided individuals, including members of the public, upon request. A copy of the Notice will be prominently displayed in the patient waiting room.

e. The Notice will be promptly revised whenever there is a material change to the Company's practices described in the Notice.[28] Unless required by law, material revisions will not be implemented prior to the effective date of the revised Notice.[29] Revised Notices will be made available upon request and posted prominently in the patient waiting room.

f. The Company's Notice will be retained for six (6) years from the date it was last in effect.

g. If and when The Company operates and maintains a web site, The Company will post the Notice in a prominent location on its web site and make the Notice available electronically through the web site. Individuals may request an additional copy be sent to them in electronic or paper format. If the first service delivery to an individual is delivered electronically, the Company must provide electronic notice automatically and contemporaneously in response to the individual's first request for service. Additionally, the Company will establish a mechanism to require and capture a patient's acknowledgement electronically.

2. Right to Request Restrictions on the Uses and Disclosures of Protected Health Information

a. The Company will permit patients to make requests to restrict the Company's use and disclosure of protected health information for treatment, payment, health care operations or disclosures pursuant to Section II(D).

b. Nevertheless, it is the policy of the Company to not agree to such requests.[30]

3. Right to Request Confidential Communications

a. The Company will permit individuals to request that it provide confidential communications involving protected health information to the individual.

b. The Company will accommodate reasonable requests by individuals to receive communications of protected health information from the Company by alternative means or at alternative locations. [31]

c. The Company may require the individual to make a request for a confidential communication in writing.

d. Requiring an explanation from the individual as to the basis for the request for confidential communications is prohibited.

4. Right to Access Protected Health Information

a. The Company will give individuals access to their protected health information contained in designated record sets. Designated record sets include a patient's medical record, billing record, and any other document or record used to make decisions about the patient. The Privacy Officer shall be responsible for receiving and processing requests for access.

b. Written requests for access to their protected health information will be accepted.[32] All written requests for access will be have the date the request was received. Oral requests may be accepted in special circumstances.

c. The Company will arrange for review by the patient at a convenient time and location or mail the information to the patient, upon the patient's request, unless an exception that permits the denial of the request is present.[33]

d. The Company will provide the patient 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. If not, the information will be produced in a readable hard copy form.[34]

e. The Company will charge a reasonable copying fee per page in connection with a request for access.[35]

f. The Company may deny a person access to his or her protected health information for any of the reasons set out in the accompanying footnote.[36]

g. If the Company denies a request for access, the Company must provide a timely, written denial to the individual. The denial must contain the basis for the denial and a description of how to complain to the Company or the Secretary.[37]

h. The Company will maintain the designated record sets and the titles of the person(s) in charge of receiving and processing requests for access for six (6) years from the date the records were created.

5. Right to Amendment

a. Patients have a right to request an amendment to their protected health information which is contained in designated record sets. The Privacy Officer will receive and process these requests.

b. The Company may deny a patient's request if the information:

- is accurate and complete;
- is not contained in a designated record set;
- would not be subject to the right of access; or
- was not created by the Company, unless the patient provides a reasonable basis to believe the entity which created the information is no longer available to act on the request.

c. The Company may require the patient to put the request for amendment in writing and to give a reason for the request (e.g., the patient feels the information is incorrect) provided that the Company informs a patient of these requirements in advance.[38] All requests will be stamped with the date they were received.

d. All requests for amendment will be subject to approval by the Privacy Officer who shall consult with the Company's management. The Privacy Officer will maintain this documentation, along with requests for amendment, statements of denial, statements of disagreement and rebuttals for a period of six (6) years from the date they were created or last in effect, whichever is later.[39]

e. The Company must act on a request for an amendment no later than sixty (60) days from receipt of the request. All written requests will be stamped with the date it was received. If the Company accepts the request, it must make the amendment and notify the patient that the amendment was accepted within sixty (60) days. Amendment may be made by identifying the records in the designated record set that are affected and appending or otherwise providing a link to the location of the amendment. The Company must make reasonable efforts to provide the amendment within a reasonable amount of time to persons identified by the patient as having received protected health information needing the amendment. It must also notify persons, including business associates, that the covered entity knows to have the information and that may have relied on the information to the detriment of the patient.

f. If the Company denies the requested amendment, in whole or part, it must provide the patient with a written denial within sixty (60) days of the request. The written denial must contain the following: (1) the basis for the denial; (2) a statement that the patient has a right to submit a statement of disagreement and describe how the patient may file such a statement [40]; (3) an explanation that the patient may request that the Company provide the patient's request for amendment and its denial with any further disclosures of the patient's protected health information in lieu of a statement of disagreement; and (4) the denial must describe how the patient may complain to the Company or the Secretary about the denial.[41]

g. The Company may prepare a written rebuttal to a patient's statement of disagreement, a copy of which must be provided to the patient.[42]

h. When informed by another covered entity of amendment to protected health information in its possession, the Company will make the amendment in the manner described in this Section II(I)(5).

6. Right to an Accounting of Disclosures

a. Patients have the right to an accounting of disclosures made by the Company and its business associates for disclosures other than these:

- for treatment, payment or health care operations;
- disclosures incidental to a disclosure otherwise permitted so long as the minimum necessary standard is met and reasonable precautions are taken to limit the disclosures;
- to a patient concerning the patient's protected health information;
- pursuant to an authorization;
- to persons assisting in a patient's care (made pursuant to their agreement);
- for national security or intelligence purposes;
- to correctional institutions or law enforcement officials as provided for under the Privacy Standards;
- disclosures as part of a limited data set; or
- disclosures that occurred prior to the compliance date, which is currently April 14, 2003.

b. Patients have a right to an accounting of the applicable disclosures that have been made by the Company and its business associates in the six (6) year period prior to the date of the request for an accounting, except that no accounting is required for disclosures made before April 14, 2003.[43]

c. An accounting of a disclosure must include all required information. [44]

d. The Company will provide an accounting within sixty (60) days of receiving such a request. If the Company is unable to do so, the Company may have a one-time extension of no more than thirty (30) days, provided that within the initial sixty (60) day time period, the Company supplies the patient a written statement of the reasons for the delay and the date by which the Company will complete its action on the request.

e. Patients will be given one free accounting per twelve (12) month period. For each additional request by a patient within the twelve (12) month period, the Company may, with prior notice,[45] charge a reasonable, cost-based fee.

f. In order to meet HIPAA's requirements relative to accountings of disclosures, the Company will begin to maintain a system, such as a log, for recording the relevant information needed to produce an accounting. The Privacy Officer will be responsible

for maintaining the system. Unless the disclosure is excepted from the right to an accounting as described in Section II(I)(6)(a), above, personnel are required to consult with the Privacy Officer prior to making a disclosure of protected health information so that the required information can be logged.

7. Affiliated Entities

a. Legally distinct covered entities that share common ownership or control may designate themselves as a single covered entity for purposes of the Privacy Standards. If the Company chooses to make such a designation (such as with a practice and a related ambulatory surgery center), it may develop a single Notice of Privacy Practices which will govern the use and disclosure of protected health information between the covered entities which comprise the single covered entity. By designating itself as a single covered entity, it may also use and disclose protected health information freely between the separate entities for health care operations purposes.

b. The Company will document any such designation and maintain that documentation for six (6) years from the date it was created or last in effect, whichever is later.

J. Safeguards

1. The Company will institute administrative, technical and physical safeguards to protect the privacy of protected health information.

2. The Company will take all reasonable steps to safeguard protected health information from any intentional or unintentional use or disclosure in violation of HIPAA.

3. The Company will take all reasonable steps to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

4. Specifically, the Company requires that the following safeguards be taken:

- At each office of the Company, protected health information will be maintained in one location which can be secured either by locking the file drawers or containers that contain such records or locking the door to the room where records are kept or, if that is not possible, ensuring that the office is locked at the end of each day.

- The Company will keep all medical records in files marked with a numerical colored tab. At each Company office, all medical records will be maintained in one location which can be secured either by locking the file drawers that contain such records or locking the door to the room where records are kept or, if that is not possible, ensuring that the office is locked at the end of each day.

- Access controls will be used to protect electronically maintained protected health information;

- Computers containing protected health information will not be placed in areas where the information may be viewed by unauthorized individuals;

- All documents containing protected health information will be shred before they are thrown away;

- Protected health information will not be faxed without a fax transmittal sheet that states that the information contained in the fax is confidential and intended for the identified recipient only. It should also state that unauthorized dissemination is strictly prohibited;

- Personnel should also use due care in addressing the fax sheet and keying in the proper fax numbers;

- Given that e-mail is inherently an insecure communication medium, sensitive protected health information will not be routinely e-mailed; and

- Personnel should also use due care in transporting protected health information from one office to another.

5. Company personnel are free to engage in oral communications as required for quick, effective and high quality health care. Sometimes "overheard communications" are unavoidable; nevertheless, where it is reasonable to do so, Company personnel are directed to speak quietly.

K. Effect of State Law

1. The Company will comply with all laws, which relate to the use and disclosure of protected health information, including state laws. If there is a conflict between the requirements of HIPAA and another state law, so that the Company cannot follow both laws, the Privacy Officer will follow the legal standard that provides the greatest protection to the information of the patient. The Privacy Officer may consult with legal counsel, as necessary, on these issues.

2. State laws that are more protective of health information than the HIPAA Privacy Standards are not preempted by those Standards and will operate to increase or raise the Company's obligations beyond those described in this document.

Endnotes

[1] Individually identifiable health information is that subset of health information that:

- Is created by or received by a health care provider, health plan, employer, or health care clearinghouse;
- Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
- Identifies the individual or which provides a reasonable basis to believe that it could probably be used to identify the individual who is the subject of the information.

[2] The Privacy Standards establish requirements for public policy uses and disclosures related to:

- Disclosures required by state or federal law.
- Public health activities, such as vital statistics, communicable disease reporting, child abuse or neglect reporting, post-marketing surveillance or adverse event reporting, department of motor vehicles visual acuity reporting, and certain OSHA-related workplace medical surveillance or work-related illness or injuries.
- Reports of adult abuse, neglect, or domestic violence. Disclosures are permissible if they are (i) required by law or (ii) expressly authorized by law and necessary to prevent serious harm to the individual or other potential victims, based upon the professional judgment of the Company or if the individual is unable to agree to the disclosure because of incapacity, a law enforcement or other public official represents that the information is not intended to be used against the individual, and that immediate enforcement activity would be materially and adversely affected by waiting until the individual would agree to the disclosure. The individual (or his or her personal representative) must be informed that the protected health information has been disclosed, unless the Company believes this would (i) place the individual at risk of serious harm or (ii) the personal representative is reasonably believed to be responsible for the abuse, neglect, or injury.
- Health oversight activities, such as investigations, payor coding and billing audits, consequently, this exception permits a health care provider to produce patient medical records in connection with a government payment audit without obtaining patient permission, licensure or disciplinary actions, or criminal, civil or administrative proceedings. Consequently, this exception permits a health care provider to produce patient medical records in connection with a government payment audit without obtaining patient permission.
- Judicial and administrative proceedings pursuant to an order of a court or administrative tribunal, a subpoena, or a discovery request. Before furnishing information not requested by a court or administrative order (i.e. in response to a subpoena, discovery request, or other similar request), the Company must receive assurances that the individual has received notice of the request or reasonable efforts have been made to notify the individual or the requesting party has obtained protective order from a court or administrative tribunal. In the alternative, the Company may make reasonable efforts to provide notice to the individual or to seek a qualified protective order. The Privacy Standards contain a detailed explanation of how these obligations may be satisfied. Due the complexities of this provision, laboratories should consult with appropriate legal counsel before information is disclosed under this provision.
- Law enforcement activities as required by law or pursuant to a court order, warrant, subpoena, summons, or discovery request. If the material is requested pursuant to an administrative subpoena or civil investigative demand, the request must be relevant and material to a legitimate law enforcement inquiry, limited in scope, and de-identified information cannot reasonably be substituted. As it may be difficult for many health care providers to make these determinations, providers should consult with appropriate counsel before information is provided to law enforcement officials under this provision. Additionally, these provisions allow disclosures (i) of limited information for identification and location purposes, (ii) in response to a law enforcement official's request about an individual who is, or is suspected to be, a victim of a crime, (iii) to alert law enforcement about an individual who has died, (iv) that the Company believes

in good faith constitute evidence of criminal conduct that occurred on the premises of the practice and (v) to report crime occurring during emergencies.

- Law enforcement activities for the purposes of identifying a victim or locating a suspect, fugitive, missing person or witness.
- Decedents and donated tissues and organs, including disclosures to coroners, medical examiners, funeral directors, organ procurement organizations, transplant centers, and eye or tissue banks.
- Research, including conducting epidemiological studies, evaluating outcomes, and other purposes, if an Institutional Review Board or Privacy Board determines, among other things, that the use or disclosure involves no more than a minimal risk to the privacy of individuals participating in the research.
- Serious threats to health or safety of the public at large. Information may only be disclosed if the Covered Entity believes the use or disclosure (1) is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and is to a person reasonably able to prevent or lessen the threat, including the target of the threat, or (2) necessary for law enforcement authorities to identify or apprehend an individual. This exception is limited by other applicable laws and standards of ethical conduct. Providers in California, for example, should be aware of privacy constraints imposed by the state constitution.
- Specialized government functions, such as the military, Secret Service, or national security activities and correctional facilities operations.
- Workers' compensation, to the extent required by state law.

[3] However, disclosure of a code or other means of re-identifying the information is considered the same as disclosing identified information to which the Standards would apply. If information is re-identified, the Company may use or disclose the information only as permitted or required by the Standards.

[4] The following are identifiers: names, all geographic subdivisions smaller than a state, including street address and zip codes (except for the initial three digits of a zip code if, according to current data available from the Bureau of the Census, the geographic unit formed by combining all zip codes with the same initial three digits contains more than 20,000 people, and the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000); all elements of dates (except year), for dates directly related to an individual, including birth date; and all ages over 89 and all elements of dates (including year), (except that ages may be aggregated into a category of age 90 or older); telephone numbers, fax numbers, e-mail addresses, social security numbers, medical record numbers, health plan beneficiary numbers, account numbers, certificate /license numbers, vehicle identification and serial numbers, including license plate numbers, device identifiers and serial numbers, Web Universal Resource Identifiers, Internet Protocol address numbers, biometric identifiers, full face photographic images and comparable images, and any other identifier from the record which could be used to identify an individual.

[5] The following identifiers must be removed to create a limited set: names, postal address information other than town, city, state, and zip code; telephone numbers; fax numbers; electronic mail addresses; social security numbers; medical record number; health plan beneficiary numbers; account numbers; certificate/license numbers; vehicle identifiers and serial numbers, including license plate numbers; device identifiers and serial numbers; URLs; IP (Internet Protocol) address numbers; biometric identifiers, including finger and voice prints; and full face photographic images any comparable images.

[6] Payment means the activities undertaken by a health care provider to obtain reimbursement for the provision of health care, including:

- Billing, claims management, and collection activities;
- Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
- Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and

- Disclosures to consumer reporting agencies of the following information: 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.

[7] Health care operations is broadly defined to mean the following:

- conducting quality assessment and improvement activities**,** including outcomes evaluation and development of clinical guidelines or protocols, population based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, and contacting health care providers and patients about treatment alternatives;
- reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, conducting training programs in which students 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;
- conducting or arranging for medical review, legal services and auditing services, including compliance programs;
- business planning and development, such as conducting cost-management and planning-related analyses; and
- business management and general administrative activities of the Company, including, customer service; resolution of internal grievances; creating de-identified information; the sale, transfer or consolidation of all or part of a covered entity with another covered entity or an entity that following such activity will become a covered entity and related due diligence; and creating a limited data set and fundraising.

[8] Even if state or other law does not demand the use of consents, the Company is free to use consents if it chooses. Additionally, there are special rules imposed on uses and disclosures for psychotherapy notes which impact the ability of a covered entity to use and disclose protected health information for these purposes. See 45 CFR § 164.508(a)(2).

[9] See the first two bullet points under footnote 7 for a list of permissible health care operation disclosures that may be made in this context.

[10] A patient's relationship with an ophthalmic practice typically qualifies as a direct treatment relationship. The Company would be in an indirect treatment relationship with a patient if (a) it provides treatment at the request of another provider and (b) it provides the services or products, or reports the diagnosis or results associated with the health care, directly to the health care provider who requested the service, who provides the services or products or reports to the patient.

[11] This requirement does not apply in emergency situations.

[12] For instance, if a patient arranges to be driven home after cataract surgery by a friend, who is assisting the patient with his care, Company personnel may disclose what kinds of post-surgical symptoms would require a call to the treating physician, but may not disclose information in the patient's medical record regarding other conditions which do not relate in any way with the patient's eye surgery.

[13] The provision of Section II(D)(2) and (3) only apply to such uses and disclosures to the extent the Company, in the exercise of its professional judgment, determines that the requirements do not interfere with its ability to respond to an emergency.

[14] For instance, if a patient brings her husband with her to meet with a physician, the physician may assume that the patient has agreed to the disclosure of protected health information to her husband.

[15] In general, the Privacy Standards require authorization in order to use or disclose PHI for marketing activities. Marketing, under the Privacy Standards, means (1) a communication about a product or service to encourage recipients to purchase or use the product or service or (2) an arrangement between a Covered Entity and a

third party where PHI is shared with the third party, for direct or indirect compensation, so the third party may make marketing communications about its own products and services. Although a Covered Entity must obtain an authorization to use or disclose PHI for marketing purposes, there are numerous exceptions to the definition of marketing. Marketing does not include communications made to an individual:

> (1) to describe the entities participating in a health care provider network, or to describe health-related products or services provided by the covered provider;
> (2) for treatment of that individual; or
> (3) for case management or care coordination for that individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to that individual.

Prescription refill reminders and appointment notifications fit within the exclusions above, so activities will not require individual authorization. In fact, authorization would not be required to use or disclose protected health information to market any health-related product or service of the Company **when marketed directly by the Company**. However, authorization is required to use or disclose protected health information to market the health-related product or service of a third party. Finally, the Company may engage in face-to-face marketing communications and to distribute promotional materials of nominal value, such calendars, pens, and mugs with logos, without having to obtain an authorization.

[16] See Exhibit 2 for the content requirements for authorizations.

[17] Reasons include:

- the expiration date has passed or the expiration event has occurred;
- it has been revoked;
- it has not been filled out completely, with respect to a required element;
- any material information contained in the authorization is known to be false; and
- the authorization is combined with another document in a way which inappropriately creates a compound authorization or the Company inappropriately conditioned treatment on the signature of the authorization.

[18] However, an authorization for the use and disclosure of protected health information for a specific research study may be combined with another type of written permission for the same study, such as a consent to participate in research. Additionally, the Company may combine an authorization, except for an authorization to use or disclose psychotherapy notes, with another authorization, except when the Company conditions treatment on the patient signing one of the authorizations.

[19] For instance, if the Company contracts with another company to provide examinations to establish fitness for work, the Company may condition such treatment on an individual signing an authorization that will allow the Company to disclose its findings to the company.

[20] The Company may elect not to treat a person as a personal representative if the Company, in the exercise of its professional judgment, decides that it is not in the best interest of the individual to do so and the Company has a reasonable belief that it is a situation where (a) domestic violence, abuse or neglect is present or (b) treating the person as the personal representative could endanger the individual.

[21] An emancipated minor is a person under eighteen (18) years who is totally self-supporting.

[22] The Company may not disclose more information than the representative is authorized to receive. For instance, if a personal representative is only given the power to make decisions about life saving treatment, the Company is not permitted to disclose the results of routine laboratory tests to the personal representative.

[23] If voices are kept appropriately low, for example, oral communications that commonly occur when health care providers coordinate services are permitted. The Company is also permitted to call out patient names in waiting rooms and to continue using sign-in sheets and X-ray light boards that may be visible to passers-by. While the

Company may use light boards, it must take reasonable precautions to protect imaging services and their patient labels from being viewed by the public.

[24] The IRB or Privacy Board must also provide documentation or represent that the requirements for waiver of authorization for uses and disclosures for research purposes have been met, where applicable.

[25] Such steps may include:

- requiring the business associate to submit periodic reports to the Company concerning its privacy practices;
- requiring the business associate to reacquire, at its expense, any information it inappropriately sold to a third party; or
- requiring, as a condition of keeping its contract with the Company, that the business associate terminate the employee of the business associate responsible for the breach.

If the Company is unable to correct or cure the business associate violation, it will terminate the agreement, where feasible. The Privacy Officer will have the authority to terminate a business associate contract, subject to the approval of the Company's management. Where there are no feasible alternatives to the business associate or terminating would be unreasonably burdensome on the Company, the Company may choose not to terminate. If the Company finds that it is not practical to terminate, it must notify the Secretary of its decision.

[26] Even if one of the Company's contracts qualifies for an extension, the Company should think carefully about deferring the Business Associate requirements. This is because without contractual obligations created by a Business Associate Agreement there is no way to require the Business Associate to assist the Company in its compliance efforts and obligations.

[27] In an emergency treatment situation, Notice must be provided as soon as reasonably practicable after the emergency.

[28] A covered entity may not apply a revision to information received or maintained prior to the revision unless it has reserved the right to do so in its Notice.

[29] The effective date of the Notice is the date it is printed or otherwise published.

[30] If the Company wishes to agree to requests for additional protections, then insert these policies:

(1) The Company will permit patients to make requests to restrict the Company's use and disclosure of protected health information for treatment, payment, health care operations or to persons assisting in a patient's care. Any such request will be directed to the Privacy Officer. The Privacy Officer may agree to the restriction, with the approval, or subject to the instructions of the Company's management.
(2) A restriction may not be imposed to prevent the use or disclosure of protected health information for the public policy-related uses and disclosures discussed in footnote 2 or required disclosures to the Secretary for compliance purposes.
(3) Information subject to the restriction will be marked, stamped or maintained in a separate file to notify Company personnel of the agreed upon restriction.
(4) If the Company agrees to a restriction, it will not use or disclose protected health information in violation of that restriction. However, it is permissible for the Company to use or disclose the information where the information is needed for emergency treatment of the individual. If a disclosure is made to another provider in the event of an emergency, the Company must request that the provider not further use or disclose the information.
(5) The Company may terminate an agreement to a restriction if the individual agrees to or requests the termination in writing, the individual orally agrees to the termination and the oral agreement is documented, or the Company informs the individual that it is terminating its agreement to a restriction, except that such termination is only effective with respect to protected health information created or received after it has so informed the individual.

(6) Restrictions agreed to by the Company will be documented in written form and maintained for six (6) years from the date they were created or last in effect, whichever is later.

[31] For example, if a patient would like to receive communications from the Company at her place of employment instead of her home, the Company will accommodate this request.

[32] If the Company decides that only written requests will be accepted, it must notify patients of this requirement. One way to do this is to include the requirement in the Company's Notice.

[33] The Company shall provide the requested access or send the individual a written notice of denial within thirty (30) days of the request. If the information is not maintained or accessible by the Company on-site, the Company must take action on the request within sixty (60) days. If the Company is unable to take the action required by this paragraph within the applicable timeframe, the Company may exercise a one time thirty (30) day extension, if the Company provides the individual with a written explanation for the delay and the date by which the Company will take final action on the request.

[34] The Company may provide the individual with a summary of the individual's protected health information instead of access to the records containing the information, if the individual agrees in advance to the summary and agrees to any fees associated with providing the summary.

[35] The charge may be based on the Company's costs for copying, including the cost of supplies and labor associated with the copying and postage, if applicable. No other fees may be charged for a request for access or copying.

[36] Those reasons are:

- the information is not contained within a designated record set;
- the information qualifies as psychotherapy notes;
- the records are being compiled in anticipation of litigation;
- the records are exempt from disclosure under the Clinical Laboratory Improvements Amendments ("CLIA");
- the information is created or obtained by the Company for clinical research, assuming the patient agreed to such as restriction;
- the information was obtained from someone other than a health care provider under a promise of confidentiality and access would be reasonably likely to reveal the source of the information;
- a licensed health care professional has determined, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;
- the information references another person and a licensed health professional has determined that the access is reasonably likely to cause harm to such other person; or
- the request is made by the patient's personal representative, and a licensed health professional has determined that the provision of access to the personal representative is reasonably likely to cause substantial harm to the patient or another person.

[37] If access to the information was denied under any of the last three bullet points set out in footnote 36, the denial must also state that the individual has a right to have the Company's decision reviewed by a licensed health care professional designated by the Company who did not participate in the original decision regarding access and explain how to exercise this right. Any such request will be promptly referred to such licensed health care professional. The review determination must be made within a reasonable period of time and the Company shall promptly provide notice of the determination. The Company must follow the determination made by the reviewer.

[38] This may be included in the Company's Notice.

[39] If the Company is unable to take the actions described above within sixty (60) days, the Company may have a one-time extension of no more than thirty (30) days, provided that within the initial sixty (60) day time

period, the Company supplies the patient a written statement of the reasons for the delay and the date by which the Company will complete its action on the request.

[40] The Company may reasonably limit the length of the statement of disagreement.

[41] The description must include the name or title, and telephone number of the contact person or office within the Company who will receive complaints.

[42] The Company will identify the record or protected health information in the designated record set which is the subject of the request for amendment and append or otherwise link the patient's request, the Company's denial, if any, the patient's statement of disagreement, if any, and the Company's rebuttal, if any. If a statement of disagreement is submitted by the patient, all future disclosures of the patient's protected health information which are the subject of the request for amendment must contain either (1) the materials described in the previous sentence or (2) an accurate summary of these materials. If the patient does not submit a statement of disagreement, all future disclosures will contain the patient's request for amendment and the Company's written denial or a summary of these materials, assuming the patient has requested this of the Company. When the subsequent disclosure by the Company is made using a standard electronic transaction which does not permit the inclusion of additional materials such as the ones described here, the Company may send the materials separately to its intended recipient.

[43] The Company must temporarily exclude disclosures to a health oversight agency or law enforcement official from the accounting, if the agency or official provides the Company with a written statement that an accounting would be reasonably likely to impede the agency or official's activities and specifies the time of the exclusion. If the agency or official statement is made orally, the Company must : (1) document the statement, including the identity of the agency or official making the statement, (2) temporarily suspend the patient's right to an accounting of the relevant disclosures and (3) limit the suspension to a thirty (30) day period unless a written statement of the type described above is submitted within the thirty (30) day period.

[44] Required information includes the date of the disclosure; the name of the entity or person who received the protected health information; and, if known, their last known address; and a brief description of the protected health information disclosed. The accounting must also contain a brief statement of the purpose or reason for the disclosure or, in lieu of the statement, a copy of a written request for disclosure from the Secretary or other appropriate party made pursuant to one of the public policy-related purposes discussed in the Privacy Standards. However, if the Company has made multiple disclosures of protected health information to the same person or entity for a single purpose to the Secretary or for one of the public policy-related disclosures discussed in footnote 2, the accounting may provide this information for the first disclosure during the accounting period; the frequency or number of the disclosures made during the accounting period; and the date of the last such disclosure during the accounting period. There are special rules for disclosures for research purposes. See 45 CFR § 164.528(b)(4)(i)-(ii).

The Company will document and maintain (1) the information required to be included in accountings, (2) accountings provided patients, (3) the titles of the persons or offices responsible for receiving and processing requests for an accounting and (4) statements by health care oversight agencies or law enforcement officials regarding the need to temporarily suspend a patient's right to an accounting. It will maintain this documentation for a period of six (6) years from the date is was created or last in effect, whichever is later.

[45] The Company may accomplish this through its Notice.