Advantage Dental
From DentaQuest

Policy Name: Privacy Policy	**Policy Number: CP04-Privacy Policy-CARE**
Type of Policy: Care Delivery Compliance	**Effective Date: 8/9/2018**
Responsible Department: Compliance Department	
Page Number (s): 24	**Revised Date: 8/9/2018**
Approved By: Compliance Committee	**Approved Date: 8/9/2018**

PURPOSE: To ensure the protection and confidentiality of *protected health information* that is created, received, maintained, or transmitted with regard to members and patients of Our organization or an organization with whom We have a *Business associate* agreement with.

DEFINITIONS:

"Breach" means an impermissible *use* or *disclosure* under the Privacy Rule that compromises the security or privacy of the *PHI*. An impermissible *use* or *disclosure* of *PHI* is presumed to be a *breach* unless the *covered entity* or *Business associate*, as applicable, demonstrates that there is a low probability that the *PHI* has been compromised based on a risk assessment of at least the following factors:

The nature and extent of the *PHI* involved, including the types of identifiers and the likelihood of re-identification;
The unauthorized person who *used* the *PHI* or to whom the *disclosure* was made;
Whether the *PHI* was actually acquired or viewed; and
The extent to which the risk to the *PHI* has been mitigated.

"Business associate" is an individual or entity that provides data transmission services with respect to *PHI* to a *covered entity* and that requires access on a routine basis to such *PHI*; an individual that offers a personal health record to one or more individuals on behalf of a *covered entity*; or a subcontractor that creates, receives, maintains, or transmits *PHI* on behalf of the *Business associate*. (See exclusions specific to *health care provider*s, plans sponsors, government agencies and covered entities)

"Covered entity" is a *Health plan*, *Health care clearinghouse* or *Health care provider* who transmits health information in electronic form in connection with one or more transactions.

"Designated record set" means an item, collection, or grouping of information that includes *PHI* or *nonpublic personal information* and is maintained, collected, *used*, or disseminated by or for a *covered entity*.

"Disclosure" means releasing, transferring, or divulging information outside the entity holding the information, or providing access to the information for any entity other than the entity holding the information.

"Electronic Protected Health Information (ePHI)" means *Protected Health Information* that is

transmitted by electronic media or maintained in electronic media.
"Group health plan" (also see definition of *health plan* in this section) means an employee welfare benefit plan (as defined in section 3(1) of the Employee Retirement Income and Security Act of 1974 (ERISA), 29 U.S.C. 1002(1)), including insured and self-insured plans, to the extent that the plan provides medical care (as defined in section 2791(a)(2) of the Public Health Service Act (PHS Act), 42 U.S.C. 300gg-91(a)(2)), including items and services paid for as medical care, to employees or their dependents directly or through insurance, reimbursement, or otherwise, that:

(1) Has 50 or more participants (as defined in section 3(7) of ERISA, 29 U.S.C. 1002(7)); or

(2) Is administered by an entity other than the employer that established and maintains the plan.

"Health care" is care, services, or supplies related to an individual's health.

"Health care clearing house" means a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches, that does either of the following functions:

(1) Processes or facilitates the processing of *health information* received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.

(2) Receives a standard transaction from another entity and processes or facilitates the processing of *health information* into nonstandard format or nonstandard data content for the receiving entity.

"Health care operations" means any of the following activities of the covered entity 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; patient safety activities (as defined in 42 CFR 3.20); population-based activities relating to improving health or reducing *health care* costs, protocol development, case management and care coordination, contacting of *health care providers* and patients with information about *treatment* alternatives; and related functions that do not include *treatment*;

(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) Except as prohibited under § 164.502(a)(5)(i), underwriting, enrollment, premium rating, and other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for *health care* (including stop-loss insurance and excess of loss insurance), provided that the requirements of § 164.514(g) are met, if applicable;

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

(5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

(6) Business management and general administrative activities of the entity, including, but not limited to:

(i) Management activities relating to implementation of and compliance with the requirements of this subchapter;

(ii) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer.

(iii) Resolution of internal grievances;

(iv) The sale, transfer, merger, or consolidation of all or part of the *covered entity* with another covered entity, or an entity that following such activity will become a *covered entity* and due diligence related to such activity; and

(v) Consistent with the applicable requirements of § 164.514, creating *de-identified health information* or a *limited data set*, and fundraising for the benefit of the *covered entity*.

"Health care provider" is a person or entity who furnishes, bills, or is paid for *health care* in the normal course of business.

"Health information" means any information, including genetic information, whether oral or recorded in any form or medium, that:

(1) Is created or received by a *health care provider*, *health plan*, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

(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.

"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, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, 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 plan" means an individual or group plan that provides, or pays the cost of, medical care.

"Individually identifiable health information" is information that is a subset of health

information, including demographic information collected from an individual, and:

(1) Is created or received by a *health care provider*, *health plan*, employer, or *health care clearinghouse*; and

(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

(i) That identifies the individual; or

(ii) With respect to which there is a reasonable basis to believe the information can be *used* to identify the individual.

Marketing:

(1) Except as provided in paragraph (2) of this definition, marketing means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.

(2) Marketing does not include a communication made:

(i) To provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by the *covered entity* in exchange for making the communication is reasonably related to the *covered entity*'s cost of making the communication.

(ii) For the following *treatment* and *health care operations* purposes, except where the covered entity receives financial remuneration in exchange for making the communication:

(A) For *treatment* of an individual by a *health care provider*, including 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) To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the *covered entity* making the communication, including communications about: the entities participating in a *health care provider* network or *health plan* network; replacement of, or enhancements to, *a health plan*; and health-related products or services available only to a *health plan* enrollee that add value to, but are not part of, a plan of benefits; or

(C) For case management or care coordination, contacting of individuals with information about *treatment* alternatives, and related functions to the extent these activities do not fall within the definition of *treatment*.

(3)Financial remuneration means direct or indirect payment from or on behalf of a third party whose product or service is being described. Direct or indirect payment does not include any payment for *treatment* of an individual.

"Minimum necessary" means the minimum amount of *PHI* necessary to accomplish the intended purpose of the *use*, *disclosure*, or request. This does not apply to *uses* or *disclosures* that are for treatment, to the individual who is the subject of the *PHI*, pursuant to an authorization, to the Secretary of HHS, required by law, or required for compliance with HIPAA rules.

"Payment" means:

(1) The activities undertaken by:

(i) Except as prohibited under § 164.502(a)(5)(i), a *health plan* to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the *health plan*; or

(ii) A *health care provider* or *health plan* to obtain or provide reimbursement for the provision of *health care*; and

(2) The activities in paragraph (1) of this definition relate to the individual to whom *health car*e is provided and include, but are not limited to:

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

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

(iii) 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;

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

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

(vi) Disclosure to consumer 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; and

(F) Name and address of the *health care provider* and/or *health plan*.

"Personal representative" is:

Person legally authorized to make *health care* decisions on behalf of an individual who is an adult or emancipated minor.

Executor, administrator, or person legally authorized to act on behalf of a deceased individual or the estate.

Parent, guardian, or person acting <u>in loco parentis</u> legally authorized to make *health care* decisions on behalf of an individual who is an unemancipated minor, unless:

(a) The minor agrees to *health care*, no other agreements are required by law, and the minor has not requested a parent, guardian, person acting in

loco parentis, or another person to be regarded as a *personal representative*.

(b) The minor, a court, or a legally authorized person agrees to *health care*, and applicable State or other law allows the minor to obtain the *health care* without agreement of a parent, guardian, or person acting in loco parentis.

(c) The parent, guardian, or person acting in loco parentis assents to a confidentiality agreement between the minor and the covered *health care provider* regarding *health care*.

"Plan sponsor" means

(1) The employer in the case of an employee benefit plan established or maintained by a single employer,

(2) The employee organization in the case of a plan established or maintained by an employee organization, or

(3) in the case of a plan established or maintained by two or more employers or jointly by one or more employers and one or more employee organizations, the association, committee, joint board of trustees, or other similar group of representatives of the parties who establish or maintain the plan.

"Protected Health Information (PHI)" means *individually identifiable health information*:

(1) Except as provided in paragraph (2) of this definition, that is:

(i) Transmitted by electronic media;

(ii) Maintained in electronic media; or

(iii) Transmitted or maintained in any other form or medium.

"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 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.

"Research" means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

"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.

"Unsecured protected health information" means *protected health information* that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5.

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

"Workforce" means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a *covered entity* or *Business associate*, is under the direct control of such *covered entity* or *Business associate*, whether or not they are paid by the *covered entity* or *Business associate*.

POLICY: This Policy applies to *protected health information (PHI)* that We (as a *covered entity* offering *health plan* coverage or health services, we as a *Business associate* administering dental or vision coverage and other *health plan* services on behalf of Our client's *health plans*) or We as a Group Health Plan offering *health plan* coverage to plan sponsors and You (as a member of Our *workforce*) *use*, *disclose*, transmit or maintain in any format (including electronic, paper, and spoken).

PROCEDURES:

REQUIRED AND PERMITTED USES AND DISCLOSURES

1) *Covered entity* Required and Permitted *Uses* and *Disclosures* 164.502(a) (1), (2)
    a. We will *disclose PHI* as required to:
        i. To the individual when they request access to or an accounting of their *PHI*; and
        ii. To the Secretary of HHS to investigate or determine Our compliance with HIPAA regulations.
    b. We will *disclose PHI* as permitted:
        i. To the individual;
        ii. For treatment, payment, or *health care* operations;
            1. We will *use PHI* for Our own treatment, payment, or *health care* operations.
            2. We will *disclose PHI* for the treatment activities of a *health care provider*.
            3. We will *disclose PHI* to a *covered entity* or *health care provider* for the payment activities of the entity that receives the information.
            4. We will *disclose PHI* to a *covered entity* for *health care* operations activities of the entity that receives the information, if both We and the entity have a relationship with the individual and the *disclosure* is for the purposes of *health care* operations or *health care* fraud, waste and abuse detection or compliance.
            5. If We participate in an organized *health care* arrangement, we may *disclose PHI* to other participants in the arrangement for any *health care* operations of those in the arrangement.
        iii. With a valid authorization as described below (164.508):
            1. We require an authorization before disclosing *PHI* for:
                a. Psychotherapy notes;
                b. Marketing purposes; and.

c. Sale of *PHI;*

2. Any financial remuneration expected for disclosure of *PHI* for marketing or sales purposes will be *disclosed* when requesting authorization.
3. A valid authorization is written in plain language and must include:
    a. A description of the information to be *used* or *disclosed*
    b. The name or other specific identification of the person(s), or class of persons, authorized to make the requested *use* or *disclosure*
    c. A description of each purpose of the requested *use* of *disclosure*. The statement "at the request of the individual" is sufficient description when individual initiates the authorization and does not, or elects not to, provide a statement of the purpose
    d. An expiration date or an expiration event. Writing "none" is acceptable.
    e. Statement of individual's right to revoke the authorization and description of how to revoke.
    f. Statement that We may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization.
    g. Signature and date of signature. If signed by a representative, a description of the representative's authority. Proof may be required of this authority.
4. A copy of the signed authorization is provided to the individual.

iv. Having allowed the opportunity for the individual to agree or to object (164.510). If the individual orally agrees to the disclosure of their *PHI*, we will *disclose* their information only as agreed to and in that specific instance being addressed in that conversation.

v. We may disclosure the individual's *PHI* without obtaining authorization in the following circumstances (164.512);
    1. When required by law;
    2. For public health purposes;
    3. To report abuse, neglect or domestic violence;
    4. To a health oversight agency;
    5. For judicial or an administrative proceeding;
    6. For law enforcement purposes;
    7. To a coroner or medical examiner;
    8. For cadaveric organ, eye or tissue donation purposes;
    9. For research purposes;
    10. Avert a serious threat to health or safety;
    11. For specialized government functions; or
    12. To comply with workers compensation laws;

vi. We may *use* and *disclose PHI* without obtaining authorization in the following circumstances:

1. In a limited data set;
2. For Our fundraising purposes if We have *disclosed* this purpose in Our Notice of Privacy Practices (164.514(f));
3. For Our underwriting purposes (164.514(g)), but We will not *use* or *disclose* genetic information for underwriting purposes (164.502(a)(5);
4. De-identified *PHI* (164.502(d), see also 164.514(a) and (b)); or
5. To a *Business associate* to create, receive, maintain, or transmit *PHI* on behalf of *covered entity.*

vii. A *covered entity workforce* member may *disclose PHI* as a whistleblower 164.502(j) (1).

viii. A *covered entity workforce* member may *disclose PHI* as a victim of a crime 164.502(j) (2).

c. When using, disclosing or requesting *PHI*, we will make reasonable efforts to limit *PHI* to the *minimum necessary* to accomplish the intended purpose of the *use*, disclosure, or request (164.502(b)).
   i. Minimum necessary does not apply to:
      1. *Disclosures* to or requests by a *health care provider* for treatment;
      2. *Uses* or *disclosures* made to the individual;
      3. *Uses* or *disclosures* made pursuant to an authorization;
      4. *Disclosures* to the Secretary of HHS;
      5. *Uses* or *disclosures* required by law – 164.512(a); or
      6. *Uses* or *disclosures* required for compliance with HIPAA regulations.

2) *Business associate* Required and Permitted *Uses* and *Disclosures* that apply to Us as a *Business associate*.
   a. We will *disclose PHI* as required (164.201(a)(4)):
      i. To the Secretary of HHS to investigate or determine compliance;
      ii. To the *covered entity* We have a *business associate*'s agreement with to satisfy their obligations; and
      iii. To the individual or individual's designee when electronic copy is requested.
   b. We will *disclose* PHI as permitted to subcontractor to create, receive, maintain, or transmit *PHI* on behalf of *Business associate* (164.504(e)(1)(i)).

3) Personal representatives.
   a. As a *covered entity*, we will treat the *personal representative* as if they were the individual 164.502(g) except when We:
      i. Have reasonable belief the individual has been or may be subjected to domestic violence, abuse, or neglect by *personal representative*
      ii. Have reasonable belief that treating them as the *personal representative* could endanger the individual
      iii. We, in the exercise of professional judgement, decide it is not in the best interest of the individual
   b. The *personal representative* of a minor is the parent, guardian or person acting *in loco parentis* is a *personal representative* of the minor except when:

i. Minor consents to *health care* service; or
ii. Minor may lawfully obtain *health care* service without their consent; or
iii. Parent, guardian or person acting in loco parentis assents to confidentiality.

c. For an individual who is deceased, the *personal representative* is an executor, administrator, or other person who has authority to act on behalf of a deceased individual or their estate is the *personal representative* of the deceased with regard to their *PHI*.

BUSINESS ASSOCIATES 164.504(e)

1) *Business associate* Contracts
   a. A *Business associate* contract or a *Business associate* subcontractor contract will:
      i. Establish permitted and required *uses* and *disclosures* of *PHI* by the *Business associate*/subcontractor per the requirements of 45 CFR 164.504.
      ii. Not allow the *Business associate*/subcontractor to *use* or further *disclose* the information other than as permitted or required by the contract or as required by law
      iii. Require *use* of appropriate safeguards and compliance, where applicable, with HIPAA security requirements with respect to electronic *PHI*, to prevent *use* or *disclosure* of the information other than as provided for by the contract
      iv. Require the *Business associate*/subcontractor to report to us any *use* of *disclosure* of the information not provided for by the contract of which it becomes aware, including *breach*es of unsecured *PHI*.
      v. Ensure that any subcontractors that create, receive, maintain, or transmit *PHI* on behalf of the *Business associates* agree to the same restrictions and conditions that apply to the *Business associate* with respect to such information.
      vi. Make available *PHI* in accordance with 164.524
      vii. Make available *PHI* for amendment and incorporate any amendments to *PHI* in accordance with 164.526
      viii. Make available the information required to provide an accounting of *disclosures* in accordance with 164.528.
      ix. Requirement to carry out Our obligations and comply with HIPAA requirements that apply to us in the performance of such obligation
      x. Make available all documents relating to the *use* and *disclosure* of *PHI* received from or created or received by the *Business associate*/subcontractor on Our behalf to the Secretary of HHS for purposes of determining Our compliance with HIPAA requirements.
      xi. Return or destroy all *PHI* received from or created or received by the *Business associate*/subcontractor on Our behalf that the *Business associate*/subcontractor still maintains in any form upon termination of the contract and retain no copies, or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further *uses* and *disclosures* to those purposes

that make the return or destruction of the information infeasible.

xii. Authorize termination of the contract by us, if We determine that the *Business associate*/subcontractor has violated a material term of the contract.

b. If We know of a pattern of activity or practice of a *Business associate* or subcontractor that constituted a material *breach* or violation of the *Business associate's* or subcontractor's obligation under the contract or other arrangement, we will take reasonable steps to cure the *breach* or end the violation, as applicable, and, if such steps are unsuccessful, terminated the contract or arrangement, if feasible.

GROUP HEALTH PLAN 164.504(f)

1) As a *group health plan*, we will restrict uses and disclosures of information in plan documents by the *plan sponsor*.

2) We will only *disclose* summary health information to the *plan sponsor* when this is requested by them for the purposes of:
    a. Obtaining premium bids from health plans for providing health insurance coverage under the *group health plan*; or
    a. Modifying, amending, or terminating the *group health plan*.
3) We will disclose information to the *plan sponsor* on whether the individual is participating in the *group health plan* or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan.
4) Plan documents from group health plans will be amended to:
    a. Establish permitted and required uses and disclosures of information in plan documents by the plan sponsor;
    b. Provide that We will disclose PHI to the *plan sponsor* only upon receipt of a certification by the *plan sponsor* that the plan documents have been amended to incorporate the following provisions that the *plans sponsor* agrees to:
        i. Not use or further disclose the information other than as permitted or required by the plan documents or as required by law;
        ii. Ensure that any agents to whom it provides *protected health information* received from the *group health plan* agree to the same restrictions and conditions that apply to the *plan sponsor* with respect to such information;
        iii. Not *use* or *disclose* the information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the *plan sponsor*;
        iv. Report to the *group health plan* any use or disclosure of the information that is inconsistent with the *uses* or *disclosures* provided for of which it becomes aware;
        v. Make available *protected health information* in accordance with § 164.524;
        vi. Make available *protected health information* for amendment and incorporate any amendments to *protected health information* in

accordance with § 164.526;

vii. Make available the information required to provide an accounting of *disclosures* in accordance with § 164.528;

viii. Make its internal practices, books, and records relating to the *use* and *disclosure* of *protected health information* received from the *group health plan* available to the Secretary for purposes of determining compliance by the *group health plan* with this subpart;

ix. If feasible, return or destroy all *protected health information* received from the *group health plan* that the sponsor still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible; and

x. Ensure that the adequate separation required in paragraph (f)(2)(iii) of this section is established.

5) We will provide for adequate separation between the *group health plan* and the *plan sponsor*. The plan documents must:
   a. Describe those employees or classes of employees or other persons under the control of the *plan sponsor* to be given access to the *protected health information* to be *disclosed*, provided that any employee or person who receives *protected health information* relating to *payment* under, *health care operations* of, or other matters pertaining to *the group health plan* in the ordinary course of business must be included in such description;
   b. Restrict the access to and use by such employees and other persons described in paragraph (f)(2)(iii)(A) of this section to the plan administration functions that the *plan sponsor* performs for the *group health plan*; and
   c. Provide an effective mechanism for resolving any issues of noncompliance by persons described in paragraph (f)(2)(iii)(A) of this section with the plan document provisions required by this paragraph.
6) We, as a *group health plan*, may:
   a. Disclose *protected health information* to a *plan sponsor* to carry out plan administration functions that the *plan sponsor* performs only consistent with the provisions of paragraph (f)(2) of this section;
   b. Not permit a health insurance issuer or HMO with respect to the *group health plan* to disclose *protected health information* to the *plan sponsor* except as permitted by this paragraph;

   c. Not *disclose* and may not permit a health insurance issuer or HMO to disclose *protected health information* to a *plan sponsor* as otherwise permitted by this paragraph unless a statement required by § 164.520(b)(1)(iii)(C) is included in the appropriate notice; and (iv) Not *disclose protected health information* to the *plan sponsor* for the purpose of employment-related actions or decisions or in connection with any other benefit or employee benefit plan of the *plan sponsor*.

NOTICE OF PRIVACY PRACTICES

1) Notice of Privacy Practices

a. We, as a *covered entity*, will create, distribute, post and maintain a Notice of Privacy Practices.
b. The content of the Notice of Privacy Practices:
    i. Must be in plain language
    ii. Must include header "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE *USED* AND *DISCLOSED* AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."
    iii. Description, including at least one example, of the types of *uses* and *disclosures* permitted for the purposes of treatment, payment, and *health care* operations. This will include sufficient detail for the individual to understand what *uses* and *disclosures* are permitted or required.
    iv. Description of other *uses* or *disclosures* permitted without the individual's written authorization. This will include sufficient detail for the individual to understand what *uses* and *disclosures* are permitted or required.
    v. Explanation that any other law prohibiting *use* or *disclosure* that is more stringent will take precedence.
    vi. Description of *uses* and *disclosures* that require an authorization.
    vii. A statement that any other *uses* and *disclosures* not described will be made only with the individual's authorization and that the individual may revoke an authorization.
    viii. A list of the individual's rights
        1. The right to request restrictions, including a statement that We are not required to agree to a requested restriction unless it is for services for which the individual has paid in full.
        2. The right to receive confidential communications of *PHI*
        3. The right to inspect and copy *PHI*
        4. The right to amend *PHI*
        5. The right to receive an accounting of *disclosures* of *PHI*
        6. The right of an individual to receive a paper copy of the notice upon request
        7. The right to file a complaint with us and to the Secretary of HHS if they believe their privacy rights have been violated, including instructions on how to file a complaint and a statement that they will not be retaliated against for filing a complaint.
    ix. A statement that We are required by law to maintain the privacy of *PHI*, to provide individuals with notice of its legal duties and privacy practices with respect to *PHI* and to notify affected individuals following a *breach* of unsecured *PHI*.
    x. A statement that We are required to abide by the terms of this notice
    xi. Explanation that We have the right to change the terms of this notice and make a new notice that applies to all *PHI* maintained and description of how We will provide individuals with a revised notice.

xii. Name or title and phone number of a person or office to contact for further information.
xiii. Effective date

c. Allowed Content
    i. We will include any additional permitted *uses* and *disclosures* as well as any allowed limitations to *uses* and *disclosures* in the notice.
d. Distribution
    i. As a *health plan*, we will promptly provide this notice to Our members upon enrollment and when there are any material changes to the notice.
    ii. As a *health plan*, we will notify members at least once every three years of the availability of the notice and how to obtain a copy.
    iii. As a *health care provider*, we will provide the notice on the date of the first service delivery.
    iv. As a *health care provider*, we will obtain a written acknowledgement of receipt of the notice, and if not obtained, document Our good faith efforts to obtain an acknowledgement with an explanation of why it was not received.
    v. As a *health care provider*, copies of the notice will be available to individuals at each service delivery site.
    vi. As a *covered entity*, we will post the notice in a clear and prominent location when individuals seeking services would be able to read the notice.
    vii. As a *covered entity*, we will post a copy of the notice on Our website in a prominent location allowing the individual the ability to read or print the notice.
    viii. As a *covered entity*, we will make updated copies available to the individual immediately upon any material change to the notice, including paper, electronic, facility postings and website postings.
e. Updates and Modifications
    i. Any changes to this notice will be made promptly when there is a material change to Our *uses* or *disclosures*, Our legal duties, the individual's rights or other privacy practices.
    ii. All versions of notices provided to individuals will be maintained along with documentation of distribution for a minimum of 6 years.

OTHER PRIVACY LAWS

1) When acting as a *covered entity*, we will comply with State and Federal laws that apply to Our *use* and *disclosure* of *PHI*. When acting as the *Business associate* of Our customer's *health plan*, we will monitor any changes to Our privacy obligations in the States in which We act as a *Business associate* and, to the extent applicable, communicate any changes to Our privacy obligations to Our *workforce*.

2) When acting as a *covered entity*, we will comply with State laws that give Our members' rights with respect to their *PHI*, including but not limited to the right to access or amend *PHI*. We will monitor any changes to Our privacy obligations in the States in which We act as a *Business associate* and, to the extent applicable, communicate any changes to

Our privacy obligations to Our *workforce*.

3) Other laws include but may not be limited to 42 CFR Part 2, FERPA and State privacy laws in the various states in which We do business.

INDIVIDUAL PRIVACY RIGHTS

1) Access – 164.524
    a. We will allow an individual access to inspect and obtain copy of their *PHI* kept by us in a *designated record set* with the exception of:
        i. Psychotherapy notes; and
        ii. Information compiled in reasonable anticipation of, or for *use* in, a civil, criminal, or administrative action or proceeding.
    b. We may deny access without providing the individual an opportunity to review if:
        i. The *PHI* is included in above exception
        ii. We, as a *health care provider*, are acting under the direction of a correctional institution and the request was from an inmate and access would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates.
        iii. The *PHI* is subject to Privacy Act, 5 U.S.C. 522a
        iv. If the *PHI* was obtained from someone other than a *health care provider* under a promise of confidentiality and the access would reasonably likely reveal the source of the information.
    c. We may deny access while providing the individual a right to have the denial reviewed in the following circumstances when a licensed *health care* professional of Our organization has determined, in the exercise of their professional judgement that:
        i. The access requested by the individual is reasonably likely to endanger the life or physical safety of the individual or another person;
        ii. The *PHI* requested makes reference to another person (not a *health care provider*) and a licensed *health care* professional of Our organization has determined, in the exercise of professional judgement, that the access is reasonably likely to cause substantial harm to the other person; or
        iii. When access is requested by a *personal representative* of the individual, that the provision of access to the *personal representative* is reasonably likely to cause harm to the individual or another person.
    d. When a review of denial of access is requested when permitted as described above, we will have a licensed *health care* professional who did not participate in the initial decision to deny review the request. Access will be provided or denied in accordance with their determination.
    e. An individual may request access to inspect or obtain a copy of their *PHI* that is maintained in a *designated record set*.
        i. This request must be in writing.
        ii. We will response to this request within 30 days of receipt of their written request. We may extend this time by 30 days if more time is needed to accommodate their request. We will notify the individual

in writing of the reason for the delay within 30 days of their written request.

iii. If We approve their request, we will provide access to the *PHI* in the form and format requested if readily producible. Otherwise We will provide a readable hard copy as agreed upon by us and the individual.

iv. If agreed upon by the individual in advance, we may provide a summary or explanation of the *PHI* and impose a fee.

v. We will arrange a convenient time and place to inspect or obtain a copy of the *PHI* or mail the *PHI* in accordance with the individual's request.

vi. If the individual requests that the *PHI* be sent to another party, we will comply with their written request outlining the designated person and where to send the copy of *PHI*.

vii. We may impose a fee to cover the costs of labor, supplies, postage and preparation of the *PHI* requested.

viii. If We deny all or a portion of their request, our response will be in writing and will include the following in plain language:

1. The basis for the denial
2. Right to request a review, if applicable
3. Process for submitting a complaint to us or to the Secretary of HHS.

ix. *Designated record set*s that are subject to access are documented.

x. The privacy officer of Our organization, or their designee, will receive and process requests for access.

2) Accounting 164.528

a. We will permit an individual to request and accounting of *disclosure* of their *PHI* made by us in the six years prior to the date of the request. This accounting will <u>not</u> include *disclosures*:

i. For the purposes of treatment, payment and *health care* operations

ii. Made to the individual requesting the accounting

iii. Authorized by the individual

iv. For national security or intelligence purposes

v. To correctional institutions or law enforcement officials having lawful custody of the individual.

vi. That are part of a limited data set

b. We will temporarily suspend this right if requested by a health oversight agency or law enforcement official for *disclosures* to that health oversight agency or law enforcement official:

i. If the agency or official provides a written or oral statement that the accounting would be likely to impede their activities and a timeframe for the suspension is provided.

ii. For no longer than 30 days unless a written statement is provided request longer

c. The accounting of *disclosures* will include:

i. The timeframe for the *disclosures*, no more than six years.

ii. *Disclosures* by or to Our *Business associates*

iii. The date of each *disclosure*

iv. The name of the entity or person who received the *PHI* and, if known, their address
v. A brief description of the *PHI disclosed*
vi. The purpose of the *disclosure*

d. The accounting of *disclosures* will be provided to the individual within 60 days of their request. We may extend this time by 30 days if more time is needed to accommodate their request. We will notify the individual in writing of the reason for the delay within 60 days of their request.
e. The first accounting request received from the individual within any 12-month period will be provided without charge. The individual will be notified that any additional requests received within that 12-month period will require a fee.
f. All *disclosures* that would be required to include in an accounting of *disclosures* will be documented in their electronic record.
g. The privacy officer of Our organization, or their designee, will receive and process requests for an accounting of *disclosures*.

3) Amendment 164.526
   a. We will permit an individual to request an amendment to their *PHI* maintained by us in a *designated record set*. This request must be in writing.
   b. We will approve or deny their request within 60 days of receipt of the written request. We may extend this time by 30 days if We are unable to complete within the required timeframe and We provide the individual written notice of the reason for the extension within 60 days of their written request.
   c. If We approve their request, We will:
      i. Inform the individual of this approval within the timeframe indicated above.
      ii. Amend this information in Our *designated record set* or note the record to indicate it is subject to an amendment and append or provide a link to the amendment.
      iii. After having obtained identification of an agreement from the individual, notify persons identified by the individual as having their *PHI* of this amendment.
      iv. Notify other persons, including *Business associates*, to whom We have *disclosed* the individual's *PHI* affected by this amendment of this amendment.
   d. We may deny their request for the following reasons:
      i. The *PHI* was not created by us
      ii. The *PHI* is not part of a *designated record set*
      iii. The *PHI* would not be available for access per the right of the individual for access.
      iv. The *PHI* is accurate and complete.
   e. If We deny their request, in whole or in part, we will provide a timely, written denial including the following in plain language:
      i. The reason for the denial
      ii. The individual's right to submit a written statement disagreeing with the denial with instructions on how to submit this statement.
      iii. The individual's right to request that their request for amendment and a copy of the denial be provided with any future *disclosures* of

the *PHI* subject to the amendment request.

iv. Process for submitting a complaint to us or the Secretary of HHS, including the name or title and phone number of the contact person or office designated for this purpose.

f. Any statement of disagreement with Our decision to deny will be added to the *PHI* in the *designated record set* subject to the disputed amendment as well as any rebuttal statement prepared by us.

g. All future *disclosures* will include documentation on a denied request for amendment, as described above.

h. If We receive notification of an amendment from another *covered entity*, we will amend the *PHI* in Our designated records set in accordance with the decision of the other *covered entity*.

i. The privacy officer of Our organization will be responsible for receiving, processing and documenting

4) Restriction 164.502(c) and 164.522

a. We will permit an individual to request a restriction to permitted *uses* and *disclosures* of *PHI*.

b. If We agree to this restriction, we will abide by it except when the individual is in need of emergency treatment and *use* or *disclosure* is required for that treatment.

c. We may disagree to a restriction request if it is a required *disclosure*.

d. We may disagree to a restriction request if it would prohibit Our ability to carry out treatment, payment and *health care* operations activities.

e. As a *health care provider*, we must agree to a restriction request if the *PHI* pertains solely to a *health care* item or service for which the individual or person other than the *health plan* on behalf of the individual has paid us in full.

f. A restriction request may be terminated if the individual requests or agrees to the termination and it does not apply to *PHI* for a *health care* item or service that was paid in full as indicated above.

g. All restriction requests will be documented in full, including whether We have agreed to the restriction or not, the effective date and any termination date.

5) Confidentiality 164.502(c) and 164.522

a. We will permit an individual to request that communications of *PHI* be received by the individual by alternative means or at alternative location.

b. We will accommodate all reasonable requests by the individual for these communications.

c. We will agree to all requests in which the individual clearly states that the *disclosure* of all or part of their *PHI* could endanger the individual.

d. The request from the individual must be in writing and must specify the other means of communication requested (i.e. phone number or address).

e. As a *health care provider*, we will not require an explanation of the reason for the request.

6) Complaints 164.530(d)

a. We will have a process for individuals to make complaints concerning Our privacy policies and procedures or Our compliance with privacy policies and procedures or HIPAA requirements.

b. All complaints received will be documented, including the resolution of each

complaint.

7) Intimidation and Retaliation 164.530(g)
    a. We will not allow any retaliation, intimidation, threatening, coercing, discrimination or retaliation by Our *workforce* members or *Business associates* against any individual for exercising their right or for their participation in any process provided for in Our policies and procedures or these requirements. This includes the filing of a complaint privacy complaint.
8) Waiver of Rights 164.530(h)
    a. We will not require individuals to waive their privacy rights as a condition of the provision of treatment, payment, enrollment in a *health plan* or eligibility for benefits.
9) Remuneration 164.530
    a. We will not request, accept, or provide remuneration in any form, directly or indirectly, in exchange for *PHI*.
        i. EXCEPTIONS. We may accept remuneration in exchange for *PHI* under the following circumstances:
            1. The exchange involves remuneration provided by a *covered entity* to a *Business associate* for activities involving the exchange of *PHI* that the *Business associate* undertakes on behalf of and at the specific request of the *covered entity* pursuant to a *Business associate* agreement as provided in Policy 3.2—*Business associates.*
            2. The purpose of the exchange is to provide an individual with a copy of the individual's *PHI*.
            3. Upon receipt of a signed authorization from the affected member or patient, provided that the authorization includes an explanation of whether the *PHI* may be further exchanged for remuneration by the person or entity receiving the affected member's *PHI*.
            4. The purpose of the exchange is for public health activities.
            5. The purpose of the exchange is for research and the remuneration We receive reflects the costs of preparation and transmittal of the *PHI* for the purpose of the research.
            6. The purpose of the exchange is for the treatment of the individual in compliance with Policy 3.1—Treatment, Payment, and *Health care* Operations, provided that the exchange complies with any rules promulgated by the Department of Health and Human Services on the subject. [Note: No such rules have been promulgated as of the original effective date of this Policy.]
            7. The purpose of the exchange is related to (i) the sale, transfer, merger, or consolidation of all or part of one *covered entity* with another *covered entity* or an entity that (following such activity) will become a *covered entity* or (ii) due diligence

related to such activities.

8. Rules promulgated by the Department of Health and Human Services that permit the exchange of remuneration for *PHI* for another purpose. [Note: No such rules have been promulgated as of the original effective date of this Policy.]

BREACH RESPONSE 164.402-414

10) The date of discovery of a *breach* is the first day on which the *breach* became known to us, or, by exercising reasonable diligence would have been known to us, a member of Our *workforce* or an agent of Our organization.
11) Risk Assessment
    a. We will assume that every impermissible *use* or *disclosure* of *PHI* is a *breach* unless a risk assessment is performed to indicate otherwise. The risk assessment will evaluate the following:
        i. Nature and Extent of the *PHI* involved including identifiers and the likelihood of re-identification.
        ii. The unauthorized person who impermissibly *used* or to whom the *PHI* was *disclosed*.
        iii. Whether or not the *PHI* was actually acquired or views or whether there was an opportunity for the *PHI* to be acquired or viewed.
        iv. Extent to which the risk has been mitigated.
    b. If this risk assessment determines that the likelihood of the information being *used* or *disclosed* is now and the *PHI* in question is not likely to be identified or impermissibly *used* or *disclosed*, then the impermissible *use* or *disclosure* will be determined to not be a *breach*.
        i. The risk assessment will be performed by the privacy officer.
        ii. A copy of the risk assessment will be kept with the documentation of the incident.
    c. If the risk assessment determines that the impermissible *use* of *disclosure* is a *breach* or if a risk assessment is not performed, the appropriate notifications will be sent as indicated below.
12) Notifications
    a. To the Individual – We will notify the individual of *breach* within 60 days of the date of discovery. 164.402
        i. This notification will be written in plain language and will include:
            1. The date of the *breach*
            2. The date of discovery
            3. A brief description of what happened
            4. A description or copy of the *PHI* involved in the *breach*
            5. Steps the individual should take to protect themselves from potential harm resulting from the *breach*
            6. A description of what We are doing to investigate, mitigate harm and protect against any further *breach*es; and
            7. Contact information and procedures for the individuals to ask question or obtain additional information. This will include a toll-free phone number, email address, web site or postal address.

ii. The notification will be sent by first-class mail to the individual at the last known address.
iii. If We do not have current contact information for 10 or more individuals affected by the *breach*, we will post a notice on the home page of Our website for a period of 90 days that includes a toll-free number for individuals to call to learn whether their *PHI* was involved in the *breach*.

b. To the media (164.406) – for *breach*es involving more than 500 residents of a State or jurisdiction, we will notify prominent media outlets serving that region no later than 60 calendar days after discovery of the *breach*. This notice will include:
   i. The date of the *breach*
   ii. The date of discovery
   iii. A brief description of what happened
   iv. A description of the *PHI* involved in the *breach*
   v. Steps the individual should take to protect themselves from potential harm resulting from the *breach*
   vi. A description of what We are doing to investigate, mitigate harm and protect against any further *breach*es; and
   vii. Contact information and procedures for the individuals to ask question or obtain additional information. This will include a toll-free phone number, email address, website or postal address.

c. To the Secretary (164.408) – We will notify the Secretary of HHS of *breach*es involving 500 or more individuals within 60 days of discovery of the *breach* and at the same time as notification is sent to the individuals. For *breach*es of less than 500 individuals, we will notify the Secretary of HHS no later than 60 days after the end of the calendar year in which the *breach* was discovered. Notifications to the Secretary will be sent according to instructions on the HHS website.

d. We, as a *Business associate*, will notify the *covered entity* of a *breach* within the timeframe required in the *Business associates* agreement to be no later than 60 calendar days after discovery of a *breach*. This notification will include the identification of each individual whose *PHI* is reasonably believe by us to have been accessed, acquired, *used* or *disclosed* during the *breach*. Any other information required for the *covered entity* to include in notifications will be provided as it is available. 164.410

e. Law enforcement delay – If notification of a *breach* could, according to a law enforcement official, impede a criminal investigation or cause damage to national security, we will delay notification no longer than 30 days unless a written statement from a law enforcement official specifies a longer timeframe. 164.412

f. Documentation of all notifications will be maintained by us for at least 6 years following the date of notification. 164.414

OVERSIGHT 164.530

13) Privacy Officer
   a. We have a designated privacy officer who is responsible for the development and implementation of the privacy policies and procedures. The privacy

officer, or their designee, is responsible for receiving and documenting privacy related complaints and concerns.

14) Training
    a. We will ensure that all members of Our *workforce* will complete HIPAA training within 10 days of hire and annually thereafter.
    b. If any changes in regulations of processes occur, all members of Our *workforce* will be educated and/or trained on these changes within a reasonable timeframe after the effective date of the change.
    c. All training materials and records will be maintained for at least six years.
15) Policies and Procedures
    a. We will have written policies and procedures comply with HIPAA and other applicable privacy standards. These will address all aspects of these requirements.
    b. Policies and procedures will be made available to and implemented by *workforce* members.
    c. Any changes to privacy regulations, requirements or processes will be promptly updated in Our policies and procedures.
    d. Privacy policies and procedures will be reviewed annually to ensure they are accurate and reflect current regulations, requirements and processes.
16) Safeguards
    a. We will implement appropriate administrative, technical, and physical safeguards to protect *PHI* from any intentional or unintentional *use* or *disclosure* that is in violation of HIPAA standards. This includes any incidental *uses* or *disclosures* made pursuant to an otherwise permitted or required *use* or *disclosure*.
17) Sanctions
    a. We will enforce appropriate sanctions against *workforce* members who do not comply with Our privacy policies and procedures.
    b. The privacy officer, or their designee, will document any sanctions applied.
18) Mitigation
    a. We will mitigate, to the extent practicable, any harmful effect of a *use* or *disclosure* of *PHI* by us or Our *Business associate* that is known to us and is in violation of Our policies and procedures or HIPAA requirements.
19) Document Retention
    a. All privacy policies, procedures and documentation required by HIPAA regulations will be maintained for at least six years from the date of creation or the date when it was last in effect, whichever is later.
20) Group Health Plans
    a. As a group health plan, we will have policies and procedures that address our HIPAA privacy responsibilities. These will be subject to the processes outlined in 17 above.

PROCEDURE

Revisions and distribution of Notice of Privacy Practices

Obtaining oral and written authorization

Verification of individual's identity process

Personal representative Documentation

Safeguarding *PHI*
- Physical
  - Locked Files
  - Building Security
  - Disposal
  - Workstation
- Verbal
  - Phone
  - Office

Electronic
- Passwords

Encryption
- Workstations

Remote and Mobile users

Sending of *PHI*
- Mail
- Fax
- Email
- Electronic Transmissions

Minimum necessary
- Routine *Disclosures*
- Individual Access

Breach
- Reporting of Violations

Documentation and Investigation
- Risk Assessment
- Notification
- Remediation and Corrective Action

Individual Rights
- Requests for Access process
- Requests for Amendments process
- Requests for an Accounting process
- Requests for Restrictions process
- Request for Confidentiality process

Privacy Complaints Handling

Privacy Training
- New Hire
- Ongoing
- Training Documentation
- Delegated Entities

REFERENCES
HIPPA; HITECH

FORMS AND OTHER RELATED DOCUMENTS (reference name)
SOPs
Attestation forms
Templates