QUEST, INC.

POLICIES FOR PROTECTION OF THE PRIVACY

OF

PROTECTED HEALTH INFORMATION

Effective: April 14, 2003

Reviewed January 2011
Revised September 2012

QUEST, INC.

POLICIES FOR PROTECTION OF THE PRIVACY OF PROTECTED HEALTH INFORMATION

TABLE OF CONTENTS

QUEST, INC.

POLICIES FOR PROTECTION OF THE PRIVACY OF PROTECTED HEALTH INFORMATION

I. INTRODUCTION

A. Purpose of These Privacy Policies.

These privacy policies for the protection of the privacy of protected health information are intended to comply with the requirements of the federal Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), regulations under HIPAA, and any applicable state law that is more stringent than the HIPAA requirements. They are designed to comply with the standards, implementation specifications, and other requirements of the HIPAA security and privacy regulations at 45 CFR Part 160 and Part 164.

In all instances, these privacy policies shall be interpreted and construed consistent with the requirements of HIPAA, its regulations, and any more stringent state law.

In the event of any conflict between a provision of these privacy policies and a requirement of HIPAA, a regulation under HIPAA, or a more stringent state law, that HIPAA, HIPAA regulation, or state law requirement shall control.

B. Disclaimer.

All of the policies contained or referred to in these privacy policies, or that may be added or otherwise established by Quest, Inc. in the future, represent the policies established by Quest, Inc. for the members of its workforce in relation to the particular subject addressed by the policy. It is the intention of Quest, Inc. that these privacy policies be used by its employees, and other members of its workforce, in meeting their responsibilities to Quest, Inc. Violation of a policy can be the basis for discipline or termination of employment; however, because these privacy policies relate to the establishment and maintenance of high standards of performance, under no circumstances shall any policy be interpreted or construed as establishing a minimum standard, or any evidence of a minimum standard, of the safety, due care, or any other obligation which may be owed by Quest, Inc, its employees, or its agents to another person.

II. PROTECTED HEALTH INFORMATION

A. What is "Protected Health Information"?

"Protected health information" is any health information maintained by Quest, Inc. that is individually identifiable except employment records held by Quest, Inc. in its role as an employer.

"Individually identifiable health information" means any health information, including demographic information, whether oral or recorded in any form or medium, including demographic information collected from an individual, that:

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

2. 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,

3. That identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

All health information maintained by Quest, Inc. is individually identifiable unless and until it is de-identified as stated in Section II.B, below.

B. De-Identification of Health Information.

1. De-Identification.

Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.

2. Requirements for De-Identification.

Before any member of Quest, Inc.'s workforce treats any information as being de-identified, it must be submitted to the Privacy Office. Whether or not health information has been de-identified will be determined by the Privacy Office. The Privacy Office may find that health information has been de-identified only if one of the following two conditions are met:

a. Condition 1: Statistical and Scientific Principles.

A person with appropriate knowledge and experience with generally accepted statistical and scientific principles and methods for rendering information not individually indentifiable:

(1) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is subject to the information; and,

(2) Documents the methods and results of the analysis that justify such determination. Such documentation shall be in accordance with the requirements stated in Section III.N and Section III.O of these privacy policies.

b. Condition 2: Removal of Identifiers.

The following identifiers of the individual or of relatives, employers, or household members of the individual are removed and Quest, Inc. does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information:

(1) Names;

(2) All geographic subdivisions smaller than a State, including street addresses, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

(a) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and

(b) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

(3) 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;

(4) Telephone numbers;

(5) Fax numbers;

(6) Electronic mail addresses;

(7) Social security numbers;

(8) Medical record numbers;

(9) Health plan beneficiary numbers;

(10) Account numbers;

(11) Certificate/license numbers;

(12) Vehicle identifiers and serial numbers, including license plate numbers;

(13) Device identifiers and serial numbers;

(14) Web Universal Resource Locators (URLs);

(15) Internet Protocol (IP) address numbers;

(16) Biometric identifiers, including finger and voice prints;

(17) Full face photographic images and any comparable images; and,

(18) Any other unique identifying number, characteristic, or code, except as permitted by Section II.B.3 of these privacy policies.

3. Requirements for Re-Identification.

A code or other means of record identification may be assigned to allow information de-identified to be re-identified by Quest, Inc. provided:

a. The code or other means of record identification shall not be derived from or related to information about the individual and shall not otherwise be capable of being translated so as to identify the individual; and,

b. The code or other means of record identification shall not be used or disclosed for any other purpose and the mechanism for re-identification shall not be disclosed.

Whether or not information shall be coded for re-identification and be re-identified shall be determined by the Privacy Office. If information is re-identified, the Privacy Office shall oversee the process of doing so.

III. ADMINISTRATIVE POLICIES

A. Organizational Policies

Organizational policies regarding information defined as confidential or sensitive or private are found in the Employee Handbook, and Corporate Policy Manual. These policies include but are not limited to Electronic Communications, Social Security Numbers, Confidentiality, Recipient Rights, etc.

B. Designation of Privacy Office.

1. Designation.

Quest, Inc.'s President shall designate the Operations department as the Privacy Office, under the direct supervision of the Director of Operations, which shall be responsible for the development, updating and implementation of Quest, Inc.'s privacy policies.

2. Documentation.

Quest, Inc.'s President shall maintain, or cause to be maintained, a written or electronic record of the designation of the Privacy Office. Such record shall be maintained for six (6) years from the date of its creation or the date it is last in effect, whichever is later.

C. Designation of Other Persons.

1. Person/Office to Receive Complaints.

Quest, Inc.'s President shall designate a contact person or office who shall:

a. Be responsible for receiving complaints concerning Quest, Inc.'s privacy policies and procedures, Quest, Inc.'s compliance with those policies and procedures, or Quest, Inc.'s compliance with the HIPAA privacy rule pursuant to Section III.H of these privacy policies; and,

b. Provide further information about matters covered by Quest, Inc.'s Notice of Privacy Practices.

2. Person/Office to Receive and Process Requests for Access.

Quest, Inc.'s President shall designate a contact person or office who shall be responsible for receiving and processing individuals' requests for access to protected health information pursuant to Section VII.B "Right of Access" of these privacy policies.

3. Person/Office to Receive and Process Requests for Amendment.

Quest, Inc.'s President shall designate a contact person or office who shall be responsible for receiving and processing individuals' requests for amendment of protected health information pursuant to Section VII.C "Right to Request Amendment" of these privacy policies.

4. Documentation

Quest, Inc.'s President shall maintain, or cause to be maintained, a written or electronic record of the title of the person or office for each person or office designed under this Section III.C. Such record shall be maintained for six (6) years from the date of its creation or the date it was last in effect, whichever is later.

5. Identification of Workforce Members' Access To Protected Health Information

Attached to these privacy policies as Appendix A is an identification of those classes of Quest, Inc.'s workforce who need access to protected health information to carry out their duties and, for each of those classes, the category or categories of protected health information to which access is needed and any conditions appropriate to that access. Failure of a member of the workforce to comply with that access or those conditions will result in disciplinary action up to and including termination of employment.

At least annually, the Privacy Office shall cause a review of the identification and categories stated in Appendix A and make such changes to Appendix A as the Privacy Office determines is necessary or desirable to keep Appendix A current.

D. Training of Workforce.

All members of Quest, Inc.'s workforce shall be trained annually on Quest, Inc.'s policies and procedures with respect to protected health information as necessary and appropriate for the members of the workforce to carry out their functions within Quest, Inc..

Each member of the workforce on April 14, 2003, shall be trained by no later than April 14, 2003. Thereafter, each new member of the workforce shall be trained within thirty (30) calendar days after the person joins the workforce. Each member of the workforce whose functions are affected by a material change in these privacy policies or procedures shall be trained within thirty (30) calendar days after the material change becomes effective.

Documentation of the training for each member of the workforce shall be kept in written or electronic form for six (6) years after the date of its creation or the date that person ceases to be a member of Quest, Inc.'s workforce, whichever is later.

E. Safeguards to Protect the Privacy of Protected Health Information.

Option 1: The administrative, technical and physical safeguards that Quest, Inc. has in place to safeguard the privacy of protected health information and to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure are stated in Appendix B to these privacy policies.

At least annually, the Privacy Office shall cause a review of the safeguards stated in Appendix B and make such changes to Appendix B as the Privacy Office determines is necessary or desirable to keep Appendix B current.

Option 2: The Privacy Office shall implement appropriate administrative, technical and physical safeguards to protect the privacy of protected health information and to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure .

F. Receipt of Notice of Amended Protected Health Information.

Any member of Quest, Inc.'s workforce who is informed by another health care provider, health plan or a healthcare clearinghouse of an amendment to an individual's protected health information shall promptly inform the Privacy Office of the amendment. The Privacy Office shall cause the protected health information concerning that individual that is maintained by Quest, Inc. to be amended as stated in Section VII.C.4.a "Making the Amendment" of these privacy policies.

G. Process for Individuals to Make Complaints.

Individuals who desire to make a complaint against Quest, Inc. concerning Quest, Inc.'s privacy policies and procedures, its compliance with those policies and procedures, or the requirements of the HIPAA privacy rule shall submit the complaint to the Director of Operations in writing.

The Director of Operations shall investigate the complaint and respond to the individual in writing concerning his or her findings and what action, if any, Quest, Inc. will take in response to the complaint.

The Director of Operations shall cause written documentation of each complaint and its disposition to be kept in written or electronic form for six (6) years after the date of its creation or the date when it was last in effect, whichever is later.

H. Sanctions.

Except for actions that are covered by and meet the conditions of Section VI.G.15 "Disclosures by Whistleblowers", Section VI.G.16 "Disclosures by Workforce Members Who are Victims of a Crime"), or Section III.K "Prohibition on Intimidating or Retaliatory Acts" of these privacy policies, any member of Quest, Inc.'s workforce who fails to comply with Quest, Inc.'s privacy policies and procedures or the requirements of the HIPAA privacy rule shall be subject to sanctions imposed through Quest, Inc.'s discipline and discharge policies.

The Vice President of Human Resources shall cause written documentation of the sanctions that are applied, if any, to be kept in written or electronic form for six (6) years after the date of its creation or the date when it is last in effect, whichever is later.

I. Mitigation of Harmful Effect.

If there is a use or disclosure of protected health information by a member of Quest, Inc.'s workforce or an Quest, Inc. business associate in violation of Quest, Inc.'s privacy policies or the requirements of the HIPAA privacy rule, the Privacy Office shall mitigate, or cause to be mitigated, to the extent practicable, any harmful effect that is known to Quest, Inc..

J. Prohibition on Intimidating or Retaliatory Acts.

Neither Quest, Inc. nor any member of Quest, Inc.'s workforce may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against:

1. Individuals.

Any individual for the exercise by the individual of any right under, or for participation by the individual in any process established by, these privacy policies or the HIPAA privacy rule, including filing a complaint under the HIPAA privacy rule or under these privacy policies.

2. Individuals and Others.

Any individual or other person for:

a. Filing of a complaint with the Secretary of Health and Human Services under the HIPAA privacy rule;

b. Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under the Administrative Simplification provisions of HIPAA; or

c. Opposing any act or practice made unlawful by the HIPAA privacy rule, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of protected health information in violation of the HIPAA privacy rule.

K. Prohibition on Waiver of Rights.

No member of Quest, Inc.'s workforce may require an individual to waive the individual's rights under these privacy policies or the HIPAA privacy rule as a condition for the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

L. Changes to Policies and Procedures.

1. Changes in Law.

The Privacy Office shall promptly change these privacy policies as necessary and appropriate to comply with changes in the law, including changes in the HIPAA privacy rule. The changed policy or procedure shall be promptly documented and implemented. If the change materially affects the content of Quest, Inc.'s Notice of Privacy Practices, the Privacy Office shall promptly make the appropriate revisions to the notice in accordance with Section V.D "Revision of Notice of Privacy Practices" of these privacy policies.

2. Changes to Privacy Practices Stated In Notice of Privacy Practices.

When Quest, Inc. changes a privacy practice that is stated in its Notice of Privacy Practices and makes corresponding changes to its policies, the following actions shall be taken:

(a) The Privacy Office shall ensure that the policy or procedure, as revised to reflect the change, complies with the HIPAA privacy rule;

(b) The Privacy Office shall document the policy or procedure, as revised, is documented as stated in Section III.N "Documentation" and Section III.O "Period of Retention" of these privacy policies; and,

(c) The Privacy Office shall revise The Notice of Privacy Practices to state the changed practice and make the revised notice available as stated in Section V.B "Provision of Notice of Privacy Practices" of these policies. The changed practice may not be implemented prior to the effective date of the revised Notice of Privacy Practices.

The change shall be effective only with respect to protected health information created or received after the effective date of the revised Notice of Privacy practices.

3. Changes to Privacy Practices Not Stated In Notice of Privacy Practices.

Quest, Inc. may change, at any time, a privacy practice that does not materially affect the content of the Notice of Privacy Practices, provided:

a. The policy or procedure involved, as revised, complies with the HIPAA privacy rule; and,

b. Prior to the effective date of the change, the policy or practice, as revised, is documented by the Director of Operations by causing it to be kept in written or electronic form.

M. Documentation.

The Privacy Office shall take, or cause to be taken, each of the following actions:

a. Maintain these privacy policies and procedures in written or electronic form;

b. If a communication is required by these privacy policies and procedures, or by the privacy rule, to be in writing, maintain that writing, or an electronic copy, as documentation;

c. If an action, activity, or designation is required by these privacy policies and procedures, or by the privacy rule, to be documented, maintain a written or electronic record of that action, activity or designation.

N. Period of Retention.

Documentation required by Section III.N "Documentation", above, shall be retained for six (6) years from the date of its creation or the date when it last was in effect, whichever is later.

O. Business Associates.

Prior to Quest, Inc. disclosing any protected health information to a business associate or allowing a business associate to create or receive protected health information on its behalf, the Privacy Office shall obtain satisfactory assurance from the business associate that the business associate will appropriately safeguard the protected health information disclosed to it or that it creates or receives on Quest, Inc.'s behalf. The satisfactory assurance shall be through a written contract with the business associate the contains at least all the provisions required by the privacy rule.

However, if the business associate is required by law to perform a function or activity on behalf of Quest, Inc. or to provide a service described in the HIPAA privacy rule's definition of a business associate (see, Section IX.B, "Business Associate") to Quest, Inc., Quest, Inc. may disclose protected health information to the business associate to the extent necessary to comply with the legal mandate without meeting the requirements for business associates, provided:

1. Quest, Inc. attempts in good faith to obtain satisfactory assurances, as stated above; and,

2. If that attempt fails, the Director of Operations causes documentation of the attempt and the reasons that the assurances cannot be obtained.

Any contract of Quest, Inc. where the other party, or one of the other parties, may be a business associate shall be submitted to the Privacy Office for review for compliance with these privacy policies and the HIPAA privacy rule prior to being signed on behalf of Quest, Inc..

P. Reporting Violations.

Each member of Quest, Inc.'s workforce must report any actual or possible violation of Quest, Inc.'s privacy policies or the HIPAA privacy rule to the Privacy Office as soon as he or she becomes aware of the actual or possible violation.

Q. Questions Concerning HIPAA Compliance.

If any member of Quest, Inc.'s workforce has a question concerning Quest, Inc.'s privacy policies, the HIPAA privacy rule, or their application to any situation, he or she should contact the Privacy Office for guidance. The Privacy Office may contact legal counsel for legal advice as he or she believes is necessary or desirable.

R. Action by Designee.

Whenever an action may be or is required to be taken under these privacy policies by the Privacy Office, Director of Operations, or any other member of Quest, Inc.'s workforce, the action may be taken by that person's designee.

IV. QUEST, INC. REQUESTS FOR PROTECTED HEALTH INFORMATION

A. Generally.

When requesting protected health information from another health care provider, a health plan or a health care clearinghouse, a member of Quest, Inc.'s workforce must limit the request to that which is reasonably necessary to accomplish the purpose for which the request is made. Except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the request, members of Quest, Inc.'s workforce may not release an entire medical record.

B. Routine and Recurring Requests.

For a request that is made on a routine and recurring basis, the Privacy Office shall from time to time develop and implement standard protocols that limit the protected health information requested to the amount that is reasonably necessary to accomplish the purpose for which the request is made. The protocols established by the Privacy Office are set forth in Appendix C to these privacy policies.

C. Other Requests.

Whenever any member of Quest, Inc.'s workforce desires to request protected health information from another provider, a health plan or a health care clearinghouse and the request is not one made pursuant to a protocol for routine and recurring requests, he or she shall first submit the request to the Privacy Office for review and approval prior to the request being made. The Privacy Office shall review the request on an individual basis using the following criteria to limit the request to the information reasonably necessary to accomplish the purpose for which the request is made:

The criteria to be applied are:

a. Whether or not the information requested is related to the purpose of the request.

b. Whether or not the information requested will assist in the accomplishment of the purpose of the request.

c. Whether or not the purpose of the request can be accomplished without the information requested.

d. Whether or not the purpose of the request can be met with information that is not protected health information.

V. NOTICE OF PRIVACY PRACTICES

A. Form of Notice of Privacy Practices.

The Notice of Privacy Practices used by Quest, Inc. shall be established from time to time by the Privacy Office and shall meet the requirements of the HIPAA privacy regulations.

B. Provision of Notice of Privacy Practices.

1. To Each Person Served:

a. Generally.

Except in an emergency treatment situation, Quest, Inc.'s Notice of Privacy Practices shall be provided to any individual person served of Quest, Inc. (except to an inmate of a correctional institution) no later than the date of the first service delivery by Quest, Inc. and to other persons upon request. In an emergency treatment situation, Quest, Inc.'s Notice of Privacy Practices shall be provided as soon as reasonably practicable after the emergency treatment situation.

The Notice of Privacy Practices also shall be made available at Quest, Inc.'s office for individuals to request to take with them.

b. Via E-Mail.

If the individual agrees and that agreement has not been withdrawn, the Notice of Privacy Practices will be provided to that individual by e-mail in lieu of physical delivery. The transmission of the Notice of Privacy Practices by e-mail will be accomplished by the Privacy Office . If the e-mail transmission fails, a paper copy of the Notice of Privacy Practices will be provided to the individual. An individual who receives electronic notice may still obtain a paper copy of the notice upon request; his or her request should be submitted to the Privacy Office..

2. Posting.

Quest, Inc.'s Notice of Privacy Practices shall be prominently posted on the public communications board at 32231 Schoolcraft, Livonia, MI. 48150 .

3. Web Site.

Quest, Inc.'s Notice of Privacy Practices shall be prominently posted on Quest, Inc.'s web site and made available electronically through the web site.

C. Obtaining Acknowledgment of Receipt of Notice of Privacy Practices.

Except in an emergency treatment situation, the Quest, Inc. staff member who provides Quest, Inc.'s Notice of Privacy Practices to an individual in conjunction

with the date of first service delivery as state shall obtain a written acknowledgment of the individual's receipt of the Notice of Privacy Practices. The written acknowledgment shall be obtained through written signature on the acknowledgment form which will be maintained in the individual's main record.

If the individual's written acknowledgment cannot be obtained, the staff member(s) who attempted to obtain it shall document their good faith efforts to obtain the acknowledgment and the reason why it was not obtained. That documentation shall be obtained through written signature on the acknowledgment form which will be maintained in the individual's main record.

D. Revision of Notice of Privacy Practices.

Whenever there is a material change to the uses or disclosures, the individual's rights, Quest, Inc.'s legal duties, or other privacy practices stated in the notice, the Privacy Office shall cause the Notice of Privacy Practices to be promptly revised, made available on request and distributed.

Except when the material change is required by law, a material change to any term of the Notice of Privacy Practices shall not be implemented prior to the effective date of the Notice of Privacy Practices in which the material change is reflected.

E. Documentation.

A copy of each Notice of Privacy Practices used by Quest, Inc. and of each written acknowledgment of receipt of the notice or documentation of good faith efforts to obtain such acknowledgment shall be maintained by Quest, Inc. in written or electronic form for six (6) years after the date the notice was last in effect.

VI. USES AND DISCLOSURE OF PROTECTED HEALTH INFORMATION

A. General Rule.

Except as otherwise stated in this Section VI, Quest, Inc. shall obtain the individual's written authorization in accordance with these privacy policies, prior to using or disclosing protected health information concerning the individual.

B. Incidental Uses and Disclosures.

A use or disclosure that is incidental to a use or disclosure that otherwise permitted or required by these privacy policies or the HIPAA privacy rule is permissible provided: (1) the applicable requirements of Section VI.C "Use and Disclosure of Only the Minimum Necessary Information", below; and, (2) reasonable safeguards have been applied to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure (see, Section III.F, "Safeguards to Protect the Privacy of Protected Health Information"

C. Use and Disclosure of Only the Minimum Necessary Information.

1. General Rule.

Except as stated in Section VI.C.2, below, when using or disclosing protected health information, members of Quest, Inc.'s workforce shall make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use or disclosure.

2. Exceptions to Minimum Necessary Requirement.

The preceding general rule concerning limiting use and disclosure of protected health information to the minimum necessary does not apply to:

a. Disclosures to a health care provider for treatment.

b.

c. Uses or disclosures made to the individual.

d. Uses or disclosures made pursuant to a written authorization in accordance with these privacy policies.

e. Disclosures made to the Secretary of Health and Human Services in accordance with the HIPAA privacy rule.

f. Uses or disclosures that are required by law.

g. Uses or disclosures that are required for Quest, Inc.'s compliance with the HIPAA privacy rule.

3. Routine and Recurring Disclosures.

For any type of disclosure that is made on a routine and recurring basis, the Privacy Office shall from time to time develop and implement standard protocols that limit the protected health information requested to the amount that is reasonably necessary to accomplish the purpose for which the disclosure is made. The protocols established by the Privacy Office are set forth in Appendix D to these privacy policies.

4. Other Disclosures.

Any disclosures that are not covered by an established protocol, shall be reviewed by the Privacy Office on an individual basis using the following criteria to limit the protected health information disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought.

The criteria to be applied are:

a. Whether or not the information requested is reasonably related to the purpose of the request.

b. Whether or not the information requested will assist in the accomplishment of the purpose of the request.

c. Whether or not the purpose of the request can be accomplished without the information requested.

d. Whether or not the purpose of the request can be met with information that is not protected health information.

5. Permitted Reliance.

If the reliance is reasonable under the circumstances, members of Quest, Inc.'s workforce may rely on a requested disclosure as the minimum necessary for the stated purpose when:

a. Making disclosures to public officials that are permitted under Section VI.G "Uses and Disclosures for which an Authorization or an Opportunity to Agree or Object is Not Required" of these privacy policies, if the public official represents that the information is the minimum necessary for the stated purpose(s);

b. The information is requested by another covered entity;

c. The information is requested by a professional who is a member of Quest, Inc.'s workforce or a business associate of Quest, Inc. for the purpose of providing professional services to Quest, Inc., if the professional represents that the information requested is the minimum necessary for the stated purpose(s); or,

d. Documentation or representations that comply with the applicable requirements of Section VI.G.10 "Uses and Disclosures for Research Purposes" of these privacy policies have been provided by the person requesting the information for research purposes.

The basis for reliance under this Section VI.C.5 shall be documented by the Privacy Office. That documentation shall be maintained in the person served's central record.

D. Uses and Disclosures to Carry Out Treatment, Payment and Health Care Operations.

Quest, Inc. may use or disclose protected health information, as follows:

1. To the individual.

2. For its own treatment, payment, or health care operations.

3. For treatment activities of a health care provider.

4. To anther entity covered by the privacy rule or a health care provider for the

payment activities of the entity that receives the information.

5. To another entity covered by the privacy rule for health care operations of the entity that receives the information, if Quest, Inc. and that other entity has or have had a relationship with the individual who is the subject of the protected health information being requested, the protected health information pertains to that relationship, and the disclosure is:

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

   b. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities

   c. For the purpose of health care fraud and abuse detection or compliance.

E. Uses and Disclosures for Which an Authorization is Required.

1. General Rule.

Except as otherwise permitted or required by these privacy policies, Quest, Inc. will not use or disclose protected heath information without an authorization that is valid under this Section VI.E. When Quest, Inc. obtains or receives a valid authorization for its use or disclosure of protected health information, Quest, Inc.'s use or disclosure must be consistent with that authorization.

2. Psychotherapy Notes.

Notwithstanding any provision of these privacy policies, other than the transition provisions in Section VI.L "Prior Authorizations, Quest, Inc. will obtain an authorization for any use or disclosure of psychotherapy notes , except:

   a. To carry out the following treatment, payment, or health care operations:

      (1) Use by the originator of the psychotherapy notes for treatment;

(2) Use or disclosure by Quest, Inc. in its own training programs in which students, trainees, employees or practitioners in mental health learn under supervision to practice or improve their skills, or,

(3) Use or disclosure by Quest, Inc. to defend a legal action or other proceeding brought by the individual; and,

b. A use or disclosure that is:

(1) Required by Section VI.G.14 "Disclosure to the Secretary of Health and Human Services" of these privacy policies concerning "Disclosures to the Secretary of Health and Human Services";

(2) Permitted by Section VI.G.2 "Uses and Disclosures Required by Law" of these privacy policies concerning "Uses and Disclosures Required by Law";

(3) Permitted by Section VI.G.5 "Uses and Disclosures for Health Oversight Activities" of these privacy policies with respect to the oversight of the originator of the psychotherapy notes;

(4) Permitted by Section VI.G.8.b "Uses and Disclosures About Decedents" of these privacy policies concerning "Coroners and Medical Examiners"; or,

(5) Permitted by Section VI.G.11.b.(1) "Serious and Imminent Threat" of these privacy policies concerning "Serious and Imminent Threat".

3. What is a Valid Authorization?

An authorization is valid if it contains all the elements required by Section VI.E.6 "Form of Authorization" of these privacy policies and it is not defective.

An authorization is defective if the document has any of the following defects:

a. The expiration date has passed or the expiration event is known by Quest, Inc. to have occurred.

b. The authorization has not been filled out completely with respect to an element required to be included in the authorization;

c. The authorization is known by Quest, Inc. to have been revoked;

d. The authorization lacks a required element (see, Section VI.E.6,

"Form of Authorization" of these privacy policies;

e. The authorization violates the requirements concerning compound authorizations (see, Section VI.E.7, "Compound Authorizations");

f. The authorization violates the requirements concerning conditioning of authorizations (see, Section VI.E.5, "Prohibition on Conditioning of Authorizations"); or,

g. If any material information in the authorization is known by Quest, Inc. to be false.

If any member of Quest, Inc.'s workforce believes an authorization is defective for any reason, he or she should promptly report that fact and the basis for his or her belief to the Privacy Office.

4. Maintaining an Authorization.

All authorizations shall be delivered to the Privacy Office who will assure that the information is filed in the person served's central record.

5. Conditioning of Authorizations.

a. General Rule.

Except as stated in Section VI.E.5.b "Exceptions", below, Quest, Inc. will not condition treatment or payment to an individual on the receipt of an authorization from that individual.

b. Exceptions.

Quest, Inc. may condition treatment or payment to an individual on the receipt of an authorization from that individual in the following situations:

(1) Research. Quest, Inc. may condition the provision of research-related treatment on provision of an authorization for the use or disclosure of protected health information for such research .

(2) Disclosure Is Sole Purpose. Quest, Inc. may condition the provision of health care that is solely for the purpose of creating protected health information for disclosure to a third party on provision of an authorization for the disclosure of the protected health information to that third party.

6. Form of Authorization.

a. Required Elements. An authorization must contain at least the following elements:

(1) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.

(2) The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.

(3) The name or other specific identification of the person (s), or class of persons, to whom Quest, Inc. may make the requested use or disclosure.

(4) 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 an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose.

(5) An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. The statement "end of the research study," "none," or similar language is sufficient if the authorization is for a use or disclosure of protected health information for research, including for the creation and maintenance of a research database or research repository.

(6) A statement of the individual's right to revoke the authorization in writing and either:

(a) The exceptions to the right to revoke, together with a description of how the individual may revoke the authorization; or,

(b) To the extent that the information is stated in the Notice of Privacy Practices a reference to that notice.

(7) A statement of the ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization by stating either:

(a) That the covered entity may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization when the prohibition on conditioning of authorizations applies; or,

(b) The consequences to the individual of a refusal to sign the authorization when the privacy rule permits the entity to condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain the authorization.

(8) A statement that information used or disclosed pursuant to the authorization may be subject to redisclosure by the recipient and no longer be protected by the privacy rule;

(9) Signature of the individual and date; and,

(10) If the authorization is signed by a personal representative of the individual, a description of that personal representative's authority to act for the individual.

b. Additional Elements.
An authorization may contain elements or information in addition to the elements stated in Section VI.E.6.a, above, concerning "Required Elements", provided those additional elements or information are not inconsistent with the elements required by this Section VI.E.

c. Plain Language.
An authorization must be written in plain language.

d. Copy to Individual.
If Quest, Inc. seeks an authorization from an individual for use or disclosure of protected health information, Quest, Inc. will provide the individual will a copy of the signed authorization.

7. Compound Authorizations.

a. General Rule.
Except as stated in Section VI.E.7.b, below, an authorization for use or disclosure of protected health information may not be combined with any other document to create a compound authorization.

b. Exceptions.
Notwithstanding Section VI.E.7.a, above, an authorization for use or disclosure of protected health information may be combined with any other document to create a compound authorization in the following situations:

(1) An authorization for the use or disclosure of protected health information created for a research study may be combined

with any other type of written permission for the same research study, including another authorization for the use or disclosure of protected health information for such research or a consent to participate in such research;

(2) An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes;

(3) An authorization, other than an authorization for a use or disclosure of psychotherapy notes, may be combined with any other authorization, except when Quest, Inc. has conditioned the provision of treatment or payment under Section VI.E.5.b "Exceptions" of these privacy policies on the provision of one of the authorizations.

8. Revocation of an Authorization.

An individual has the right to revoke an authorization in writing, except to the extent Quest, Inc. has taken action in reliance thereon.

A written revocation should be submitted to the Privacy Office who will cause the revocation to be filed in the person served's central record.

9. Documentation.

The Privacy Office will document and retain any signed authorizations under this section in writing, or an electronic copy, for six (6) years from the date of its creation or the date when it was last in effect, whichever is later.

F. Uses and Disclosures Requiring an Opportunity for the Individual to Agree or to Object.

1. General Rule.

Members of Quest, Inc.'s workforce may use or disclose protected health information without the individual's written authorization for the purposes described in this Section VI.F provided:

a. The individual is informed orally or in writing in advance of the use or disclosure; and,

b. The individual has an opportunity to agree to or prohibit or restrict the disclosure in accordance with the requirements of this Section VI.F.

2. Facility Directories.

a. Use and Disclosure.

Except when an objection is expressed by the individual, Quest, Inc. may:

(1) Use the following protected health information to maintain a directory of individuals in the facility:

(a) The individual's name;

(b) The individual's location in Quest, Inc.'s facility;

(c) The individual's condition described in general terms that does not communicate specific medical information about the individual; and,

(d) The individual's religious affiliation.

(2) Disclose for directory purposes that information:

(a) To members of the clergy; or,

(b) Except for religious affiliation, to other persons who ask for the individual by name.

b. Opportunity to Object.

The Privacy Office will inform an individual of the protected health information that it may include in a directory and the persons to whom it may disclose that information (including disclosures to clergy of information regarding religious affiliation) and provide the individual with the opportunity to restrict or prohibit some or all of the uses or disclosures permitted by this Section VI.F.2. The Privacy Office will document that opportunity and the agreement, restriction, or objection in the person served's central record.

c. Incapacity or Emergency Circumstance.

If the Privacy Office determines that the opportunity to object to uses or disclosures for directory purposes cannot practicably be provided because of the individual's incapacity or an emergency treatment circumstance, Quest, Inc. will use or disclose some or all of the protected health information permitted by this Section VI.F.2, if the disclosure is:

(1) Consistent with a prior expressed preference of the individual, if any, that is known to Quest, Inc.; and,

(2) In the individual's best interest as determined by Quest, Inc., in the exercise of professional judgment.

The Privacy Office will inform the individual and provide an opportunity to object to uses or disclosures for directory purposes when it becomes practicable to do so.

The Privacy Office will document the incapacity or emergency, how the use is consistent and in the individual's best interest in the person served's central record. The Privacy Office will also document the provision of the opportunity to object later and whether or not the individual stated any objection or restriction.

3. Persons Involved in the Individual's Care; Notification.

a. General Rules.

(1) Those Involved in Care. Members of Quest, Inc.'s work-force may, in accordance with Sections VI.F.3.b and VI.F.3.c, below, disclose to a family member, other relative, or a close personal friend of the individual, or to any other person identified by the individual, the protected health information directly relevant to that person's involvement with the individual's care or payment related to that individual's health care.

(2) Notification of Location, Condition, or Death. Members of Quest, Inc.'s workforce may use or disclose protected health information to notify, or assist in the notification of (including identifying or locating) a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition or death. Any such use or disclosure must be in accordance with Section VI.F.3.b, VI.F.3.c, or VI.F.4, below.

b. When the Individual Is Present.

If the individual is present for, or otherwise available prior to, a use or disclosure to a person(s) involved in the individual's care and the individual has the capacity to make health care decisions, a member of Quest, Inc.'s workforce may use or disclose the protected health information if he or she:

(1) Obtains the individual's agreement;

(2) Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or,

(3) Reasonably infers from the circumstances, based on the exercise of professional judgment, that the individual does not object to the disclosure.

The Quest, Inc. workforce member shall document in the person served's central record which of the preceding reasons were the basis for the use or disclosure.

c. When the Individual Is Not Present.

(1) Incapacity; Emergency Circumstances. If the individual is not present for, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, a member of Quest, Inc.'s workforce may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's health care.

The Quest, Inc. workforce member shall document in the person served's central record the individual's incapacity or the emergency and why he or she determined the disclosure was in the individual's best interests.

(2) Other Actions. A member of Quest, Inc.'s workforce may use professional judgment and experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of protected health information.

The Quest, Inc. workforce member shall document in the person served's central record the individual's incapacity or the emergency and why he or she determined the disclosure was in the individual's best interests.

4. Disaster Relief.

A member of Quest, Inc.'s workforce may use or disclose protected health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, *e.g.*, the Red Cross, for the purpose of coordinating with such entities the uses and disclosures permitted by Section VI.F.3 "Persons Involved in the Individual's Care; Notification" concerning notification of location, condition or death. However, the requirements of Sections VI.F.3.b "When the Individual Is Present" and VI.F.3.c "When the Individual Is Not Present" of these privacy policies apply to those uses and disclosures to the extent that the Quest, Inc. workforce member, in the exercise of professional judgment, determines that those requirements do not interfere with the ability to respond to the emergency circumstances.

G. Uses and Disclosures for which an Authorization or an Opportunity to Agree or Object is Not Required.

1. General Rules.

To the extent permitted by this Section VI.G, an authorized member of Quest, Inc.'s workforce may use or disclose protected health information without the authorization of the individual or the opportunity of the individual to agree or object, in the situations described in this Section VI.G.

When Quest, Inc. is required by any of these situations to inform the individual of a use or disclosure permitted by this Section VI.G or when the individual may agree to a use or disclosure required by this Section VI.G, Quest, Inc.'s information and the individual's agreement may be given orally. However, if given orally, the Quest, Inc. workforce member involved shall document the giving of the information or the agreement by written note in the person served's central record.

2. Uses and Disclosures Required by Law.

a. Informing the Privacy Office.

Any member of Quest, Inc.'s workforce who receives a request, or who proposes, to use or disclose protected health information for a use or disclosure required by law must promptly deliver or otherwise communicate the request or proposal to the Privacy Office prior to the use or disclosure being made. The Privacy Office will then oversee the use or disclosure for compliance with these privacy policies. The use or disclosure should not occur until it has been approved by the Privacy Office.

b. Permitted Uses and Disclosures.

Quest, Inc. may use or disclose protected health information to the extent that the use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of the law.

Quest, Inc. will meet the requirements of the following sections of these privacy policies, as applicable, for uses and disclosures required by law:

(1) Section VI.G.4 "Uses and Disclosures About Victims of Abuse, Neglect or Domestic Violence"

(2) Section VI.G.6 "Disclosures for Judicial and Administrative Proceedings"; and,

(3) Section VI.G.7 "Disclosures for Law Enforcement Purposes".

3. Uses and Disclosures for Public Health Activities.

a. Informing the Privacy Office.

Any member of Quest, Inc.'s workforce who receives a request, or who proposes, to use or disclose protected health information for public health activities must promptly deliver or otherwise communicate the request or proposal to the Privacy Office prior to the use or disclosure being made. The Privacy Office will then oversee the use or disclosure for compliance with these privacy policies. The use or disclosure should not occur until it has been approved by the Privacy Office.

b. Permitted Disclosures.

An authorized member of Quest, Inc.'s workforce may disclose protected health information for the public health activities and purposes described below:

(1) A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including but not limited to, the reporting of disease, injury and vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of the public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority;

(2) A public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect;

(3) A person subject to the jurisdiction of the United States Food and Drug Administration (FDA) with respect to an FDA - regulated product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity. Such purposes include:

(a) To collect or report adverse events (or similar activities with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations;

(b) To track FDA-regulated products;

(c) To enable product recalls, repairs, or replacement, or lookback (including locating and notifying individuals who have received products that have been recalled, withdrawn, or are the subject of lookback); or,

(d) To conduct post marketing surveillance.

(4) A person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if Quest, Inc. or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation; or

(5) An employer, about an individual who is a member of the workforce of the employer, if:

(a) Quest, Inc. provides health care to the individual at the request of the employer:

i) To conduct an evaluation relating to medical surveillance of the workplace; or,

ii) To evaluate whether the individual has a work-related illness or injury; or,

(b) The protected health information that is disclosed consists of findings concerning a work-related illness or injury or a work-related medical surveillance;

(c) The employer needs such findings in order to comply with its obligations under 29 CFR Parts 1904 through 1928 (concerning occupational safety and health), 30 CFR parts 50 through 90 (concerning mine safety and health), or similar state law, to record such illness or injury or to carry out responsibilities for workplace medical surveillance; and,

(d) Quest, Inc. provides written notice to the individual that protected health information relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed by the employer:

i) By giving a copy of the notice to the individual at the time the health care is provided; or

ii) If the health care is provided on the work site of the employer, by posting the notice in a prominent place at the location where the health care is provided.

4. Uses and Disclosures About Victims of Abuse, Neglect or Domestic Violence.

a. Delivery to Privacy Office.

Any member of Quest, Inc.'s workforce who receives a request, or who proposes, to use or disclose protected health information about a victim of abuse, neglect or domestic violence must promptly deliver or otherwise communicate the request or proposal to the Privacy Office prior to the use or disclosure being made. The Privacy Office will then oversee the use or disclosure for compliance with these privacy policies. The use or disclosure should not occur until it has been approved by the Privacy Office.

b. General Rule.

Except for reports of abuse or neglect that are permitted by Section VI.G.3.b.(2) "Permitted Disclosures" of these privacy policies, an authorized member of Quest, Inc.'s workforce may disclose protected health information about an individual that workforce member reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect or domestic violence:

(1) To the extent the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of that law;

(2) If the individual agrees to the disclosure; or,

(3) To the extent the disclosure is expressly authorized by statute or regulation and:

(a) The Quest, Inc. workforce member, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the individual or other potential victim; or,

(b) If the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that:

i) The protected health information for which disclosure is sought is not intended to be used against the individual; and,

ii) An immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

c. Informing the Individual.

If a member of Quest, Inc.'s workforce makes a disclosure permitted by VI.G.4.b "General Rule", above, the Privacy Office shall promptly inform the individual that such a report has been or will be made, except if:

(1) The Privacy Office, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or

(2) The Privacy Office would be informing a personal representative, and he or she reasonably believes the personal representative is responsible for the abuse, neglect or other injury, and that informing that person would not be in the best interests of the individual as determined by Quest, Inc., in the exercise of professional judgment.

5. Uses and Disclosures for Health Oversight Activities.

a. Delivery to Privacy Office.

Any member of Quest, Inc.'s workforce who receives a request, or who proposes, to use or disclose protected health information for purposes of a health oversight activity must promptly deliver or otherwise communicate the request or proposal to the Privacy Office prior to the use or disclosure being made. The Privacy Office will then oversee the use or disclosure for compliance with these privacy policies. The use or disclosure should not occur until it has been approved by the Privacy Office.

b. General Rule.

An authorized member of Quest, Inc.'s workforce may disclose protected health information to a health oversight agency, *e.g.*, state department of health, CMS, for oversight activities authorized by law, including: audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or other actions; or, other activities necessary for appropriate oversight of:

(1) The health care system;

(2) Government benefit programs for which health information is relevant to beneficiary eligibility;

(3) Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or,

(4) Entities subject to civil rights laws for which health information is necessary for determining compliance.

c. Exceptions.

For purposes of the disclosures permitted by Section VI.G.5.b "General Rule", above, a health oversight activity does not include an investigation or other activity in which the individual is the subject of the investigation or activity and such investigation or other activity does not arise out of and is not directly related to:

(1) The receipt of health care;

(2) A claim for public benefits related to health; or,

(3) Qualification for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or services.

d. Joint Activities or Investigations.

Notwithstanding the exceptions stated in Section VI.G.5.c, above, if a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health, the joint activity or investigation is considered a health oversight activity for purposes of this section.

6. Disclosures for Judicial and Administrative Proceedings.

a. Delivery to Privacy Office.

Any member of Quest, Inc.'s workforce who receives an order of a court or administrative tribunal or a subpoena, discovery request, or other lawful process must promptly deliver or otherwise communicate the document to the Privacy Office prior to the disclosure being made. The Privacy Office will then oversee the disclosure for compliance with these privacy policies. The disclosure should not occur until it has been approved by the Privacy Office.

b. General Rules.

Quest, Inc. will disclose protected health information in the course of any judicial or administrative proceeding:

(1) In response to an order of a court or administrative tribunal, provided Quest, Inc. will disclose only the protected health information expressly authorized by the order; or,

(2) In response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal, if:

(a) Quest, Inc. receives satisfactory assurance, as described below, from the party seeking the information that reasonable efforts have been made by that party to ensure that the individual who is the subject of the protected health information that has been requested has been given notice of the request; or,

(b) Quest, Inc. receives satisfactory assurance, as described below, from the party seeking the information that reasonable efforts have been made by that party to secure a qualified protective order that meets the requirements stated below.

(c) Notwithstanding (a) and (b), above, Quest, Inc. may disclose protected health information in response to a subpoena, discovery request or other lawful process that is not accompanied by an order of the court or administrative tribunal, without satisfactory assurance, if Quest, Inc., itself:

i) Makes reasonable efforts to provide notice to the individual sufficient to meet the requirements stated below for satisfactory assurance of such a notice; or ,

ii) Seeks a qualified protective order sufficient to meet the requirements stated below for a qualified protective order.

c. Satisfactory Assurance.

(1) That Individual Has Received Notice. Quest, Inc. will be considered to have received "satisfactory assurance" from a party seeking protected health information that the individual has received notice if Quest, Inc. receives from that party a written statement and accompanying documentation demonstrating that:

(a) The party requesting the information has made a good faith attempt to provide written notice to the individual (or, if the individual's location is unknown, to mail a notice to the individual's last known address);

(b) The notice included sufficient information about the litigation or proceeding in which the protected health information is requested to permit the individual to raise an objection to the court or administrative tribunal; and,

(c) The time for the individual to raise objections to the court or administrative tribunal has elapsed, and:

i) No objections were filed; or,

ii) All objections filed by the individual have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with that resolution.

(2) That Qualified Protected Order Sought. Quest, Inc. will be considered to have received "satisfactory assurance" from a party seeking protected health information that a qualified protected order has been sought if Quest, Inc. receives from that party a written statement and accompanying documentation demonstrating that:

(a) The parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or,

(b) The party seeking the protected health information has requested a qualified protected order from that court or administrative tribunal.

(3) Meaning of "Qualified Protective Order". A "qualified protective order" means an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:

(a) Prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which the information was requested; and,

(b) Requires the return to Quest, Inc. or destruction of the protected health information (including all copies made) at the end of the litigation or proceeding.

d. Not Limitation on Other Uses and Disclosures.
The provisions of this section dealing with disclosures for judicial and administrative proceedings do not supersede other provisions of these privacy policies that otherwise permit or restrict uses of disclosures of protected health information.

7. Disclosures for Law Enforcement Purposes.

a. Delivery to Privacy Office.

Any member of Quest, Inc.'s workforce who receives a request, or proposes, to disclose protected health information for law enforcement purposes must promptly deliver or otherwise communicate the request or proposal to the Privacy Office prior to the disclosure being made. The Privacy Office will then oversee the use or disclosure for compliance with these privacy policies. The use or disclosure should not occur until it has been approved by the Privacy Office.

b. Pursuant to Process and As Otherwise Required by Law.
An authorized member of Quest, Inc.'s workforce may disclose protected health information:

(1) As required by law including laws that require the reporting of certain types of wounds or other physical injuries, except:

(a) For laws concerning a public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect (see, Section VI.G.3.b.(1) "Permitted Disclosures"); or,

(b) To the extent the disclosure is pursuant to a mandatory reporting law concerning reporting of abuse, neglect, or domestic violence and the disclosure complies with and is limited to the relevant requirements of that law (see, Section VI.G.4.b.(1).

(2) In compliance with and as limited by relevant requirements of:

(a) A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;

(b) A grand jury subpoena; or,

(c) An administrative reQuest, Including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that:

i) The information sought is relevant and material to a legitimate law enforcement inquiry;

ii) The request is specific and limited in scope to the extent reasonably practical in light of the purpose for which the information is sought; and,

iii) De-identified information could not reasonably be used.

(For verification of an administrative request see Section VI.K.3.a, "Conditions on Disclosures".)

c. Limited Information for Identification and Location Purposes.

Except for disclosures required by law as permitted by VI.G.7.b, VI.G.7.b, above, an authorized member of Quest, Inc.'s workforce may disclose protected health information in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that:

(1) Quest, Inc. may disclose only the following information:
   (a) Name and address;
   (b) Date and place of birth;
   (c) Social security number;
   (d) ABO blood type and rh factor;
   (e) Type of injury;
   (f) Date and time of treatment;
   (g) Date and time of death, if applicable; and,
   (h) A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence of absence of facial hair (beard or moustache), scars, and tattoos.

(2) Except as stated in (1), above, a member of Quest, Inc.'s workforce may not disclose for the purposes of identification or location under this section any protected health information related to the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.

d. Victims of a Crime.

Except for disclosures required by law as permitted by VI.G.7.b, VI.G.7.b, above, an authorized member of Quest, Inc.'s workforce may disclose protected health information in response to a law enforcement official's request for such information about an individual who is or is suspected to be a victim of a crime, other than disclosures that are subject to Section VI.G.7.b, VI.G.7.b and Section VI.G.7.c, if:

(1) The individual agrees to the disclosure; or,

(2) Quest, Inc. is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, provided that:

   (a) The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim;

(b) The law enforcement official represents that immediate law enforcement activity that depends on the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and,

(c) The disclosure is in the best interests of the individual as determined by Quest, Inc., in the exercise of professional judgment.

e. Decedents.

An authorized member of Quest, Inc.'s workforce may disclose protected health information about an individual who has died to a law enforcement official for the purpose of alerting law enforcement of the death of the individual if Quest, Inc. has a suspicion that such death may have resulted from criminal conduct.

f. Crime on the Premises.

An authorized member of Quest, Inc.'s may disclose to a law enforcement official protected health information that he or she believes in good faith constitutes evidence of criminal conduct that occurred on the premises of Quest, Inc..

g. Reporting Crime in Emergencies.

If Quest, Inc. is providing emergency health care in response to a medical emergency, other than on the premises of Quest, Inc., an authorized member of Quest, Inc.'s workforce may disclose protected health information to a law enforcement official if such disclosure appears necessary to alert law enforcement to:

(1) The commission and nature of a crime;

(2) The location of such crime or of the victim(s) of such crime; and,

(3) The identity, description, and location of the perpetrator of the crime.

If the member of Quest, Inc.'s workforce believes the medical emergency is the result of abuse, neglect, or domestic violence of the individual in need of emergency health care, the preceding does not apply and any disclosure to a law enforcement official for law enforcement purposes is subject to Section VI.G.7.c.

8. Uses and Disclosures About Decedents.

a. Delivery to Privacy Office.

Any member of Quest, Inc.'s workforce who receives a request, or proposes, to use or disclose protected health information to a coroner, medical examiner, or funeral director must promptly deliver or otherwise communicate the request or proposal to the Privacy Office prior to the use or disclosure being made. The Privacy Office will then oversee the use or disclosure for compliance with these privacy policies. The use or disclosure may not occur until it has been approved by the Privacy Office.

b. Coroners and Medical Examiners.

An authorized member of Quest, Inc.'s workforce may disclose protected health information to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law.

c. Funeral Directors.

An authorized member of Quest, Inc.'s workforce may disclose protected health information to funeral directors consistent with applicable law, as necessary to carry out their duties with respect to the decedent. If necessary for funeral directors to carry out their duties, Quest, Inc. may disclose the protected health information prior to, and in reasonable anticipation of, the individual's death.

9. Uses and Disclosures for Cadaveric Organ, Eye or Tissue Donation.

a. Delivery to Privacy Office.

Any member of Quest, Inc.'s workforce who receives an a request, or proposes, to use or disclose protected health information for purposes of cadaveric organ, eye or tissue donation must promptly deliver or otherwise communicate the request or proposal to the Privacy Office prior to the use or disclosure being made. The Privacy Office will then oversee the use or disclosure for compliance with these privacy policies. The use or disclosure may not occur until it has been approved by the Privacy Office.

b. Permitted Uses and Disclosures.

An authorized member of Quest, Inc.'s workforce may use or disclose protected health information to organ procurement organizations or other entities engaged in the procurement, banking or transplantation of cadaveric organs, eyes or tissue for the purpose of facilitating organ, eye or tissue donation and transplantation.

10. Uses and Disclosures for Research Purposes.

a. Delivery to Privacy Office.

Any member of Quest, Inc.'s workforce who receives a request, or proposes, to use or disclose protected health information for research purposes must promptly deliver or otherwise communicate the request or proposal to the Privacy Office prior to the use or disclosure being made. The Privacy Office will then oversee the use or disclosure for compliance with these privacy policies. The use or disclosure may not occur until it has been approved by the Privacy Office.

b. Permitted Uses and Disclosures.

An authorized member of Quest, Inc.'s workforce may use or disclose protected health information for research, regardless of the source of funding for the research, provided that:

(1) Board Approval of a Waiver of Authorization. Quest, Inc. obtains documentation that an alteration to or waiver, in whole or in part, of the individual authorization required by these privacy policies for use and disclosure of protected health information has been approved by either:

(a) An Institutional Review Board (IRB) established in accordance with the federal regulations set forth in the HIPAA privacy rule; or,

(b) A privacy board that meets the requirements of the HIPAA privacy rule, *see*, 45 CFR §164.512(i)(1)(i)(B).

The documentation must include all of the information required by the HIPAA privacy rule, *see*, 45 CFR §164.512(i)(2).

(For verification of the board approval of a waiver see Section VI.K.3.b of these privacy policies.)

(2) Reviews Preparatory to Research. Quest, Inc. obtains from the researcher representations that:

(a) Use or disclosure is sought solely to review protected health information as necessary to prepare a research protocol or for similar purposes preparatory to research;

(b) No protected health information will be removed from Quest, Inc. by the researcher in the course of the review; and,

(c) The protected health information for which use or access is sought is necessary for the research purposes.

(3) Research on Decedent's Information. Quest, Inc. obtains from the researcher:

(a) Representation that the use or disclosure is sought is solely for research on the protected health information of decedents;

(b) Documentation, at the request of Quest, Inc., of the death of such individuals; and,

(c) Representation that the protected health information for which use or disclosure is sought is necessary for the research purposes.

11. Uses and Disclosures to Avert a Serious Threat to Health or Safety.

a. Delivery to Privacy Office.

Any member of Quest, Inc.'s workforce who receives a request, or proposes, to use or disclose protected health information to avert a serious threat to health or safety must promptly deliver or otherwise communicate the request or proposal to the Privacy Office prior to the use or disclosure being made. The Privacy Office will then oversee the use or disclosure for compliance with these privacy policies. The use or disclosure may not occur until it has been approved by the Privacy Office.

b. Permitted Uses and Disclosures.

An authorized member of Quest, Inc.'s workforce may, consistent with applicable law and standards of ethical conduct, use or disclose protected health information, if the member of Quest, Inc.'s workforce, in good faith, believes the use or disclosure:

(1) Serious and Imminent Threat.

(a) Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and,

(b) Is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat.

(2) Law Enforcement. Is necessary for law enforcement authorities to identify or apprehend an individual:

(a) Because of a statement by an individual admitting participation in a violent crime that Quest, Inc. reasonably believes may have caused serious physical harm to the victim; or,

(b) Where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody.

c. Uses and Disclosures Not Permitted.
A use or disclosure pursuant to Section VI.G.11.b.(2)(a), above, concerning a statement of an individual may not be made if the information described in that section is learned by Quest, Inc.:

(1) In the course of treatment to affect the propensity to commit the criminal conduct that is that basis for the disclosure under that section, or counseling or therapy; or,

(2) Through a request by the individual to initiate or to be referred for the treatment, counseling, or therapy described in Section VI.G.11.b.(2)(a), above.

A disclosure made pursuant to Section VI.G.11.b.(2)(a), above, shall contain only the statement described in that section and the protected health information described in Section VI.G.7.c.(1) "Limited Information for Identification and Location Purposes" of these privacy policies.

12. Uses and Disclosures for Specialized Government Functions.

a. Delivery to Privacy Office.
Any member of Quest, Inc.'s workforce who receives an a request, or proposes, to use or disclose protected health information for purposes of a specialized government function described in this Section VI.G.12 must promptly deliver or otherwise communicate the request or proposal to the Privacy Office prior to the use or disclosure being made. The Privacy Office will then oversee the use or disclosure for compliance with these privacy policies. The use or disclosure may not occur until it has been approved by the Privacy Office.

b. Military and Veterans Activities.

(1) Armed Forces Personnel. An authorized member of Quest, Inc.'s workforce may use and disclose the protected health information of individuals who are Armed Forces personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, if the appropriate military authority has published by notice in the *Federal Register* the following information:

(a) Appropriate military command authorities; and,

(b) The purposes for which the protected health information may be used or disclosed.

(2) Foreign Military Personnel. An authorized member of Quest, Inc.'s workforce may use and disclose the protected health information of individuals who are foreign military personnel to their appropriate foreign military authority for the same purposes for which uses and disclosures are permitted for Armed Forces personnel under the notice published in the *Federal Register*.

c. National Security and Intelligence Activities.
An authorized member of Quest, Inc.'s workforce may disclose protected health information to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act, 50 U.S.C. 401 *et seq* and implementing authority, *e.g.*, Executive Order 12333.

d. Protective Services for the President and Others.
An authorized member of Quest, Inc.'s workforce may disclose protected health information to authorized federal officials for the provision of protective services to the President of the United States or other persons authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or to for the conduct of investigations authorized by 18 U.S.C. 871 and 879.

e. Correctional Institutions and Other Law Enforcement Custodial Situations.

(1) Permitted Disclosures. An authorized member of Quest, Inc.'s workforce may disclose to a correctional institution or a law enforcement official having lawful custody of an inmate or other individual protected health information about such inmate or individual, if the correctional institution or such law enforcement official represents that such protected health information is necessary for:

(a) The provision of health care to such individuals;

(b) The health and safety of such individual or other inmates;

(c) The health and safety of the officers or employees of or others at the correctional institution;

(d) The health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another;

(e) Law enforcement on the premises of the correctional institution; and,

(f) The administration and maintenance of the safety, security, and good order of the correctional institution.

(2) No Application After Release. For purposes of this provision, an individual is no longer an inmate when released on parole, probation, supervised release, or otherwise is no longer in lawful custody.

13. Disclosures for Workers' Compensation.

a. Delivery to Privacy Office.
Unless the use or disclosure has previously been approved by the Privacy Office, a member of Quest, Inc.'s workforce who receives a request, or proposes, to disclose protected health information to comply with laws relating to workers compensation or other similar programs, must promptly deliver or otherwise communicate the request or proposal to the Privacy Office prior to the disclosure being made. The Privacy Office will then oversee the use or disclosure for compliance with these privacy policies. The use or disclosure should not occur until it has been approved by the Privacy Office.

b. Permitted Disclosures.
An authorized member of Quest, Inc.'s workforce may disclose protected health information as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illnesses without regard to fault.

14. Disclosure to the Secretary of Health and Human Services.

a. Delivery to Privacy Office.
Any member of Quest, Inc.'s workforce who receives a request, or proposes, to disclose protected health information to the Secretary of Health and Human Services must promptly deliver or otherwise communicate the request or proposal to the Privacy Office prior to the disclosure being made. The Privacy Office will then oversee the disclosure for compliance with these privacy policies. The use or

disclosure should not occur until it has been approved by the Privacy Office.

b. Permitted Disclosures.

Acting through its Privacy Office, Quest, Inc. will permit access by the Secretary of Health and Human Services during normal business hours to its facilities, books, records, accounts and other sources of information, including protected health information, that are pertinent to ascertaining compliance with the applicable requirements of the HIPAA privacy rule. If the Secretary of Health and Human Services determines that exigent circumstances exist, such as when documents may be hidden or destroyed, Quest, Inc. will permit access by the Secretary of Health and Human Services at any time and without notice.

If any information required of Quest, Inc. under this section is in the exclusive possession of any other agency, institution, or person and that other agency, institution or person fails or refuses to furnish the information, the Privacy Office will so certify and set forth what efforts Quest, Inc. has made to obtain the information.

15. Disclosures by Whistleblowers.

A member of Quest, Inc.'s workforce or a business associate may disclose protected heath information, provided that:

a. The workforce member or business associate believes in good faith that Quest, Inc. has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services or conditions provided by Quest, Inc. potentially endangers one or more persons served, workers, or the public; and,

b. The disclosure is to:

(1) A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of Quest, Inc. or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by Quest, Inc.; or,

(2) An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct described in Section a., above.

The disclosure does not need to be approved by the Privacy Office before it is made.

16. Disclosures by Workforce Members Who are Victims of a Crime.
A workforce member who is the victim of a criminal act may disclose protected health information to a law enforcement official, provided that:

a. The protected health information disclosed is about the suspected perpetrator of the criminal act; and,

b. The protected health information disclosed is limited to the following information:
   (1) Name and address;
   (2) Date and place of birth;
   (3) Social security number;
   (4) ABO blood type and Rh factor;
   (5) Type of injury;
   (6) Date and time of treatment;
   (7) Date and time of death, if applicable; and,
   (8) A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence of absence of facial hair (beard or moustache), scars, and tattoos.

The disclosure does not need to be approved by the Privacy Office before it is made.

17. Disclosures to Business Associates.

a. Delivery to Privacy Office.
Unless the use or disclosure has previously been approved by the Privacy Office, any member of Quest, Inc.'s workforce who receives an a request, or proposes, to disclose protected health information to a business associate of Quest, Inc. must promptly deliver or otherwise communicate the request or proposal to the Privacy Office prior to the disclosure being made. The Privacy Office will then oversee the use or disclosure for compliance with these privacy policies. The use or disclosure may not occur until it has been approved by the Privacy Office.

b. Permitted Disclosures.
Authorized members of Quest, Inc.'s workforce may disclose protected health information to a business associate and may allow a business associate to create or receive protected health information on Quest, Inc.'s behalf, if Quest, Inc. has a written contract with the business associate that meets the requirements of the HIPAA privacy rule.

H. Uses and Disclosures for Marketing.

1. General Rule.

Except as stated in section VI.H.2, below, a member of Quest, Inc.'s work-force may not use protected health information for marketing without an authorization that meets the applicable requirements of Section VI.E of these privacy policies, except as stated in this Section VI.H.

Any use of protected health information for marketing without an authorization must be approved in advance by the Privacy Office.

2. Exceptions.

An authorization does not need to be obtained if Quest, Inc. uses or discloses protected health information to make a marketing communication to an individual that is in the form of:

a. A face-to-face communication made by Quest, Inc. to an individual; or,

b. A promotional gift of nominal value provided by Quest, Inc..

If the marketing involves direct or indirect remuneration to Quest, Inc. from a third party, the authorization must state that such remuneration is involved.

3. "Marketing" Defined.

"Marketing" means:

a. To make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service, unless the communication is made:

(1) To describe a health-related product or service...that is provided by ...the covered entity making the communication....

(2) For treatment of the individual; or,

(3) 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.

b. An 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 service that encourages recipients of the communication to purchase that product or service."

I. Uses and Disclosures for Fundraising.

1. General Rule.

An authorized member of Quest, Inc.'s workforce may use, or disclose to a business associate or to an institutionally related foundation, the following protected health information for the purpose of raising funds for its own benefit, without an authorization meeting the requirements of Section VI.E "Uses and Disclosures for Which an Authorization is Required" of these privacy policies:

a. Demographic information relating to an individual; and,

b. Dates of health care provided to an individual.

Any use of protected health information for the purpose of raising funds for Quest, Inc.'s benefit without an authorization must be approved in advance by the Privacy Office.

2. Opting Out.

Any fundraising materials Quest, Inc. sends to an individual must include a description of how the individual may opt out of receiving any further fundraising communications.

Quest, Inc. must make reasonable efforts to ensure that individuals who decide to opt out of receiving future marketing communications are not sent future communications.

J. Limited Data Set.

1. General Rule.

Quest, Inc. may use or disclose a limited data set that meets of the requirements of Section VI.J.3 "Limited Data Set Defined" , below, if Quest, Inc. enters into a "data use agreement" with the limited data set recipient. Prior to Quest, Inc. using or disclosing any protected health information as part of a "limited data set", both the limited data set and the data use agreement must be approved by the Privacy Office as meeting the requirements of this Section VI.J.

2. Permitted Uses.

a. A limited data set may be used and disclosed only for the purposes of research, public health, or health care operations.

b. Quest, Inc. may use protected health information to create a limited data set or disclose protected health information to a business associate of Quest, Inc. for that purpose, whether or not the limited data set is to be used by Quest, Inc..

3. "Limited Data Set" Defined.

A "limited data set" is protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

(i) Names;
(ii) Postal address information, other than town or city, State, and zip code;
(iii) Telephone numbers;
(iv) Fax numbers;
(v) Electronic mail addresses;
(vi) Social security numbers;
(vii) Medical record numbers;
(viii) Health plan beneficiary numbers;
(ix) Account numbers;
(x) Certificate/license numbers;
(xi) Vehicle identifiers and serial numbers, including license plate numbers;
(xii) Device identifiers and serial numbers;
(xiii) Web Universal Resources Locators (URLs);
(xiv) Internet Protocol (IP) address numbers;
(xv) Biometric identifiers, including finger and voice prints; and
(xvi) Full face photographic images and any comparable images.

4. Data Use Agreement.

A date use agreement between Quest, Inc. and the limited data set recipient must:

a. Establish the permitted uses and disclosures of the limited data set by the limited data set recipient consistent with the permitted uses stated above. The data use agreement may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate the requirements of these policies or the HIPAA privacy rule if done by Quest, Inc.;

b. Establish who is permitted to use or receive the limited data set; and,

c. Provide that the limited data set recipient will:

(1) Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;

(2) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;

(3) Report to the covered entity any use or disclosure of the information not provided for by its data use agreement of which it becomes aware;

(4) Ensure that any agents, including a subcontractor, to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and,

(5) Not identify the information or contact the individuals.

K. Verification of Identity and Authority.

1. General Rule.

Prior to any disclosure of protected health information, the authorized member of Quest, Inc.'s workforce who is making the disclosure must:

a. Except with respect to disclosures under VI.F, "Uses and Disclosures Requiring an Opportunity for the Individual to Agree or to Object" of these privacy policies, verify the identity of a person requesting protected health information and the authority of that person to have access to protected health information under these privacy policies, if the identity of that person is not known to Quest, Inc.; and,

b. Obtain any documentation, statements, or representations, whether oral or written, from the person requesting the protected health information when such documentation, statement, or representation is a condition of the disclosure under these privacy policies.

2. Personal Representatives.

Unless the person and his or her authority is known to Quest, Inc., the authorized member of Quest, Inc.'s workforce who is making a disclosure to an individual's personal representative shall verify the person's identity by way of a government issued document with a picture (e.g., a driver's license, passport) and verify the person's authority (*e.g.*, requiring a copy of a power of attorney/guardianship, asking questions to establish relationship to a child.)

3. Conditions on Disclosures.

If a disclosure is conditioned by these privacy policies on particular documentation, statements, or representations form the person requesting the protected health information, the authorized member of Quest, Inc.'s work-force who is making the disclosure may rely, if such reliance is reasonable under the circumstances, on documentation, statements, or representations that, on their face, meet the applicable requirements.

In this regard:

a. The conditions in Section VI.G.7.b.(2)(c) under "Disclosures for

Law Enforcement Purposes" of these privacy policies may be satisfied by the administrative subpoena or similar process or by a separate written statement that, on its face, demonstrates that the applicable requirements have been met.

b. The documentation required by Section VI.G.10.b.(1), "Board Approval of a Waiver of Authorization" of these privacy regulations, may be satisfied by one or more written statements provided that each is appropriately dated and signed in accordance with the HIPAA privacy rule, 45 CFR §164.512(i)(2)(i)&(v).

4. Identity of Public Officials.

Quest, Inc. may rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity when the disclosure of protected health information is to a public official or a person acting on behalf of a public official:

a. If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;

b. If the request is made in writing, the request is on the appropriate government letterhead; or,

c. If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

5. Authority of Public Officials.

Quest, Inc. may rely, if such reliance is reasonable under the circumstances, on any of the following to verify authority when the disclosure of protected health information is to a public official or a person acting on behalf of a public official:

a. A written statement of the legal authority under which the information is requested, or , if a written statement would be impractical, on oral statement of such legal authority;

b. If a request is made pursuant to legal process, warrant, subpoena, order or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.

6. Exercise of Professional Judgment.
The verification requirements of this section are met if a member of Quest, Inc.'s workforce relies on the exercise of professional judgment in making a use or disclosure in accordance with Section VI.F, "Uses or Disclosures Requiring an Opportunity for the Individual to Agree or Object" of these privacy policies or acts on a good faith belief in making a disclosure in accordance with Section VI.G.11, "Uses or Disclosures to Avert a Serious Threat to Health or Safety" of these privacy policies.

L. Prior Authorizations.

1. General Rule.
Notwithstanding other sections of these privacy policies, Quest, Inc. may use or disclose protected health information, consistent with Section VI.L.2 and Section VI.L.3, below, pursuant to an authorization or other express legal permission obtained from an individual permitting the use or disclosure of protected health information, informed consent of the individual to participate in research, or a waiver of informed by an Institutional Review Board.

2. Effect of Prior Authorization for Purposes Other Than Research.
Notwithstanding any provisions of Section VI.E "Uses and Disclosures for Which an Authorization is Required" of these privacy policies (see Page 22), Quest, Inc. may use or disclose protected health information that it created or received prior to April 14, 2003, pursuant to an authorization or other express legal permission obtained from an individual prior to April 14, 2003, provided the authorization or other express legal permission specifically permits such use or disclosure and there is no agreed-to restriction in accordance with Section VII.A.1 "Right to Request Privacy Protection"of these privacy policies .

3. Effect of Prior Permission for Research. Notwithstanding any provisions in Section VI.E "Uses and Disclosures for Which an Authorization is Required" of these privacy policies and Section VI.G.10 "Uses and Disclosures for Research Purposes" of these privacy policies (see Page 47), Quest, Inc. may, to the extent allowed by one of the following permissions, use or disclose, for research, protected health information that it created or received either before or after April 14, 2003, provided there is no agreed-to restriction in accordance with Section VII.A.1 "Right to Request Privacy Protection" of these privacy policies, and Quest, Inc. has obtained prior to April 14, 2003, either:

a. An authorization or other express legal permission from an individual to use or disclose protected health information for the research;

b. The informed consent of the individual to participate in the research;

or,

c. A waiver, by an institutional Review Board, of informed consent for research in accordance with the requirements of the HIPAA Privacy Rule, *see*, 45 CFR §164.532(c)(3), provided that Quest, Inc. must obtain authorization as required by Section VI.E "Uses and Disclosures for Which an Authorization is Required" of these privacy policies, if, after April 14, 2003, informed consent is sought from an individual participating in the research.

VII. RIGHTS OF INDIVIDUALS

A. Right to Request Privacy Protection.

1. Restriction of Uses and Disclosures.

a. Generally.

Quest, Inc. will permit an individual to request that Quest, Inc. restrict:

(1) Uses and disclosures of protected health information about the individual to carry out treatment, payment or health care operations; and,

(2) Disclosures permitted under Section VI.F.3, "Persons Involved in the Individual's Care; Notification" of these privacy policies, for involvement in the individual's care and notification purposes.

Whether or not Quest, Inc. will agree to the restriction will be determined by the Director of Operations. If a restriction is agreed to, a written or electronic record of that restriction shall be retained by Quest, Inc. for six years from the date of its creation or the date when it was last in effect, whichever is later.

If Quest, Inc. agrees to a restriction, the protected health information shall not be used or disclosed in violation of such restriction, except that, if 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, the restricted protected health information may used by Quest, Inc., or may be disclosed by an authorized member of Quest, Inc.'s workforce to a health care provider, to provide such treatment to the individual. If the information is disclosed to a health care provider for emergency treatment, the member of Quest, Inc.'s workforce making the disclosure shall request that health care provider not further use or disclose the information.

A restriction agreed to by Quest, Inc. under this Section VII.A.1.a is not effective to prevent uses or disclosures:

(a) To the individual when requested by the individual pursuant to the individual's right of access to the information (see, Section VII.B, "Right of Access" of these privacy policies);

(b) For facility directories pursuant to Section VI.F.2, "Facility Directories" of these privacy policies; or,

(c) When the use or disclosure does not require an authorization or opportunity to agree or object is not required (see, Section VI.G, "Uses and Disclosures for which an Authorization or an Opportunity to Agree or Disagree is Not Required" of these privacy policies).

b. Termination of Restriction.

Quest, Inc. may terminate its agreement to a restriction under this Section VII.A.1, if:

(1) The individual agrees to or requests the termination in writing;

(2) The individual orally agrees to the termination and the oral agreement is documented; or,

(3) Quest, Inc. informs the individual that it is terminating its agreement to the restriction, except that such termination shall be effective only with respect to protected health information created or received after Quest, Inc. has so informed the individual.

2. Restriction on Means and Location of Communications.

a. Generally.

Quest, Inc. shall permit individuals to request and, subject to the conditions stated below, shall accommodate reasonable requests by individuals to receive communications of protected health information from Quest, Inc. by alternative means or at alternative locations. The request by the individual to receive communications by alternative means or at alternative locations must be in writing.

b. Conditions.

Quest, Inc.'s accommodation of such requests shall be conditioned on:

(a) When appropriate, information as to how payment, if any,

will be handled; and,

(b) Specification by the individual of an alternative address or other method of contact.

Quest, Inc. shall not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.

B. Right of Access.

1. Generally.

Except when access is denied under Section VII.B.5 , "Denial of Access" of these privacy policies, an individual shall have a right of access to inspect and obtain a copy of protected health information about the individual for as long as the protected health information is maintained in that record set except for:

a. Psychotherapy notes;

b. Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and

2. Request for Access.

The individual's request for access must be submitted in writing to Director of Operations.

3. Action on Request for Access.

a. Time Limits for Action.

The Director of Operations shall act on a request for access no later than thirty (30) calendar days after Quest, Inc.'s receipt of the request. However, if the request for access is for protected health information that is not maintained or accessible to Quest, Inc. on-site, the Director of Operations shall act on the request for access no later than sixty (60) calendar days after Quest, Inc.'s receipt of the request.

If the Director of Operations is unable to take an action on the request within the applicable time required by the preceding paragraph, Director of Operations may extend the time for the action by no more than thirty (30) calendar days, provided:

(1) Within the applicable time required by the preceding paragraph, the Director of Operations shall provide the individual with a written statement of the reason(s) for the

delay and the date by which Quest, Inc. will complete its action on the request; and,

(2) Only one such extension shall be permitted on a request for access.

b. Inform Individual of Action on Request.

If the request is granted, in whole or in part, the Privacy Office shall inform the individual of the acceptance of the request and provide the access requested in accordance with Section VII.B.4, below.

If the request is denied, in whole or in part, the Privacy Office shall provide the individual with a written denial, in accordance with Section VII.B.6.b, "Actions if Access is Denied", of these privacy policies.

4. Providing Access.

a. Access.

If the individual is granted access, in whole or in part, to protected health information, Quest, Inc. shall provide the access requested by the individual, including inspection and obtaining a copy, or both, of the protected health information about the individual in designated record sets. If the same protected health information that is the subject of a request for access is maintained in more than one designated record set or at more than on location, the protected health information will only be produced once in response to a request for access.

b. Form and Format.

The protected health information will be provided to the individual in the form or format requested by the individual, if it is readily producible in that form or format. If it is not readily producible in that form or format, it shall be provided in a readable hard copy form or such other form or format as agreed to by the Director of Operations and the individual.

c. Summary In Lieu of Access.

The individual may be provided a summary of the protected health information requested, in lieu of providing access to the protected health information, or may be provided an explanation of the protected health information to which access has been provided, if:

(1) The individual agrees in advance to such a summary or explanation; and,

(2) The individual agrees in advance to the fees imposed, if any, by Quest, Inc. for such summary or explanation.

d. Time and Manner of Access.

Access shall be provided in a timely manner as stated in Section VII.B.3.a, "Action on Request for Access" of these privacy policies, including arranging with the individual for a convenient time and place to inspect or obtain a copy of the protected health information, or mailing the copy to the individual at the individual's request. The Director of Operations may discuss the scope, format and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access.

e. Fees.

If the individual requests a copy of the protected health information, or agrees to a summary or explanation of such information, Quest, Inc. shall impose charges as set forth in Appendix E to these privacy policies.

5. Denial of Access.

a. Unreviewable Grounds for Denial.

Quest, Inc. may deny an individual access without providing the individual an opportunity for review, in any the following circumstances:

(1) Information Is Exempted. The protected health information is exempted from the right of access as stated in Section VII.B.1, "Generally", of these privacy policies.

(2) Inmates. When Quest, Inc. is acting under the direction of a correctional institution, Quest, Inc. may deny, in whole or in part, an inmate's request to obtain a copy of protected health information, if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or reasonable for the transporting of the inmate.

(3) Research. An individual's access to protected health information created or obtained by Quest, Inc. in the course of research that included treatment may be temporarily suspended for so long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and Quest, Inc. has informed the individual that

the right of access will be reinstated upon completion of the research.

(4) Information Obtained From Others. An 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.

b. Reviewable Grounds for Denial.
Quest, Inc. may deny an individual access, provided that the individual is given a right to have the denial reviewed as stated in Section VII.B.6.c, "Review of Denial", of these privacy policies, in any the following circumstances:

(1) Endangerment. A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;

(2) Reference to Another Person. 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; or

(3) Personal Representative. 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.

6. Actions if Access is Denied.

If an individual's access to protected health information is denied, in whole or in part, Quest, Inc. shall comply with the following:

a. Making Other Information Accessible.
Quest, Inc. shall, to the extent possible, give the individual access to any other protected health information requested, after excluding the protected health information as which Quest, Inc. had the ground to deny access.

b. Written Denial.

The Director of Operations shall provide a written denial to the individual within the applicable time period stated in Section VII.B.6.c, "Review of Denial", of these privacy policies. The denial shall contain:

(1) The basis for the denial;

(2) If applicable, a statement of the individual's review rights, including a description of how the individual may exercise such review rights;

(3) A description of how the individual may complain pursuant to Quest, Inc.'s complaint procedures or to the Secretary of Health and Human Resources, including the name or title, and the telephone number of the Quest, Inc. contact person or office designated to receive complaints.

(4) If Quest, Inc. does not maintain the protected health information that is the subject of the individual's request for access, and Quest, Inc. knows where the requested information is maintained, a statement informing the individual where to direct the request for access.

c. Review of Denial.

If access is denied on a ground permitted under Section VII.B.5.b, "Reviewable Grounds for Denial" of these privacy policies, above, the individual shall have the right to have the denial reviewed by a licensed health care professional who is designated by the Privacy Office to act as a reviewing official and who did not participate in the original decision to deny.

The individual's request for review shall be promptly referred to that designated reviewing official. The designated reviewing official shall then determine, within a reasonable period of time, whether or not to deny the access requested based on the standards stated in Section VII.B.5.b, "Reviewable Grounds for Denial"of these privacy policies.

The Privacy Office shall then promptly provide written notice to the individual of the determination of the designated reviewing official and implement the designated reviewing official's determination.

7. Documentation.

The Privacy Office shall maintain, or cause to be maintained, documentation of:

a. The designated record sets that are subject to access by individuals;

and,

b. The titles of the persons or offices responsible for receiving and processing request for access by individuals.

The documentation shall be maintained by Quest, Inc. in written or electronic form for six years after the date of its creation or the date when it was last in effect, whichever is later.

C. Right to Request Amendment.

1. Generally.

Except when access is denied under Section VII.C.5, "Grounds for Denying the Amendment" of these privacy policies, an individual shall have a right to have Quest, Inc. amend protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in the designated record set.

2. Request for Amendment.

The individual's request for amendment must be submitted in writing to the Director of Operations and must state in the written request a reason to support the requested amendment. Individuals shall be informed in advance of these requirements in Quest, Inc.'s Notice of Privacy Practices.

3. Action on Request for Amendment.

a. Time Limits for Action.

The Director of Operations shall act on a request for access no later than sixty (60) calendar days after Quest, Inc.'s receipt of the request.

If the Director of Operations is unable to take an action on the request within that sixty (60) day period, the Director of Operations may extend the time for the action by no more than thirty (30) calendar days, provided:

(1) Within that sixty (60) day period, the Director of Operations shall provide the individual with a written statement of the reason(s) for the delay and the date by which Quest, Inc. will complete its action on the request; and,

(2) Only one such extension shall be permitted on a request for amendment.

b. Inform Individual of Action on Request.

If the request for amendment is accepted, in whole or in part, the

Privacy Office shall inform the individual of the acceptance of the request and make the amendment requested in accordance with Section VII.C.4.a, above, of these privacy policies.

If the request for amendment is denied, in whole or in part, the Privacy Office shall provide the individual with a written denial, in accordance with Section VII.C.6, "Actions if Amendment is Denied" of these privacy policies, and shall take the other actions required by that Section VII.C.6.

4. Accepting the Amendment.

If the individual's request for amendment is accepted, in whole or in part, the Privacy Office shall:

a. Making the Amendment.

The Privacy Office shall make the appropriate amendment to the protected health information or record that is the subject of the request for amendment by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment.

b. **Informing the Individual.**

The Privacy Office shall inform the individual as stated in Section VII.C.3.b, "Inform Individual of Action on Request" of these privacy policies, that the amendment as been accepted and obtain the individual's identification of and agreement to have Quest, Inc. notify the relevant persons with the amendment needs to be shared in accordance with Section VII.C.4.c, below.

c. Informing Others.

The Privacy Office shall make an reasonable effort to inform and provide the amendment within a reasonable time to:

(1) Persons identified by the individual as having received protected health information about the individual and needing amendment;

(2) Persons, including Quest, Inc. business associates, that Quest, Inc. knows have the protected health information that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.

5. Grounds for Denying the Amendment.

An individual's request to amend protected health information may be denied if the Director of Operations determines that the protected health information or record that is the subject of the request:

a. Was not created by Quest, Inc., unless the individual provides a reasonable basis to believe that the originator of the protected health information is no longer available to act on the requested amendment;

b. Is not part of the designated record set;

c. Would not be available for inspection (see, Section VII.B.1, "Generally" of these privacy policies); or,

d. Is accurate and complete.

6. Actions if Amendment is Denied.

If an individual's requested amendment is denied, in whole or in part, Quest, Inc. shall comply with the following:

a. Written Denial.

The Privacy Office shall provide a written denial to the individual within the applicable time period stated in Section VII.C.3.a, "Time Limits for Action" of these privacy policies. The denial shall contain:

(1) The basis for the denial;

(2) The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;

(3) At statement that, if the individual does not submit a statement of disagreement, the individual may request that Quest, Inc. provide the individual's request for amendment and the denial with any future disclosures of the protected health information that is the subject of the requested amendment; and,

(4) A description of how the individual may complain to Quest, Inc. pursuant to Quest, Inc.'s complaint procedure or to the Secretary of the United States Department of Health and Human Services. The description shall include the name or title and telephone number of the contact person or office designed by Quest, Inc. to receive complaints.

b. Statement of Disagreement.

The individual may submit a written statement disagreeing with the denial of all or part of a requested amendment and the basis for such disagreement. The written statement must be not more than one (1) page.

c. Rebuttal Statement.

The Privacy Office may prepare, or cause to be prepared, a written rebuttal of Quest, Inc. to the individual's statement of disagreement. If a rebuttal statement is prepared, a copy of it shall be provided to the individual who submitted the statement of disagreement.

d. Recordkeeping.

As appropriate, the Privacy Office shall identify the record or protected health information in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for amendment, Quest, Inc.'s denial of the request, the individual's statement of disagreement, if any, and Quest, Inc.'s rebuttal, if any, to the designated record set.

e. Future Disclosures.

(1) If a statement of disagreement has been submitted by the individual, Quest, Inc. will include the material appended in accordance with section VII.C.6.d, above, or, at the election of the Privacy Office, an accurate summary of any such information, with any subsequent disclosure of the protected health information to which the disagreement relates.

(2) If the individual has not submitted a written statement of disagreement, Quest, Inc. will include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the protected health information only if the individual has requested such action in accordance with Section VII.C.6.a.(3), "Actions if Amendment is Denied" of these privacy policies.

(3) When a subsequent disclosure described in (1) or (2), above, is made using a transaction that does not permit the additional material to be included with the disclosure, Quest, Inc. shall separately transmit the material to the recipient of the transaction.

7. Documentation.

The Privacy Office shall maintain documentation of the titles of the persons or offices responsible for receiving and processing requests for amendment. The documentation shall be maintained by Quest, Inc. in written or electronic form for six (6) years after the date the notice was last in effect.

D. Right to an Accounting of Disclosures.

1. Right to Accounting.

a. General Rule.

Except as stated in VII.D.1.b, "Exceptions" or VII.D.1.c "Suspension of Right for Certain Disclosures", below, an individual shall have a right to receive an accounting of disclosures of protected health information made by Quest, Inc. in the six (6) years prior to the date on which the accounting is requested or for such shorter period as the individual may request.

b. Exceptions.

The right to an accounting of disclosures does not apply to the following types of disclosures:

(1) To carry out treatment, payment and health care operations as provided in Section VI.D, "Uses and Disclosures to Carry Out Treatment, Payment and Health Care Operations" of these privacy policies;

(2) To individuals of protected health information about them;

(3) Incident to a use or disclosure otherwise permitted or required by these privacy policies as provided in Section VI.B "Incidental Uses and Disclosures";

(4) Pursuant to an authorization as provided in Section VI.E "Uses and Disclosures for Which an Authorization is Required" of these privacy policies;

(5) For the facility's directory or to persons involved in the individual's care or other notification purposes as provided in Section VI.F, "Uses and Disclosures Requiring an Opportunity for the Individual to Agree or Object" of these privacy policies;

(6) For national security or intelligence purposes as provided in Section VI.G.12.c, "National Security and Intelligence Activities" of these privacy policies;

(7) To correctional institutions or law enforcement officials as provided in Section VI.G.12.e, "Correctional Institutions and Other Law Enforcement Custodial Situations"of these privacy policies;

(8) As part of a limited data set in accordance with Section VI.J "Limited Data Set" of these privacy regulations; or,

(9) That occurred prior to April 14, 2003.

c. Suspension of Right for Certain Disclosures.
An individual's right to receive an accounting of disclosures to a health oversight agency (see, Section VI.G.5, "Uses and Disclosures for Health Oversight Activities" on Page 37 of these privacy policies) or to a law enforcement official (see, Section VI.G.7, "Disclosures for Law Enforcement Purposes" of these privacy policies) shall be temporarily suspended for the time specified by the agency or official, if the agency or official provides Quest, Inc. with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required.

If the agency or official statement is made orally, the Privacy Office shall:

(1) Document the statement, including the identity of the agency or official making the statement;

(2) Temporarily suspend the individual's right to an accounting of disclosures subject to the statement; and,

(3) Limit the temporary suspension to no longer than thirty (30) calendar days from the date of the oral statement, unless a written statement as described above is submitted during that time.

2. Content of the Accounting.
The written accounting provided to the individual shall meet the following requirements:

a. Content. Except as otherwise stated in Section VII.D.1.b, "Exceptions" of these privacy policies, the accounting must include the disclosures of protected health information that occurred during the period the individual requests up to a maximum of six (6) years prior to the date of the reQuest, Including disclosures to or by business associates of Quest, Inc..

b. Information. Except as stated in Section VII.D.2.c, "Multiple Disclosures for a Single Purpose" or Section VII.D.2.d "Disclosures

for Particular Research" of these privacy policies, the accounting must include for each disclosure:

(1) The date of the disclosure;

(2) The name of the entity or person who received the protected health information and, if known, the address of such entity or person;

(3) A brief description of the protected health information disclosed; and,

(4) A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure; or, in lieu of such statement:

(a) A copy of a written request for disclosure by the Secretary of Health and Human Services under Section VI.G.14, "Disclosure to the Secretary of Health and Human Services" of these privacy policies, if any; or,

(b) A copy of a written request for disclosure under Section VI.G, "Uses and Disclosures for which an Authorization or an Opportunity to Agree or Object is Not Required" of these privacy policies, if any.

c. Multiple Disclosures for a Single Purpose.

If, during the period covered by the accounting, Quest, Inc. has made multiple disclosures of protected health information to the same person or entity for a single purpose under Section VI.G.14, "Disclosure to the Secretary of Health and Human Services" or Section VI.G, "Uses and Disclosures for which an Authorization or an Opportunity to Agree or Object is Not Required" of these privacy policies, the accounting may with respect to such multiple disclosures, provide:

(1) The information required by Section VII.D.2.b of these privacy policies, for the first disclosure during the accounting period;

(2) The frequency, periodicity, or number of the disclosures made during the accounting period; and,

(3) The date of the last such disclosure during the accounting period.

d. Disclosures for Particular Research.

If during the period covered by the accounting, Quest, Inc. has made disclosures of protected information for a particular research purpose in accordance with Section VI.G.10 "Uses and Disclosures for Research Purposes" of these privacy policies for 50 or more individuals, the accounting may, with respect to the disclosures for which the protected health information about the individual may have been included, provide:

(1) The name of the protocol or other research activity;

(2) A description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records;

(3) A brief description of the type of protected health information that was disclosed;

(4) The date or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period;

(5) The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and,

(6) A statement that the protected health information of the individual may or may not have been disclosed for a particular protocol or other research activity.

If Quest, Inc. provides an accounting for research disclosures in accordance with this Section VII.D.2.d, "Disclosures for Particular Research", and if it is reasonably likely that the protected health information of the individual was disclosed for that research protocol or activity, Quest, Inc. shall, at the request of the individual, assist in contacting the entity that sponsored the research and the researcher.

3. Provision of the Accounting.

a. Time Limit to Provide the Accounting.

The Director of Operations shall act on a request for an accounting no later than sixty (60) calendar days after Quest, Inc.'s receipt of the request. Within that sixty (60) day period, the Director of Operations shall:

(1) Provide the individual with the accounting requested; or,

(2) If the Director of Operations is unable to take an action on the request within that sixty (60) day period, the Director of Operations may extend the time for the action by no more than thirty (30) calendar days, provided:

(a) Within that sixty (60) day period, the Privacy Office shall provide the individual with a written statement of the reason(s) for the delay and the date by which Quest, Inc. will provide the accounting; and,

(b) Only one such extension shall be permitted on a request for amendment.

b. Fee for Accounting.

The first accounting to an individual in any twelve (12) month period will be provided to the individual without charge. For each subsequent request for an accounting by the same individual with the twelve (12) month period shall be as stated in Appendix F to these privacy policies; before charging the fee, however, the Privacy Office shall notify the individual in advance of the fee and provide the individual an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

c. Documentation.

The Privacy Office shall document and retain the following:

(1) The information required to be included in an accounting under Section VII.D.2, "Content of Accounting" (see, Page 78) of these privacy policies, for disclosures of protected health information that are subject to an accounting;

(2) The written accounting that is provided to the individual under this section; and,

(3) The titles of the persons of offices responsible for receiving and processing requests for an accounting by individuals.

The documentation shall be maintained by Quest, Inc. in written or electronic form for six years after the date of its creation or the date when it was last in effect, whichever is later.

VIII. PERSONAL REPRESENTATIVES

A. General Rule.

Except as otherwise stated or permitted in these privacy policies, Quest, Inc. will treat a personal representative as the individual for purposes of these privacy policies.

B. Adults and Emancipated Minors.

If, under state law, a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, Quest, Inc. will treat such person as a personal representative with respect to protected health information relevant to such personal representative.

C. Unemancipated Minors.

1. General Rule.

If, under state law, a parent, guardian, or other person acting in loco parentis has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, Quest, Inc. will treat such person as a personal representative with respect to protected health information relevant to such personal representative.

Notwithstanding the general rule stated, above, a person will not be treated as a personal representative of an unemancipated minor, and the minor has the authority to act as an individual, with respect to protected health information pertaining to health care services, if:

a. The minor consents to such health care service; no other consent to such health care services is required by state law, regardless of whether the consent of another persona has also been obtained; and, the minor has not requested that such person be treated as the personal representative.

b. The minor may lawfully obtain such health care service without the 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 such health care service; or,

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

2. Exception.

Notwithstanding the preceding subparagraph 1:

a. If, and to the extent, permitted or required by an applicable provision of state or other law, including applicable case law, a covered entity may disclose, or provide access in accordance with Section VII.B "Right of Access" of these privacy policies to protected health information about an unemancipated minor to a parent, guardian, or other person acting *in loco parentis*;

b. If, and to the extent, prohibited by an applicable provision of state or other law, including applicable case law, Quest, Inc. may not disclose, or provide access in accordance with Section VII.B "Right of Access" of these privacy policies to, protected health information about an unemancipated minor to a parent, guardian, or other person acting *in loco parentis*; and,

c. Where the parent, guardian, or other person acting *in loco parentis*, is not the personal representative under subparagraphs VIII.C.1.a, VIII.C.1.b and VIII.C.1.c of this Section VIII.C "Unemancipated Minors" of these privacy policies and where there is no applicable access provision under state or other law, including case law, Quest, Inc. may provide or deny access under Section VII.B "Right of Access" of these privacy policies to a parent, guardian, or other person acting *in loco parentis*, if such action is consistent with state or other applicable law, provided that such decision must be made by a licensed health care professional, in the exercise of professional judgment.

D. Deceased Individuals.

If under state law an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, Quest, Inc. will treat that person as a personal representative under these privacy policies with respect to protected health information relevant to such person representation.

E. Abuse, Neglect, Endangerment Situations.

Notwithstanding anything in state law or these privacy policies to the contrary, Quest, Inc. may elect not to treat a person as the personal representative of an individual if:

1. Quest, Inc. has a reasonable belief that:

   a. The individual has been or may be subjected to domestic violence, abuse, or neglect by such person; or,

   b. Treating that person as the personal representative could endanger the individual; and

2. Quest, Inc., in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as the individual's personal representative.

IX. DEFINITIONS

A. Authorized Member of Quest, Inc.'s Workforce.

"Authorized member of Quest, Inc.'s workforce" means a member of Quest, Inc.'s workforce who has been authorized to take the action involved by: (a) his or her job description; (b) a protocol established by the Privacy Office; or, (c) by the Privacy Office.

B. Business Associate.

Option 1: "Business associate" means, with respect to Quest, Inc., a person or other legal entity that:

1. On behalf of Quest, Inc., but other than as a member of Quest, Inc.'s workforce, performs, or assists in the performance of:

    a. A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or,

    b. Any other function or activity regulated by the HIPAA privacy rule; or

2. Provides, other than as a member of Quest, Inc.'s workforce, legal, actuarial, accounting consulting, data aggregation, management, administrative, accreditation, or financial services to or for Quest, Inc., where the provision of such service involves the disclosure of individually identifiable health information from Quest, Inc., or from another business associate of Quest, Inc., to the person or legal entity.

Option 2: "Business associate" means, with respect to Quest, Inc., a person or other legal entity that:

1. On behalf of Quest, Inc. or an organized health care arrangement in which Quest, Inc. participates, but other than as a member of Quest, Inc.'s workforce, performs, or assists in the performance of:

    c. A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or,

    d. Any other function or activity regulated by the HIPAA privacy rule; or

2. Provides, other than as a member of Quest, Inc.'s workforce, legal, actuarial, accounting consulting, data aggregation, management, administrative, accreditation, or financial services to or for Quest, Inc., or for an organized health care arrangement in which Quest, Inc. participates, where the provision of such service involves the disclosure of individually identifiable health information from Quest, Inc., or from another business associate of Quest, Inc., to the person or legal entity.

However, in any of those situations, if a covered entity participating in a organized health care arrangement performs the function, activity or service for, on behalf of, or to the organized health care arrangement, that by itself does not make that

covered entity a business associate of Quest, Inc. or any other covered entity participating in the organized health care arrangement.

C. Covered Entity.

"Covered entity" means a health plan, a health care clearinghouse, or a health care provider that is covered by the HIPAA privacy rule.

D. Designated Record Set.

"Designated record set" means a group of records maintained by or for Quest, Inc. that is:

1. The medical records and billing records about individuals maintained by or for Quest, Inc.; or,

2. Used, in whole or in part, by or for Quest, Inc. to make decisions about individuals.

For purposes of this definition, the term "record" means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for Quest, Inc..

E. Disclosure.

"Disclosure" means the release, transfer, provision of access to, or divulging in any other manner of information outside Quest, Inc..

F. Health Care Operations.

"Health care operations" means any of the following activities of Quest, Inc. to the extent that the activities are related to covered functions:

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; 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 persons served with information about treatment alternatives; and related functions that do not include treatment;

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;

3. Conducting or arranging for medical review, legal services, and auditing

functions, including fraud and abuse detection and compliance programs;

4. 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,

5. Business management and general administrative activities of Quest, Inc., including, but not limited to:

   a. Management activities relating to implementation of and compliance with the requirements of these privacy policies and the HIPAA privacy rule;

   b. Customer service;

   c. Resolution of internal grievances;

   d. The sale, transfer, merger, or consolidation of all or part of Quest, Inc. 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. Consistent with the applicable requirements of Section II.B, "De-Identification of Health Information, creating de-identified health information or a limited data set, and fundraising for the benefit of Quest, Inc., and marketing for which an individual authorization is not required.

G. Health Care.

"Health care" means care, services, or supplies related to the health of an individual.

"Health care" includes, but is not limited to, the following:

1. Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and,

2. Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

H. Health Oversight Agency.

"Health oversight agency" means an agency or authority of the United States, a state, a territory, a political subdivision of a state or territory, or an Indian tribe that is authorized by law to oversee the health care system (whether public or private) 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.

"Health oversight agency" includes the employees or agents of such a public agency or its contractors or persons or entities to whom it has granted authority.

I. HIPAA Privacy Rule.

"HIPAA privacy rule" means 45 CFR Part 160 and 45 CFR Part 164 as amended from time to time.

J. Inmate.

"Inmate" means a person incarcerated in or otherwise confined to a correctional institution.

K. Law Enforcement Official.

"Law enforcement official" means an officer or employee of any agency or authority of the United States, a state, a territory, or an Indian tribe, who is empowered by law to:

1. Investigate or conduct an official inquiry into a potential violation of law; or,

2. Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

L. Payment.

"Payment" means the activities undertaken by Quest, Inc. to obtain reimbursement for the provision of health care that relate to the individual for whom health care is provided.

"Payment" includes but is not limited to:

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

2. 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;

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

4. Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and,

5. Disclosure to person served reporting agencies of any of the following protected health information relating to collection of premiums or

reimbursement:

a. Name and address;
b. Date of birth;
c. Social security number;
d. Payment history;
e. Account number;
f. Name and address of Quest, Inc..

M. Psychotherapy Notes.

"Psychotherapy notes" means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of a 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.

N. Secretary of Health and Human Services.

"Secretary of Health and Human Services" means the Secretary of the United States Department of Health and Human Services or any other officer or employee of that Department to whom the authority involved has been delegated.

O. These Privacy Policies.

"These privacy policies" means these privacy policies adopted by Quest, Inc. concerning the protection of the privacy of protected health information.

P. Treatment.

"Treatment" means 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 a patient; or the referral of a patient for health care from one health care provider to another.

Q. Use.

"Use" means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of that information within Quest, Inc..

R. Workforce.

"Workforce" means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for Quest, Inc., is under the direct control of

Quest, Inc., whether or not they are paid by Quest, Inc..

APPENDIX A

Identification of Workforce Members' Access To Protected Health Information.

(1)	Physician:	A physician must have access to all protected health information of persons served of Quest, Inc. to whom she is providing services.. There are no conditions applicable to that access.
(2)	Chief Financial Officer:	The Chief Financial Officer must have access to any and all financial information concerning persons served of Quest, Inc.. There are no conditions applicable to that access.
(3)	Registered Nurse (Field Staff):	A Registered Nurse (Field Staff) must have access to all clinical information of persons served to whom she/he is providing services. There are no conditions applicable to that access. She/he must have access to billing information concerning a patient if the Billing Clerk must discuss billing matters concerning that patient with the Registered Nurse (Field Staff).
(4)	Finance Staff:	The Finance Staff must have access to all billing and payment information concerning the person served. There are no conditions applicable to that access. She/he must have access to clinical information concerning the patient to the extent necessary to bill for services, obtain entitlements on their behalf, manage all person served accounts and their funds, complete census forms, manage all accounts payable and accounts receivable functions.
(5)	Receptionist:	The Receptionist must have access to the names of all persons served and of their personal representatives. There are no conditions applicable to that access.
(6)	Cleaning Staff:	The Cleaning Staff does not need assess to any protected health information concerning any patient of Quest, Inc..
(7)	President	The President must have access to all protected health and financial information of the employees and person serveds of Quest, Inc. There are no conditions applicable to that access.
(8)	Director of Operations	The Director of Operations must have access to all protected health and financial information of person serveds of Quest, Inc. There are no conditions

		applicable to that access.
(9)	Benefits Manager	The Benefits manager must have access to all billing information concerning the employees. There are no conditions applicable to that access. She must have access to clinical information concerning the employees to the extent necessary to reply to Workers Compensation and FMLA paperwork.
(10)	Quality Assurance Specialist	The Quality Assurance Specialist must have access to all protected health information of person serveds of Quest, Inc. to whom they are providing services.. There are no conditions applicable to that access.
(11)	Area Supervisors	The Area Supervisor must have access to all protected health information of person serveds of Quest, Inc. to whom they are providing services.. There are no conditions applicable to that access.
(12)	Director of Vocational Programs	The Director must have access to all protected health information of person serveds of Quest, Inc. to whom they are providing services.. There are no conditions applicable to that access.
(13)	Program Director / Manager	Program Director / Manager must have access to all protected health information of person serveds of Quest, Inc. to whom they are providing services.. There are no conditions applicable to that access.
(14)	Vocational Supervisors	The Supervisors must have access to all protected health information of person serveds of Quest, Inc. to whom they are providing services.. There are no conditions applicable to that access.
(15)	Occupational Therapists	The Supervisors must have access to all protected health information of person serveds of Quest, Inc. to whom they are providing services.. There are no conditions applicable to that access.
(16)	Occupational Therapists Aides	The Supervisors must have access to all protected health information of person serveds of Quest, Inc. to whom they are providing services.. There are no conditions applicable to that access.
(17)	Vocational Instructors	A Vocational Instructor must have access to all clinical information of persons served to whom she/he is providing services. There are no conditions applicable to that access.

(18)	Personal Assistants	A Personal Assistant must have access to all clinical information of persons served to whom she/he is providing services. There are no conditions applicable to that access.
(19)	Human Resource Staff	The human resource staff must have access to all information concerning the employees. There are no conditions applicable to that access. Must have access to clinical information concerning the employees to the extent necessary to hire, fire, complete payroll, reply to Workers Compensation and FMLA paperwork. Must have access to persons served clinical information to the extent to complete any related payroll and or payroll billing actions.

APPENDIX B
Safeguards to Protect the Privacy of Protected Health Information

I. Computers.

A. Passwords

Passwords are to be changed every sixty days, be at least eight (8) characters long, and be complex in nature. Passwords must be re-entered each time you come back to your work station, Passwords are not to be disclosed to anyone outside of the Employer, and only on a need to know basis within the Employer.

B. Security / Locking Computer

When you leave your workstation you need to lock your computer. Includes anytime you leave your computer on and move away from your work area, bathroom break, make copies etc.

C. Email Usage

Persons are never to use any identifying information by which a third party might be able to deduce the identity of the person served or employee Protected Health Information is utilized

D. Physical Transfer of Health Protected Information

No protected health information may be removed from the office on computer disk without the prior approval of the Privacy Office. When removal is permitted by the Privacy Office, the disk shall be encrypted and password protected.

II. Confidentiality

Employees have access to a wide range of confidential information. "Confidential information" is information which is not generally known and which the Employee obtained solely as a result of his or her employment at the Employer. It includes, but is not limited to, written records and lists as well as knowledge of Persons Served, the Employer's suppliers, methods of operation, contracts, policies, trade secrets, pricing, financial conditions, including information related to profits, net income, and debt.

Each Person Served and Employee has a right to confidentiality. In accepting employment with the Employer. an Employee is in a position of trust in regard to information concerning the Persons Served and other Employees of this Employer.

Information concerning the Persons Served or Employees is not to be discussed outside the home or work site. Information must not be released, whether written, oral, or over the phone to any individual or agency without the expressed approval of the Employer. No records, data about the Persons Served, Employee, or site operations of the Employer are to leave the home or work site or administrative office.

All reports, records, statements, and data are confidential which pertain to the testing, care, treatment, reporting, and research associated with any serious communicable diseases such as HIV infection or Acquired Immunodeficiency Syndrome. Any Employee who releases information in any form about a person pertaining to HIV status or other named serious communicable diseases may be charged with a misdemeanor, punishable by imprisonment

for not more than one year or a fine of no more than $5,000, or both, and is liable in a civil action for actual damages or $1,000, whichever is greater, and costs and reasonable attorney fees. If an Employee is aware of such an applicable situation they should contact a Supervisor or an Administrative officer

III. Electronic Communication Systems Policy

The Employer at its own expense, provides selected Employees, ("Users") the ability to use and access the Internet, the Employer's Intranet, electronic mail ("E-mail"), voice mail, telephones, facsimile machines, smart phones, PDA, computers, and other electronic communication systems (the "Systems"). The Employer owns the right to use the Systems. Users are to use the Systems only for the Employer's business purposes. The systems, equipment, and data stored on these systems are company property and remain so at all times. All messages sent, received, or stored on the system remain exclusive the property of the Employer and are not considered the private property of any Employee. Select Employees have privileges to utilize email and the Internet. This privilege may be changed/revoked at any time at the sole discretion of the Employer.

IV. Email Usage

All employees must use extreme caution when using email. No general email is secure and employees must utilize email with the expectation that it is a public forum and that any one might read it.

Persons are never to use any identifying information by which a third party might be able to deduce the identity of any person served in general email. Encrypted email or email while signed into a secure system allows for the usage of identifying information in email messages. Prior approval from the President is required before using any identifying information in email.

Identifying information may include but is not limited to names, initials, case numbers, social security numbers, home or site names with a general description of the person served, and any other identifying characteristics.

Written communication with identifying information about persons served must be mailed or faxed. If the information is faxed then the Fax Security Policy must be followed. Received and sent normal email is to be kept no longer than six months. After six months days the user is to delete all email sent and received email message. Archival email may be kept longer if it pertains to contracts, notices, and agreements with vendors, and accounts.

Never read / open any unsolicited email. If you are not expecting email from some one, call the sender before reading and or opening. Never open any attachments received through email, unless you know the sender and are expecting them. If you are not sure then call the sender before opening.

Utilize the following disclaimer in all outgoing email messages: This message is intended for use solely by the individual or organization to which it is addressed. This message may contain confidential information. If you are not the intended recipient, please do not copy, distribute or pass this message along to anyone. Please notify the sender if you have received this message in error and delete it. Thank you.

V. Records & Files

Any records being transported in a motor vehicle outside of the office, shall be transported in the trunk of the vehicle. If the vehicle does not have a trunk, records shall be transported in a container which does not identify the contents as protected health information.

A. During the Workday

During the workday files containing protected health information shall remain in the appropriate file drawers except when being used. When being used, the person who removes the file shall place a red file divider at the location of the file in the file drawers indicating that the file is with that person. At the end of the work day, all files containing protected health information shall be returned to the appropriate file drawers.

B. Office Closed

When the office is closed, all file drawers containing protected health information shall be closed and the office locked.

C. Records

Any records being transported in a motor vehicle outside of the office, shall be transported in the trunk of the vehicle. If the vehicle does not have a trunk, charts shall be transported in a container which does not identify the contents as person served charts.

VI. Record Keeping

Employer realizes that personal as well as protected information is valuable to each employee and person receiving services. Care and caution must be taken by all employees with all paper and electronic versions records. Creating, storing or archiving and disposal all must be handled in a secure way.

Employees are expected to maintain all record keeping in a current, secure fashion, and will only be shared with authorized persons as a need to know basis.

Employees are expected to exercise care, caution and guarded actions when utilizing any records.

Employees are expected to re-file all records immediately after usage.

Employees are expected to never leave out sensitive and or confidential information.

Employees will keep current and accurate record keeping of all duties and services provided to persons served.

Employees will complete all documentation as the event occurs, and no later than when their respective scheduled shift ends.

Employees must not leave the shift until all documentation regarding person served services, health, safety, illnesses and accidents are completed.

All employees will present all received records via mail, fax, and or personal delivery to their immediate supervisor. If the supervisor is not available, then these records will be

placed in a secure place, and the supervisor notified.

Employee and or person served records are to filed within (5) days of receiving. Until filed these documents are to be kept in a secure place.

All records will be handled in a secure manner. No employee and or person served records are to be kept out in an unsecured place or where any unauthorized person may see, make copy or take a picture.

All documentation must be done per the individual Person Center Plan, or based upon Reporting Requirements, and or other policies.

Services to persons served must be documented with an Employee Signature, Title, and Date.

Employees negligent in providing service delivery documentation and or any other required documentation, will result in corrective actions, which may include termination.

Employees knowingly providing false documentation will result in corrective actions, which may include termination, criminal charges, fines and other penalties.

VII. Safeguards of Telephone, Cell Phones, Fax, and Mail system use

The telephones in the work site are for conducting work-related business and for the personal use of the Persons Served living in the home.

Employees may use the telephone for personal emergencies up to five (5) minutes of personal call time per shift. Employees may not charge any long distance calls to the work site telephone number. Employees are strictly forbidden from using any Employer telephones for international calls, and or calls to businesses that charge the employer telephone number for the usage of their services. Employees are not to receive personal phone calls during work time. Calls to friends and family should be made on the Employee's off time.

Employee's (not including administrative and management Employees) bringing personal cell phones and beepers into the work site must follow the five (5) minutes of personal call time per shift rule the same as for a telephone. The Employee's attention needs to be with the Person Served and not with out side phone calls. The Supervisor may require an Employee to remove the cell phone from the work site at the Supervisor's discretion.

Pictures from Camera Phones are not allowed. Employees are forbidden from to taking pictures with their phones of persons served, work site, or other Employees. Managers and Administrative personnel may allow the usage of camera phones when signed consent forms are present for person(s) in the picture. This consent is for persons served and employees.

Text Messaging, Blogging, and Tweeting on cell phones is not allowed while signed in for the Employer.

Fax machines are for the use of business related to the Persons Served and should not be used for Employee's personal business. Employees will follow the Fax Security Policy for using the facsimile machines. Employees will not use the fax machine to make copies for personal usage.

The use of the Employer's paid postage for personal correspondence is not permitted.

VIII. Received Faxes

The designated Employee(s) in each department shall remove all received faxes from the fax machine promptly upon the faxes' receipt and deliver the fax to the intended recipient. If delivery cannot be accomplished immediately, the designated Employee, shall maintain the faxes in a confidential file until delivery is accomplished.

IX. Sending Faxes

All faxes must be sent with a fully completed company approved cover sheet. Each fax number to which the materials are being faxed shall be double checked before being sent.

X. Safeguards for Social Security Number

Policy

It is the policy of the Employer to protect the confidentiality of Social Security numbers obtained in the ordinary course of the Employer's business from employees, vendors, contractors, customers or others. No person shall knowingly obtain, store, transfer, use, disclose, or dispose of a Social Security number that the Employer obtains or possesses except in accordance with the Act and this Privacy Policy.

Procedure

Social Security numbers should be collected only where required by federal and state law or as otherwise permitted by federal and state law for legitimate reasons consistent with this Privacy Policy. Legitimate reasons for collecting a Social Security number may include, but are not limited to:

1. Applicants may be required to provide for purposes of a pre-employment background check.

2. Copies of Social Security cards for purposes of verifying employee eligibility for employment.

3. Social Security numbers may be obtained from employees for tax reporting purposes, for new hire reporting or for purposes of enrollment in any Employer employee benefit plans.

4. Social Security numbers may be obtained from creditors or vendors for tax reporting purposes.

5. Social Security numbers may be obtained and used for completing person served entitlement applications, renewals and reports.

6. Social Security numbers may be obtained and used for person served medical, dental and other clinical services.

Access to Social Security Numbers
Only personnel who have legitimate business reasons to know will have access to records containing Social Security numbers. The department head having access to records containing Social Security numbers shall determine which other personnel within their departments have a legitimate reason in the Employer's ordinary course of business to have access to such social Security numbers. Personnel using records containing Social Security numbers must take appropriate steps to secure such records when not in immediate use.

Account Numbers
All or more than four sequential digits of a Social Security number shall not be used as a primary account number for an individual.

Computer Transmission
All or more than four sequential digits of a Social Security number shall not be used or transmitted on the Internet or on a computer system or network unless the connection is secure or the transmission is encrypted.

Disposal
Documents containing Social Security numbers will be retained in accordance with the requirements of state and federal laws. At such time as documents containing Social Security numbers may be disposed of, such disposal shall be accomplished in a manner that protects the confidentiality of the Social Security numbers, such as shredding.

Mailed Documents
Employer documents containing all or more than four sequential digits of a Social Security number shall only be sent in cases where state or federal law, rule, regulation, or court order or rule authorizes, permits or requires that a Social Security number appear in the document. Documents containing all or more than four sequential digits of a Social Security number, that are sent through the mail, shall not reveal the number through the envelope window or otherwise be visible from outside the envelope or package.

Mandated Use of Social Security Number
As an employer, Employer is required by federal and state law to use Social Security numbers (SSNs) to report and withhold payroll taxes. The Employer will use employee SSNs for payroll functions, expense reimbursement, and federal and state income tax reporting purposes.

Public Display
All or more than four sequential digits of a Social Security number shall not be placed in identification cards, badges, time cards, employee rosters, bulletin board, permits, licenses or any other materials or documents designed for public display. Documents, materials or computer screens that display all or more than four sequential digits of a Social Security number shall be kept out of public view at all times.

Storage
All documents containing Social Security numbers shall be stored in a physically secure manner. Social Security numbers shall not be stored on computers or other electronic devices that are not secured against unauthorized access.

Unauthorized Use or Disclosure of Social Security Numbers
The Employer shall take reasonable measures to enforce this Privacy Policy and to correct and prevent the reoccurrence of any known violations. Any employee, who knowingly obtains, uses or discloses Social Security numbers for unlawful purposes or contrary to the requirements of this privacy policy shall be subject to discipline up to and including discharge. Additionally, certain violations of the Act carry criminal and/or civil sanctions. The Employer will cooperate with appropriate law enforcement or administrative agencies in the apprehension and prosecution of any person who knowingly obtains uses or discloses Social Security numbers through the Employer for unlawful purposes.

XI. Trash.

All trash that contains protected health information must be placed shredded or placed in the designated receptacles to be shredded. The designated receptacles shall be located only in office rooms that can be locked when the office is closed.

APPENDIX C

Protocols for Routine and Recurring Requests by Quest, Inc.

(1) Requests for Information When Receiving a Referral.

The information requested should be limited to the person served's name, address, telephone number, diagnosis, present condition, and the services required.

(2) Requests for Information to Verify Insurance Coverage.

The information requested should be limited to the person served's name, address, telephone number, diagnosis, present condition, the services required, insurance identification numbers, and, for group insurance, the name of the person who holds the coverage.

APPENDIX D

Protocols for Routine and Recurring Disclosures

(1) Disclosure for Referral Of Person served for Alternative Services.

The information disclosed should be limited to the person served's name, address, telephone number, diagnosis, present condition, and the services required.

(2) Disclosure for Insurance Reimbursement.

The information disclosed should be limited to the person served's name, the insurance enrollee's name, the insurance numbers, any additional insurance name and numbers, dates of service, diagnosis, date of birth, date of death if applicable, visit notes, and the charges for services.

APPENDIX E

Fees for Copies of Protected Health Information

Fees will be collected by the Privacy Office prior to the release of any information. The current fee schedule is set at:

$ .50 per page of information

APPENDIX F

Fees for Accounting

- For the first accounting in a twelve (12) month period - No Charge.
- For the second or greater accounting in a twelve (12) month period - $30.00 per accounting

Quest, Inc., INC.

POLICIES FOR PROTECTION OF THE PRIVACY OF PROTECTED HEALTH INFORMATION

INDEX