PRIVACY POLICY

Overview & Definitions

1. In General. Under the federal Health Insurance Portability and Accountability Act of 1996 ("HIPAA") privacy, security and standard transaction regulations (45 \ Parts 160, 162 and 164) ("HIPAA Rules"), Business Data Applications, Inc. ("Company") is considered a Business Associate of its clients that are Covered Entities or that are Business Associates when it creates, receives, maintains or transmits Protected Health Information on their behalf. Company will treat Protected Health Information (or PHI) as defined below in accordance with these policies and procedures ("HIPAA Policies"). These HIPAA Policies apply only to PHI. Other policies may apply to the confidentiality and security of information that is not PHI and to personal information held by Company when not acting as a Business Associate.

2. Definitions. Terms contained in these HIPAA Policies shall have the meanings set forth below. If not defined below, any terms used in these HIPAA Policies that are defined in the HIPAA Rules shall have the meaning given to such terms in the HIPAA Rules. Business Associate means a person or entity who:

(1) on behalf of a Covered Entity, but other than in the capacity of a member of the workforce of such Covered Entity, creates, receives, maintains, or transmits PHI for a function or activity regulated by the HIPAA Rules, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed in 42 CFR § 3.20, billing, benefit management, practice management, and repricing; or

(2) provides, other than in the capacity of a member of the workforce of a Covered Entity, legal, actuarial, accounting, consulting, data aggregation (as defined in 45 CFR § 164.501), management, administrative, accreditation, or financial services to or for such Covered Entity, where the provision of the service involves the disclosure of PHI from such Covered Entity, or from another Business Associate of such Covered Entity, to the person.

- Breach means the acquisition, access, use or disclosure of PHI in a manner not permitted by the privacy provisions of HIPAA and that compromises the security or privacy of the PHI, unless an exception applies as described in Policy #HIPAA-8. Covered Entity is a health plan, healthcare provider or healthcare clearinghouse that is subject to the HIPAA Rules and is acting in such capacity. Most clients of Company are Covered Entities. Some of Company's clients may be Business Associates of Covered Entities.
- De-identified Information means information that does not include any of the following identifiers of an individual or the individual's employer, family members or household members: name; all geographic subdivisions smaller than a state (including street address, city, county, precinct and zip code); all elements of dates related to an individual (including birth date, admission date and discharge date) except for years (other than year of birth for those over 89);

telephone numbers; fax numbers; electronic mail address; social security number; medical record number; health plan beneficiary number; account number; certificate/license number; serial number of a vehicle or other device identifier; Internet URL; Internet protocol (IP) address number; biometric identifiers, including finger and voice prints; full face photographic images and any other unique information that could reasonably be used alone or in combination with other information to identify an individual.

- Designated Record Set means a group of records maintained by or for a Covered Entity (or a client that is a Business Associate) that is:
  - the medical record and billing records about individuals maintained by or for a covered health care provider;
  - the enrollment, payment, claims adjudication and case or medical management record systems maintained by or for a health plan; or
  - used, in whole or in part, by or for the Covered Entity to make decisions about individuals. Electronic PHI means PHI that is transmitted by electronic media or maintained in electronic media.
  - The term "electronic media" means:
  - electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or
  - transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet (wide-open), extranet (using Internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media because the information being exchanged did not exist in electronic form before the transmission.
- Genetic Information means information about:
  - an individual's genetic tests,
  - the genetic tests of family members of the individual, and
  - the manifestation of a disease or disorder in family members of such individual. It includes any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by the individual or any family member of the individual. It does not include information about the sex or age of any individual. HHS means the U.S. Department of Health and Human

3. Services. Protected Health Information ("PHI") means information that

(1) is received from, or created or received by a Business Associate, on behalf of a Covered Entity (or a Business Associate of a Covered Entity), whether oral, written or electronic;
(2) relates to the past, present or future physical or mental health 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) identifies the individual or provides a reasonable basis to believe the information at issue can be used to identify the individual.

- PHI is "protected" in all forms, including paper records, oral communications and electronic media. PHI includes Genetic Information. PHI pertains to both living and deceased individuals unless the individual has been deceased for more than fifty (50) years. Company will assume that an individual has not been deceased for more than fifty (50) years unless it has received documentation or evidence of death of the individual.
- De-identified information (as defined above) is not PHI.
- Security Incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
- Subcontractor means a person or entity to whom a Business Associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such Business Associate. Subcontractors that create, receive, maintain or transmit PHI on behalf of a Business Associate are also considered to be Business Associates. When Company is acting on behalf of a client that is a Business Associate of a Covered Entity, Company is a Subcontractor and will comply with these HIPAA Policies in the same manner as when Company contracts directly with a client that is a Covered Entity.
- Unsecured PHI means PHI that is not rendered unusable, unreadable or indecipherable to unauthorized individuals through the use of a technology or methodology specified on the HHS Website (www.hhs.gov/ocr/ privacy). For example, PHI that has not been encrypted in accordance with HHS guidance or that has not been shredded or destroyed so that the information cannot be read or reconstructed is unsecured PHI.
- Workforce members means employees, volunteers and other persons whose conduct, in the performance of work for Company, is under the direct control of Company, whether or not they are paid by Company, and who have access to PHI.

4. Privacy Officer. Danielle Anderson is the designated Privacy Officer of Company. The Privacy Officer shall oversee the implementation and enforcement of these HIPAA Policies. The obligations of the Privacy Officer described in these HIPAA Policies shall be performed by the Privacy Officer or the Privacy Officer's designee. The Privacy Officer is responsible for all obligations specified in these HIPAA Policies as being an action required to be performed by, or supervised by, the Privacy Officer and for taking acts necessary to carry out these HIPAA Policies, including but not limited to the following:

- Ensuring Business Associate Agreements are in place with Company's clients and ensuring that Subcontractor Business Associate Agreements are in place with Company's vendors who handle PHI on its behalf;
- Reviewing, approving and negotiating Business Associate Agreements and Subcontractor Business Associate Agreements;
- Training Company workforce members on these HIPAA Policies;
- Responding to patterns of activity or practices that constitute violations of these HIPAA Policies;
- Overseeing prompt and appropriate investigation and resolution of incidents or complaints;
- Implementing steps necessary to mitigate harm caused by violations of the HIPAA Rules or these HIPAA Policies by Company;
- Implementing client requests related to patient rights;
- Maintaining documentation required by these HIPAA Policies;
- Making required HIPAA-related reports to clients and being the point person for interacting with clients for issues related to compliance with the HIPAA Rules;
- Reviewing and revising these HIPAA Policies as necessary to comply with the HIPAA Rules, Company's contractual obligations to clients and changes to Company's operations.

Business Associate Obligations & Agreements

1. Business Associate Agreements. When Company is acting as a Business Associate, Company must comply with the terms of its Business Associate Agreements. As a Business Associate, Company is also directly liable under the HIPAA Rules for the privacy and security obligations applicable to Business Associates, as set forth in these HIPAA Policies.

2. Agreements with Clients. Company has developed a standard Business Associate Agreement template that meets the requirements set forth in the HIPAA Rules that is maintained by the Privacy Officer. At the beginning of a new client relationship that involves Company acting as a Business Associate and before receiving PHI, Company will confirm that a Business Associate Agreement is in place with the client. When possible, Company will use its Business Associate Agreement template. If a client requests Company to sign its form or requests changes to Company's form, the agreement or requested changes will be forwarded to the Privacy Officer for review, approval and negotiation, if necessary. Business Associate Agreements may not be signed without the Privacy Officer's prior approval.

The Privacy Officer or his/her designee will sign all Business Associate Agreements with clients (that are not incorporated into the relevant service agreement) and return an original to the client. Copies of all signed Business Associate Agreements will be forwarded to the Privacy Officer and kept for a minimum of six years following original signature or the last date the agreement was in effect, whichever is longer.

3. Subcontractors of Company. Before allowing any Subcontractors of Company to create, receive, maintain or transmit PHI on behalf of Company, Company will confirm that a Subcontractor Business Associate Agreement is in place with the Subcontractor. Company is required to obligate Subcontractors to the same restrictions and conditions as agreed to by Company in its Business Associate Agreements with clients. An example of a Subcontractor of Company is any non-workforce member who Company engages to perform a task that will require access, use, handling or disclosure of PHI, such as consultant, software developers who must access PHI and temporary non-employee workers who may access PHI. Whenever possible, Company will use its standard Subcontractor Business Associate Agreement. It will be modified as necessary to remain consistent with Company's obligations to its clients. If a Subcontractor requests Company to sign its form or requests changes to Company's form, the agreement or requested changes will be forwarded to the Privacy Officer for review, approval and negotiation, if necessary. Subcontractor Business Associate Agreements may not be signed without the Privacy Officer's prior approval. Company will perform reasonable and appropriate reviews of its Subcontractors. The scope and frequency of such reviews will vary depending on the nature and extent of PHI being shared with the Subcontractor and may involve surveys, obtaining signed certifications and on-site reviews as deemed appropriate by the Privacy Officer (in coordination with the Security Officer for Subcontractors that access or receive electronic PHI). If a Company workforce member becomes aware of any pattern of activity or practice of a Subcontractor that constitutes a material breach or violation of the agreement with the

Subcontractor, the Company workforce member must promptly notify the Privacy Officer. Company will take reasonable steps to cure the breach or end the violation. If such steps are unsuccessful, Company shall terminate the agreement between the parties.

4. Required Components of Business Associate Agreement or a Subcontractor Business Associate Agreement. A Business Associate Agreement or a Subcontractor Business Associate Agreement (collectively, a "BAA") must contain terms:

a. Requiring Company (or the Subcontractor) to only use or disclose PHI in accordance with the BAA or as required by law. The services and duties of the Subcontractor must either be specified in an underlying service agreement or in the BAA.

b. Requiring Company (or the Subcontractor) to maintain appropriate administrative, technical and physical safeguards to protect the confidentiality of PHI and to comply with the applicable provisions of 45 CFR Part 164, Subpart C of the HIPAA Rules with respect to electronic PHI to prevent any use or disclosure of such information other than as provided by the BAA.

c. Requiring Company (or the Subcontractor), to the extent that Company (or the Subcontractor) is to carry out an obligation of a Covered Entity under the HIPAA Rules, to comply with the requirements of the HIPAA Rules that apply to the Covered Entity in the performance of such obligation.

d. Requiring Company (or the Subcontractor) to report non-permitted uses and disclosures, security incidents and breaches to the client (or in the case of Subcontractors, to Company).

e. Requiring Company (or the Subcontractor) to obligate Subcontractors that create, receive, maintain or transmit PHI on behalf of Company (or the Subcontractor) to agree in writing to be bound by the same restrictions and conditions that apply to Company (or to the Subcontractor) with respect to such PHI.

f. Requiring Company (or the Subcontractor) to make PHI available and to amend PHI to satisfy the patient rights provisions of the HIPAA Rules. If the requested PHI is maintained electronically, Company (or the Subcontractor) must provide a copy of the PHI in the electronic form and format requested by the individual, if it is readily producible, or, if not, in a readable electronic form and format as agreed to by the Covered Entity and the individual.

g. Requiring Company (or the Subcontractor) to document disclosures required to be reported under the accounting obligation and to provide such documentation to the client (or in the case of a Subcontractor, to Company).

h. Requiring Company (or the Subcontractor) to provide access to its internal practices, books and records to HHS for purposes of determining compliance with the HIPAA Rules.

i. Requiring Company (or the Subcontractor) to return or destroy all PHI upon termination of the BAA, if feasible, and to continue to abide by the BAA with respect to any PHI that is infeasible to return or destroy and only use and disclose retained PHI for purposes that make return or destruction infeasible.

j. Authorizing termination of the BAA if Company (or the Subcontractor) violates a material term of the BAA.

k. Setting forth any other items required by the HIPAA Rules, as may be amended from time to time. The BAA may also expressly address other items such as the minimum necessary standard, restrictions on the use or disclosure of PHI for marketing or fundraising, prohibitions on the sale of PHI, a statement that Company (or the Subcontractor) may be subject to the penalty provisions of the HIPAA Rules and a statement that either party may report the other to HHS if the other party breaches and termination is not feasible.

Uses and Disclosures of PHI

1. In General. In compliance with the applicable provisions of this Policy and the terms of the applicable Business Associate Agreement with the client, Company may use and disclose PHI as necessary to provide its services to its clients, as otherwise permitted by the Business Associate Agreement and as required by law.

Any Company workforce member who is not sure whether a contemplated use or disclosure is permissible must consult with the Privacy Officer before making the use or disclosure. Although a use or disclosure may be permissible, in some cases, certain procedures must be followed (See, for example, the minimum necessary requirements set forth in Section 2 below and the verification requirements set forth in Section 10 below). Company will use De-identified Information (instead of PHI) when reasonably practical. In addition, when on-site at a client's location, Company workforce members will also comply with client policies to the extent such policies are provided to Company. Before disclosing any PHI to a Subcontractor of Company, Company must enter into a Subcontractor Business Associate Agreement.

2. Minimum Necessary. When practicable, Company will only use, disclose and request PHI that constitutes a Limited Data Set. A "Limited Data Set" is information that is de-identified, except that the individual's town, city, state and zip code, birth date and other dates may remain. In most cases, using or disclosing only a Limited Data Set will not be practicable. In those cases, Company will only use, disclose and request the minimum amount of PHI necessary to accomplish the permitted use or disclosure of the PHI.

2.1 Each Company workforce member will only use and access the amount of PHI necessary to perform his or her assigned job duties. A list of workforce member job descriptions and the types of PHI to which each position is permitted to access it attached as Exhibit A to these HIPAA Policies.

2.2 For any routine disclosures or requests for PHI made by Company, the Privacy Officer will develop protocols to limit the amount of PHI disclosed or requested to the minimum amount of PHI necessary for the disclosure or request, based on such factors as

(a) the type of PHI to be used, disclosed or requested;

(b) the types of persons who will use the disclosure or who will receive the disclosure or the requests;

(c) the conditions that will apply to the use, disclosure or request; and (d) the purpose for which the PHI will be used, disclosed or requested. The Privacy Officer has determined, after review, that the Company does not currently make any routine requests for PHI.

2.3 For non-routine disclosures and requests made by Company, Company will limit the PHI disclosed or requested to the information reasonably necessary to accomplish the purpose of

the disclosure or request. Company will comply with this standard by considering the following criteria for non-routine requests or disclosures:

(1) what is the purpose of the request or disclosure?

(2) what type of PHI is needed for this purpose?

(3) how important is the need for the PHI (versus De-identified Information)?

(4) are there reasonable alternatives to requesting PHI?

(5) is the request or disclosure limited to the scope of PHI needed for the purpose of the disclosure or request? and

(6) any other relevant factors specific to the request or disclosure.

2.4 Company will not use, disclose or request an entire medical record except when the entire record is specifically justified as the amount reasonably necessary to accomplish the purpose of the use, disclosure or request.

3. Marketing. The use and disclosure of PHI for Marketing (as defined below) is strictly regulated under HIPAA. Company will only use and disclose PHI for Marketing in compliance with the HIPAA Rules and its Business Associate Agreements with clients. The HIPAA Rules prohibit the use or disclosure of PHI for Marketing without an authorization, with exceptions for

(a) face-to-face Marketing to an individual; and

(b) providing a promotional gift of nominal value to an individual. Company may not use or disclose PHI for Marketing unless it has authorizations signed by all affected individuals (see Section 7 below) (or the face-to-face exception or nominal gift exception applies) and the use and/or disclosure is expressly permitted by the Business Associate Agreement with the applicable client(s).

The Company does not anticipate using and disclosing PHI for Marketing. Workforce members who have questions about whether a proposed service for, or arrangement with, a client would involve the use or disclosure of PHI for Marketing must contact the Privacy Officer before proceeding. The Privacy Officer will confirm that the services do not involve Marketing or assist with obtaining required authorizations and confirming the use or disclosure is permitted by the applicable Business Associate Agreement(s).

For purposes of the HIPAA Rules, “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, provided that “marketing” does not include the following:

(a) Communications to provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, 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;

(b) Communications 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, provided that no financial remuneration is received in exchange for making the communication;

(c) Communications 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, provided that no financial remuneration is received in exchange for making the communication; and

(d) Communications 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, provided that no financial remuneration is received in exchange for making the communication. As used this definition of Marketing, the term 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 the treatment of an individual.

4. Administrative Uses and Disclosures. To the extent permitted by Company's Business Associate Agreements with its clients, Company may use and disclose PHI for purposes of Company's management and administration and to carry out its legal responsibilities.

For example, Company may use information that includes PHI when necessary to evaluate its job performance and to make quality improvements. If Company needs to disclose PHI to any third party for purposes of its management and administration or to carry out its legal responsibilities, the disclosure must be required by law or the recipient must agree in writing

(a) to keep the PHI confidential and only use it or further disclose it as required by law or for the purpose for which it was received and

(b) to notify Company of any instances of which it is aware in which the confidentiality of the PHI has been breached. Before disclosing PHI pursuant to this Section 3, the Privacy Officer should be consulted.

The Privacy Officer will confirm that the contemplated disclosure complies with this Policy and is permissible under the applicable Business Associate Agreement(s). Company may disclose PHI as required by a valid subpoena, search warrant or court order under this Section 4 provided that Company may be required to receive additional assurances (such as a qualified protective order) prior to making

the disclosure. Any subpoena, search warrant, court order or other judicial or law enforcement request that appears to require the disclosure of PHI must immediately be forwarded to the Privacy Officer. The Privacy Officer will oversee the response to the request, in consultation with legal counsel and the applicable client as necessary.

5. Sale of PHI. The HIPAA Rules prohibit the sale of PHI without an authorization. Company may not sell PHI unless it has authorizations signed by all affected individuals (see Section 7 below) and the sale of PHI is expressly permitted by the Business Associate Agreement with the applicable client(s).

The "sale of PHI" means a disclosure of PHI by Company where Company receives payment directly or indirectly from or on behalf of the recipient of the PHI in exchange for the PHI. There are certain narrow exceptions to the definition of the "sale of PHI," such as disclosures of PHI for payment collection activities that are permitted as payment disclosures.

For example, the limitations on the sale of PHI would not restrict a Covered Entity from selling accounts receivable (containing PHI) to a collection agency for payment purposes. The limitation on the sale of PHI also does not prohibit Company's clients from paying Company for its services (even if those services involve Company providing the client's PHI to that client). Company does not anticipate engaging in the sale of PHI. Any Company workforce member who is considering a disclosure of PHI that would involve Company receiving compensation in connection with the disclosure or that could otherwise be viewed as a sale of PHI must receive the Privacy Officer's approval in advance.

6. Fundraising Involving PHI. The HIPAA Rules place limitations on the use or disclosure of PHI for fundraising purposes. Company does not anticipate using or disclosing PHI for fundraising purposes. Any Company workforce member who has a question as to whether a particular use or disclosure of PHI would constitute fundraising should consult with, and receive the approval of, the Privacy Officer before making the use or disclosure.

7. Authorizations. The HIPAA Rules permit certain other uses and disclosures of PHI, such as disclosing PHI pursuant to a compliant, written authorization. Because Company is acting as a Business Associate, such uses or disclosures are only permissible if permitted by the applicable Business Associate Agreement(s). Company will only use or disclose PHI pursuant to an authorization if it complies with this Section 7 and the applicable Business Associate Agreement permits the use or disclosure. Any Company workforce member considering whether to use or disclose PHI pursuant to an authorization or who receives an authorization from a third party will consult with the Privacy Officer and obtain the Privacy Officer's approval prior to making the use or disclosure. To be compliant, an authorization must be in writing and contain the following information:

- A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.
- Name or specific identification of the person or persons who can make the requested use or disclosure. ¬ Name or specific identification of the person or persons who may receive the requested use or disclosure.

- A description of each purpose of the requested use or disclosure (if the request was made by the patient and the patient does not wish to give the reason for the request, the authorization may include the words “per patient request” for the description).
- An expiration date or expiration event. (Expiration event must relate to the patient or the purpose of the use or disclosure. May use the statement “end of research study” if the authorization is for research.) If the authorization is for the creation or maintenance of a research database or research repository, no expiration date is needed and the statement “none” can be used.
- Statement of the individual’s rights to revoke authorization in writing, exceptions to the right to revoke and description informing the patient how to revoke the authorization.
- Statement that Company may not condition treatment, payment, enrollment or eligibility for benefits on the authorization (there are exceptions to this but they are unlikely to apply.
- Statement that information used or disclosed may be subject to re-disclosure by the recipient and no longer protected by the HIPAA Rules.
- If the authorization is for Marketing as defined above, a statement regarding any remuneration that Company will receive as a result of the use and/or disclosure of the PHI.
- If the authorization is for the sale of PHI as defined above, the authorization must state that the disclosure of PHI will result in payment to Company.
- The individual’s (or personal representative’s) signature and date signed.
- If signed by a personal representative, a description of the representative’s authority to act on behalf of the individual. An authorization cannot be combined with another type of document or permission, except for certain research purposes.

For example, an authorization for the use or disclosure of PHI for a research study may be combined with an informed consent to participate in the research. In contrast, an authorization for the use or disclosure of PHI cannot be combined with a consent to treatment form or a release of intellectual property rights. An individual can revoke an authorization in writing at any time. If Company has already used or disclosed information in reliance upon the authorization, those uses and disclosures are permissible. Once Company knows of a revocation it must take appropriate action to stop any further uses or disclosures pursuant to the authorization.

All signed authorizations and revocations of authorizations must be retained for at least six years. All signed authorizations (or copies of signed authorizations) must be forwarded to the Privacy Officer who will oversee their retention for the required time period. If the authorization was requested for Company’s own use (which is unlikely to be the case given Company’s status as a Business Associate), the individual must be provided with a copy of the signed authorization.

8. Uses and Disclosures of Genetic Information.

8.1 The Genetic Information Nondiscrimination Act of 2008 ("GINA") regulates health plans and employers but does not currently regulate health providers such as hospitals or physicians. GINA and the HIPAA Rules generally prohibit employers, health plans and related entities from:

(a) requesting or requiring Genetic Information of an individual or an individual's family members;

(b) adjusting premium or contribution amounts on the basis of Genetic Information; or

(c) requesting or requiring Genetic Information for underwriting purposes. "Underwriting purposes" includes making decisions regarding eligibility for benefits, preexisting conditions and computing premiums or contribution amounts. GINA generally prohibits employers from using Genetic Information for hiring, firing, or promotion decisions, and for any decisions regarding terms of employment. Employers are required to keep Genetic Information in a confidential medical file separate from personnel files. Employers are responsible for determining what information they provide to Company and for complying with their obligations to protect Genetic Information. To the extent Company stores Genetic Information for its clients, Company will keep Genetic Information secure consistent with these HIPAA Policies. Its clients are responsible for determining how Genetic Information is used and assuring that they file Genetic Information separately from other employer information.

8.2 Many states have also enacted laws to protect the confidentiality of Genetic Information. The majority of these require individual patient consent in order to perform a genetic test or to obtain Genetic Information and require the individual's consent to disclose Genetic Information. Company will comply with such laws to the extent applicable. The Company does not anticipate using, disclosing or receiving Genetic Information.

9. Other Uses and Disclosures. The HIPAA Rules permit certain other uses and disclosures of PHI, such as disclosing PHI to a public health authority or certain disclosures to law enforcement. Because Company is acting as a Business Associate, such uses or disclosures are only permissible if permitted by the applicable Business Associate Agreement(s).

Any Company workforce member who needs or desires to use or disclose PHI for a purpose not specifically permitted by this Policy must consult with, and receive the approval of, the Privacy Officer before making the use or disclosure. The Privacy Officer will review the request to determine whether it is permissible by the applicable Business Associate Agreement(s) and the HIPAA Rules.

10. Verification.

10.1 Verification is the process of confirming the identity and authority of any person who requests PHI and of obtaining any required documentation regarding that request. Before releasing PHI, Company must verify the identity of any person unknown to Company who

requests PHI and the authority of any person known or unknown to Company to have access to PHI (as well as confirming that the disclosure is permitted by Sections 1 through 9 of this Policy). As part of its obligation to verify a person's authority, Company must also obtain any documentation required for release of PHI from the person requesting the PHI (such as a copy of a court order when a requestor claims disclosure is required pursuant to an order). Company may rely on documentation, statements, or representations that, on their face, meet the applicable requirements for disclosure, if Company's reliance is reasonable under the circumstances and is in good faith.

10.2 The obligation to verify identity and authority does not apply if the person requesting the PHI and their authority to receive the PHI is known to Company (for example, when the PHI belongs to Client A, and the requestor is an individual known by Company to work at Client A). This Policy also does not apply if the disclosure meets certain other exceptions determined to apply by the Privacy Officer in consultation with legal counsel (the HIPAA Rules recognize certain exceptions unlikely to apply to Company given its status as a Business Associate and the types of services it provides).

10.3 If Company cannot verify a person's identity and authority to access PHI, Company will not disclose the PHI.

10.4 If the person requesting PHI claims to be a public official or to be acting on behalf of a public official, Company may rely on the following to verify the person's identity, if such reliance is reasonable:

(1) if the request is in person, presentation of an agency identification badge, other official credentials, or other proof of government status;

(2) if the request is in writing, the request is on appropriate government letterhead; or

(3) 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. Company will also request evidence of authority of the public official to access PHI.

If it is reasonable to do so under the circumstances, Company may rely on the following to verify the authority of a public official or a person acting on behalf of a public official:

(1) a written statement of the legal authority under which the information is requested or, if a written statement of legal authority would be impracticable (such as an emergency), an oral statement of such legal authority; or

(2) if the request is made pursuant to a legal process, warrant, subpoena, order or other legal process issued by a grand jury or a judicial or administrative tribunal, it is presumed to constitute legal authority.

11. Recording Certain Disclosures. If Company is aware of any disclosure that is not permitted by this Policy, Company will log the disclosure and notify the affected client(s) as described in Privacy and Security Incidents and Complaints. Any Company workforce member who is aware of a non-permitted disclosure must notify the Privacy Officer immediately. The Privacy Officer will take further appropriate action as described in these HIPAA Policies.

12. Uses and Disclosures Not Addressed by this Policy. Uses and disclosures not authorized by this Policy are not permissible.

Safeguards

1. In General. Company will maintain appropriate administrative, technical and physical safeguards to protect the confidentiality, integrity and accessibility of PHI consistent with the requirements of these HIPAA Policies and to safeguard PHI from intentional and unintentional non-permissible uses and disclosures. These safeguards will supplement and be consistent with security measures taken by Company for electronic PHI.

2. General Safeguards. Company safeguards will include the following:

a. Company will restrict access to client files containing PHI to only workforce members of Company, the client and authorized Subcontractors of Company.

b. Company will store files containing PHI in a covered location (i.e., such as a file folder).

c. Company will store files containing PHI in a secure location when not in use (i.e., locked room or file cabinet).

d. Company will use reasonable safeguards so that PHI on computer screens will not be visible to unauthorized persons, including locking down computer workstations when not in use or when leaving the workstation by activating a password protected screen saver and clearing PHI from the computer screen when the PHI is not actually being used.

e. Company will keep firewalls in place to protect electronic PHI.

f. Company will keep a Virtual Private Network (VPN) in place to protect electronic PHI.

g. Prior to discarding PHI, Company will securely destroy PHI by, among other things, shredding documents or destroying hardware that contain PHI so that they cannot be read or reconstructed. PHI stored on digital copiers or other devices must be removed or destroyed before the device is resold, returned at the end of the lease or otherwise no longer under the control of Company. Locked shred bins are located on each floor of Company's offices.

h. Company will not hold phone conversations or other discussions involving PHI in areas where unauthorized persons may overhear. Phone conversations involving PHI should not be held on speaker phone, unless everyone within listening distance is an authorized recipient of the PHI.

i. Company will limit the amount of PHI disclosed when leaving a message on an answering machine or otherwise to as little PHI as possible.

j. Prior to sending, Company will mark documents containing PHI that are delivered by mail or hand delivery as "confidential."

3. Facsimile Safeguards. Company generally does not send PHI by fax, and Company's services should not involve exchanging PHI by fax. Company will not request or encourage customers or third parties to

send PHI to Company by fax. In the event Company receives an incoming fax containing PHI, Company will pick up incoming faxes in a timely manner. Any fax machines will be located in secure areas not accessible to the general public or unauthorized staff. If Company does choose to send PHI by fax,

Company will take reasonable steps to send and receive facsimile transmissions securely, including the following safeguards:

a. Only sending PHI by fax when mail, encrypted e-mail or hand delivery are not feasible.

b. Notifying the recipient and double checking fax numbers before dialing.

c. Using the Company standardized fax cover sheet that includes a confidentiality statement and a request that any erroneous recipient destroy or return the fax.

d. Picking up incoming faxes from the fax machine in a timely manner.

e. When sending a fax, remaining at the fax machine until the fax has been scanned completely and not using a fax machine that is accessible to the public.

f. Not leaving faxes to be sent or that have been sent at the fax machine unattended.

g. If aware of a misdirected fax, contacting the recipient and asking them to discard the misdirected fax (and reporting the incident immediately to the Privacy Officer).

h. Locating fax machines in secure areas not accessible to the general public or unauthorized staff.

4. E-mail Safeguards. The minimum necessary PHI will be sent via e-mail. Any PHI transmitted by email will be protected by encryption (secure email) to prevent inadvertent disclosure. An e-mail signature block will be appended to all external recipients stating the confidentiality of the information and what to do if it is received inadvertently.

Any Company workforce member who becomes aware of a misdirected e-mail that contains PHI must notify the Privacy Officer immediately. The e-mail system and all messages generated or handled by e-mail, including backup copies, are property of Company. E-mail users have no right to privacy in their use of the computer system, including e-mail. Company may monitor the content and usage of the computer system, including e-mail, at any time and for any reason.

5. Authorizing Access to PHI. Company will take reasonable measures to authorize appropriate access to PHI. Before granting access to Company systems containing PHI to a workforce member, Company will perform a criminal background check of such workforce member and evaluate the results to ensure that the workforce member would not pose a risk to the privacy and security of PHI. Such background checks should be performed upon initial hire.

For new workforce members, the Privacy Officer or the applicable supervisor will determine the appropriate level of access in compliance with the section referenced in Uses and Disclosures of PHI above. If the workforce member's position is not addressed, the Privacy Officer will determine the level of access in coordination with the supervisor and update.

For new Subcontractors, the Privacy Officer and Security Officer must be notified of any Subcontractor requiring access to Company's facilities or information systems to ensure that only appropriate access is permitted consistent with the Company's Information Access Authorization & Authentication Security and Physical Security plans.

Recording & Accounting of Disclosures of PHI

1. In General. Subject to certain exceptions, the HIPAA Rules give individuals the right to receive an accounting of disclosures of PHI that has been used or disclosed by a Covered Entity or a Business Associate. As described below, Company must record certain disclosures made by Company and provide such recorded information to the applicable client upon request.

2. Disclosures Required to be Recorded. Company will maintain a record of disclosures of PHI for the following reasons:

a. Disclosures required by law;

b. Disclosures made to public health agencies;

c. Disclosures made for purposes of health oversight activities (disclosures to agencies and their workforce members that are authorized to oversee the health care system, government programs that use health information to determine eligibility or compliance or to enforce civil rights laws for which health information is relevant);

d. Disclosures in judicial and administrative proceedings;

e. Disclosures to law enforcement;

f. Disclosures necessary to comply with laws relating to worker's compensation programs (not including disclosures related to payment);

g. Non-permissible disclosures of PHI by Company that are known to Company.

h. Note: The above list of recordable disclosures does not mean these disclosures should be made. Any disclosure of PHI must comply with HIPAA Privacy Uses and Disclosures of PHI and the applicable Business Associate Agreement. In addition to the types of disclosures required to be included in an accounting, once HHS issues regulations, Company will be required to record disclosures made by Company from an electronic health record (and potentially other electronic PHI) for purposes of providing services to clients or for purposes of Company's management and administration. These HIPAA Policies will be modified to address this requirement when the final rules are published.

3. Information Required to be Recorded. For any disclosures that must be recorded pursuant to this Policy, Company will record the following information:

a. The date of the disclosure;

b. The name of the entity or person who received the PHI and, if known, the address of such entity or person;

c. A brief description of the PHI disclosed; and,

d. 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 copy of a written request for a disclosure.

4. Disclosure Log. The Privacy Officer will maintain a log to document disclosures required for an accounting as required by this Policy.

5. Provision of the Accounting Information to the Client. Upon request of the client, Company will provide the client with the accounting information recorded pursuant to this Policy in compliance with the terms of the applicable Business Associate Agreement. Information will be made available for 6 years prior to the date of the request, except that Company need not provide accounting information for any disclosures made before the effective date of the service agreement with the client. After final regulations are issued, disclosures of PHI from an electronic health record (and potentially other electronic PHI) need only be provided for 3 years from the date of the request (this provision is subject to clarification, including what constitutes an electronic health record, when implementing regulations are published).

6. Requests Received from an Individual. If Company receives a request directly from an individual for an accounting, the Privacy Officer will forward the request to the applicable client and coordinate its response with the client, subject to the terms of the applicable Business Associate Agreement. Any Company workforce member who receives a request for an accounting from an individual or a client must forward the request immediately to the Privacy Officer to handle in compliance with this Policy.

7. Other Documentation. Company will document and retain the following for a period of at least 6 years, or from the date of its creation or the date when it last was in effect, whichever is later:

a. Information required to be documented pursuant to this Policy;

b. Copies of any accounting information provided to the client (or directly to the individual if requested by the client); and

c. The title of the persons or officer responsible for receiving and processing requests for an accounting: the Privacy Officer.

8. Privacy Officer. The Privacy Officer or his/her designee is responsible for responding to a request from a client for an accounting of disclosures made by Company.

Access, Amendment & Other Individual Rights

1. Access and Amendment Requests. Company receives PHI from clients that may be subject to the HIPAA Rules requirements regarding access to PHI in a Designated Record Set by individuals and amendment of PHI. Any Company workforce member who receives a request from an individual or a client to amend or receive access to PHI must forward the request to the Privacy Officer immediately. The Privacy Officer will forward any access or amendment requests to the applicable client and coordinate any response to the request with the client in accordance with terms of the applicable Business Associate Agreement.

The Privacy Officer will oversee implementing any request from a client to provide PHI in response to an individual's access request or to amend PHI held by Company. In the event of a request for access to PHI that is maintained in a Designated Record Set by Company, if the requested PHI is maintained electronically, Company must provide a copy of the PHI in the electronic form and format requested by the individual, if it is readily producible, or, if not, in a readable electronic form and format as agreed to by the client and the individual.

2. Restriction Requests. Covered Entities may grant certain requests from individuals to restrict how PHI is used or disclosed. Covered Entities may deny such requests, except for requests not to disclose PHI to a health plan for purposes of payment or health care operations if the PHI solely relates to an item or service for which the individual paid in full (provided the disclosure is not required by law). If a client notifies Company of a restriction request that would restrict a use or disclosure otherwise permitted by the applicable Business Associate Agreement, Company will comply with the terms of the restriction request.

The Privacy Officer will take appropriate steps to implement the restriction request. Any Company workforce member who receives a request from an individual or a client to restrict use or disclosure of PHI must forward the request to the Privacy Officer immediately. The Privacy Officer will forward any restriction requests to the applicable client and coordinate any response to the request with the client in accordance with terms of the applicable Business Associate Agreement.

3. Other Individual Rights Requests. If Company receives any client requests that relate to other individual rights under the HIPAA Rules that impact Company's operations, the Privacy Officer will oversee implementing such requests. If Company receives any requests directly from individuals that relate to other individual rights under the HIPAA Rules (such as a request for the client's privacy notice or a request for confidential communications), the request will be forwarded to the Privacy Officer immediately. The Privacy Officer will forward any such requests to the applicable client, coordinate any further response by Company to the request with the client, and take steps reasonable and appropriate to implement a request when instructed to do so by the client.

Privacy & Security Incidents & Complaints

1. In General. Any Company workforce member who knows of, suspects, or has received a report from any individual, client or Company workforce member of a violation of these HIPAA Policies, including any non-permitted use or disclosure of PHI, must notify the Privacy Officer immediately. Security Incidents must be reported to the Security Officer as set forth in the Incident Response Security Policy. When in doubt on who must receive the report, the Company workforce member should report the potential violation to the Privacy Officer who will coordinate with the Security Officer. The Privacy Officer will oversee the review of and response to any potential violation of these HIPAA Policies, including complaints from individuals or clients.

2. No Waiver or Retaliation. Company will not require individuals to waive their rights under the HIPAA Rules or their rights to file complaints regarding compliance with the HIPAA Rules. Company will not intimidate, threaten, coerce or engage in any other form of retaliation against a person who exercises any rights under the HIPAA Rules, reports an incident or complaint under this Policy, who reports an incident to HHS or who assists in any HHS proceeding or compliance review regarding the HIPAA Rules. Any manager, supervisor or workforce member who engages in any form of retaliation is subject to discipline up to and including dismissal. If any workforce member reports a concern regarding the workforce member's own inappropriate or inadequate actions, the report does not exempt the workforce member from the consequences of those actions. However, prompt and forthright disclosure of an error by a workforce member will be considered a positive constructive action.

3. Investigation and Mitigation. The Privacy Officer will oversee the prompt and appropriate investigation and resolution of any incidents or complaints reported under this Policy. The Privacy Officer will take reasonable and appropriate actions to mitigate any harm caused by any violations of the HIPAA Rules or these HIPAA Policies by Company. Appropriate mitigation steps will depend on the facts of the particular incident. Examples of mitigation steps include:

(a) reporting a theft to the police;

(b) requesting the recipient to return or destroy the PHI and certify in writing that the PHI and all copies of the PHI has been returned or destroyed;

(c) deleting misdirected emails containing PHI;

(d) changing passwords or other means of accessing systems or devices containing PHI;

(e) adopting additional safeguards;

(f) revising existing or adopting new policies and procedures;

(g) providing additional training to affected workforce members; and

(h) terminating a relationship with a Subcontractor.

4. Notification to the Client. If Company determines that a non-permitted use or disclosure has occurred, the Privacy Officer will notify the affected client(s) in compliance with the applicable Business Associate Agreement(s). Security Incidents must also be reported to the affected client(s) consistent with the Incident Response Security Policy.

5. Other Policies or Required Actions. Company will also take appropriate action under other applicable policies in response to any incident or complaint that is determined to constitute a violation of these HIPAA Policies, including the following Policies, as applicable: Recording and Accounting of Disclosures of PHI, Breach Notification, Workforce Member Training Regarding the Privacy and Security of PHI, and Sanctions.

6. Maintain Documentation. The Privacy Officer will document each reported incident and complaint and its resolution, including mitigating actions taken by Company. This documentation will be maintained for 6 years from the date of its creation in compliance with the Record Retention Policy.

Breach Notification

1. In General. Company will report Breaches to the client(s) affected by the Breach without unreasonable delay but no longer than 60 days from discovering a Breach (or such shorter period specified by the applicable Business Associate Agreement). A Breach is treated as "discovered" by Company on the first day the Breach is known, or would have been known with reasonable diligence, by any person (other than the person committing the Breach) who is a workforce member, officer or agent of Company. All Company workforce members, officers and agents must report any incidents believed to be Breaches or non-permissible uses or disclosures of PHI to the Privacy Officer as soon as possible.

The Privacy Officer will review all incident reports received from workforce members, agents, Subcontractors or others promptly to determine:

(1) whether the reported use or disclosure was permissible under the HIPAA Rules and the applicable Business Associate Agreement(s);

(2) if not, whether the incident constitutes a Breach (see below); and

(3) whether the incident must otherwise be reported to the client(s) and/or other third parties due to a Business Associate Agreement obligation (to report uses, disclosures or Security Incidents even if they are not considered Breaches, any other contractual obligation or any other applicable law. If an incident requires a report, the Privacy Officer will make the required reports to the affected client(s) and/ or other third parties consistent with this Policy and any other applicable Policy.

2. Determining Whether an Incident is a Breach. Incidents that fall into one of the following categories are not Breaches and, thus, are not required to be reported pursuant to this Policy (unless state law requires a report– See Section 4 below; also the incident may still require a report under another Policy. Workforce members, officers and agents of Company must always report any incident believed to be a violation of these HIPAA Policies to the Privacy Officer so that the Privacy Officer can determine whether the incident is a Breach and whether corrective actions or other measures should be taken in response to the incident.

Breach Exceptions. If any of the following exceptions apply, the incident is not a Breach and is not required to be reported under this Policy (unless Section 4 below applies):

a. Certain unintentional uses. Any unintentional acquisition, access, or use of PHI by Company or any individual acting under the authority of Company if

(a) the acquisition, access, or use was made in good faith and within the scope of authority; and

(b) the information is not further used or disclosed in a manner not permitted by the HIPAA Rules.

b. Certain inadvertent disclosures. Any inadvertent disclosure by a person who is authorized to access PHI at Company or a subcontractor of Company if the information received as a result of the disclosure is not further used or disclosed in a manner not permitted by the HIPAA Rules.

c. Incidents involving no ability to retain the PHI. A disclosure of PHI where Company or its subcontractor has a good faith belief that the recipient would not reasonably have been able to retain the information (such as an envelope that is incorrectly addressed and is returned unopened as undeliverable by the U.S. Post Office). Low probability that the information has been compromised.

Except for the categories listed above, an acquisition, access, use, or disclosure of PHI in a manner not permitted by the HIPAA Rules is presumed to be a Breach unless Company can demonstrate that there is a low probability that the PHI has been compromised. In order to make this determination, the Privacy Officer will perform, and document the outcome of, a risk assessment taking into account the following factors:

a. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of reidentification;

b. The unauthorized person who used the PHI or to whom the disclosure was made;

c. Whether the PHI was actually acquired or viewed; and

d. The extent to which the risk to the PHI has been mitigated. 3. Content of Notice. The notification to the client will include, to the extent possible, the following information:

(a) names of each individual whose PHI was or is reasonably believed to have been affected by the Breach; and

(b) any other available information to assist the client with meeting its obligation to notify individuals (i.e., a description of the Breach, the date of the Breach, a list of individuals affected by the Breach, a description of the types of Unsecured PHI involved, and a description of actions being taken to mitigate harm and prevent further Breaches).

4. Other Notice. Even if an incident is determined to not be a Breach, Company will report any incident that constitutes a non-permitted use, disclosure or Security Incident to the affected client(s) as specified in the applicable Business Associate Agreement(s). Clients may also perform their own Breach analysis. Company will comply with any applicable state law requirements that impose additional breach notification duties or more restrictive breach obligations (such state laws may apply to personal information that is not considered to be PHI).

5. Subcontractors. Company will require its Subcontractors to report Breaches to Company consistent with this Policy.

6. Law Enforcement Delay. Company must delay notification to affected clients of a Breach if a law enforcement official states that notification would impede a criminal investigation or cause damage to national security as follows:

(a) if the law enforcement statement is in writing, Company will delay the notification or posting for the time period specified in the statement; or

(b) if the law enforcement statement is made orally, Company will delay the notification or posting for the time period requested or for 30 days, whichever time period is shorter. If the law enforcement official confirms an oral statement with a written request to delay notification or posting, Company will delay the notification or posting for the time period specified in the written statement.

7. Other Policies. Consistent with HIPAA Policies (Privacy & Security Incidents & Complaints, Workforce Member Training Regarding Privacy & Security of PHI and Sanctions), Company will:

(a) train its workforce members on this Policy;

(b) accept complaints from individuals concerning its compliance with this Policy;

(c) implement sanctions for violations of this Policy;

(d) refrain from intimidating, threatening, coercing, discriminating against, or taking other retaliatory action against any individual for exercising his or her rights under this Policy or any other aspect of the HIPAA Rules; and

(e) not require individuals to waive their rights under this Policy. 8. Documentation. Company will document risk assessments performed pursuant to this Policy, incident reports, Breach notifications provided to clients and any other third party, and other documentation created pursuant to this Policy for at least 6 years from the date the documentation was created or was last in effect, whichever is later, in compliance with the Record Retention Policy.

Workforce Member Training Regarding the Privacy & Security of PHI

1. In General. All Company workforce members will receive appropriate training regarding these HIPAA Policies and the privacy and security of PHI. Workforce members will be trained promptly upon initial employment with Company and on an as needed basis, including as necessary to address changes to these HIPAA Policies and to improve compliance.

2. Privacy Officer. The Privacy Officer will oversee compliance with this Policy.

3. Documentation. The Privacy Officer will maintain a record of all training materials/sessions regarding these HIPAA Policies and the privacy and security of PHI, including documentation of attendance for 6 years in compliance with the Record Retention Policy.

4. Security Awareness and Reminders. The Security Officer will provide regular security training and security awareness reminders to Company workforce members, including information on protecting Company systems from malicious software, monitoring of log-in activities and password management. Company workforce members will receive additional training in the event of environmental, operational or legal changes that affect electronic PHI, including revised or new security policies, new or upgraded equipment or software, new security technology and new legal developments, such as changes to the security provisions of the HIPAA Rules. Company will maintain a record of all training materials and sessions regarding these HIPAA Policies, including documentation of attendance, for 6 years in compliance with the Record Retention Policy.

Record Retention

1. In General. Company will maintain all documentation required to be made under these HIPAA Policies for 6 years from the date of its creation or from the date it was last in effect, whichever is later. The Privacy Officer is responsible for overseeing compliance with this documentation requirement.

2. Examples of Required Documentation. The following are examples of documentation that must be retained as specified in this Policy:

a. Signed Business Associate Agreements;

b. Signed Subcontractor Business Associate Agreements;

c. Disclosures required to be recorded under Recoding & Accounting of Disclosers of PHI;

d. Incidents or complaints and their resolution;

e. Risk assessments and breach reports created under Breach Notification Policy;

f. Training materials and documentation of the provision of workforce member training;

g. These HIPAA Policies (each version that is adopted).

3. Retention of PHI. PHI may not be maintained beyond the term of the underlying service agreement unless return or destruction of the PHI is infeasible (such as to support work that was done under the service agreement), in compliance with the terms of the applicable Business Associate Agreement. Any PHI that is retained following termination of a service agreement may only be used or disclosed for the reasons that make return or destruction infeasible and in compliance with the terms of the Business Associate Agreement at the time of termination of the underlying service agreement.

4. Availability. Documentation created pursuant to these Policies will be available to appropriate Company workforce members who need the documentation to perform their assigned duties. Copies of these Policies are available to all Company workforce members.

5. Revision/Updates. These HIPAA Policies will be revised as necessary to comply with changes in the HIPAA Rules and applicable guidance. Company may revise these HIPAA Policies as necessary to improve compliance and as part of its mitigation efforts. Company will provide training to affected workforce members in the event of material changes to these HIPAA Policies.

Sanctions

1. In General. All Company workforce members must comply with the policies and procedures of Company including these HIPAA Policies. Company will apply appropriate sanctions against workforce members who fail to comply with these HIPAA Policies.

2. Disciplinary Actions. The Privacy Officer, in conjunction with legal counsel and Human Resources, will review all reports of non-compliance and determine the severity of disciplinary actions necessary. Disciplinary actions may range from a verbal warning to termination and may include additional training, counseling, formal reprimand, reassignment, suspension or other measures consistent with Company's Human Resources policies. Factors that will impact the disciplinary action adopted include

(a) whether the non-compliance was accidental, intentional, and/or malicious;

(b) the scope of the violation, including the amount and types of PHI involved;

(c) whether the individual has previous instances of noncompliance; and

(d) whether the individual attempted to cover-up the violation, was forthcoming or tried to undermine the Privacy Officer's investigation. The unauthorized use or disclosure of PHI may also result in monetary penalties under HIPAA or other civil or criminal penalties.

3. Documentation. All sanctioning activities will be documented and retained by the Privacy Officer for a period of at least 6 years from the date of its creation or the date when it was last in effect, whichever is later in compliance with the Record Retention Policy.

4. Reports. Workforce members who become aware of a potential violation of these HIPAA Policies must report the incident as set forth in the Privacy Incidents and Complaints Policy. If the Privacy Officer is the subject of the incident report, the workforce member should report the incident to Human Resources or a member of upper management of Company simultaneously.

5. Exceptions. Company will not apply disciplinary action to the extent the use or disclosure of PHI involves one of the following:

5.1 A whistle-blower disclosure made in good faith to a health oversight agency or public health authority with respect to Company's conduct or compliance with the law or to an attorney being retained to represent the person making the disclosure for purposes of determining the legal options of the whistleblower;

5.2 A limited disclosure by a victim of a crime to a law enforcement official, where the disclosure is about the suspected perpetrator of the criminal act and the information disclosed is limited to the information that may be disclosed to a law enforcement official under the HIPAA Rules;

5.3 Filing a complaint with Company and/or HHS;

5.4 Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing concerning the HIPAA Rules;

5.5 Opposing any act or practice that is prohibited by the HIPAA Rules, provided that

(i) the person has a good faith belief that the practice being opposed is unlawful; and

(ii) the manner of opposition is reasonable and does not itself violate the HIPAA Rules.

PRIVACY POLICY ADDENDUM Mobile Applications and User Rights

Effective Date: May 20, 2026 Document Reference: PPOD2-052026-MOBILE

This addendum supplements the Business Data Applications, Inc. ("Company") Privacy Policy (Document Reference PPOD2-012020) and addresses data-handling practices specific to the Healthy Contracts mobile applications (the "Mobile Apps"). The base Privacy Policy continues to govern Protected Health Information ("PHI") handling as required under HIPAA. This addendum addresses additional categories of information processed by the Mobile Apps and the rights of Mobile App end users with respect to that information.

1. Mobile Applications Covered

This addendum applies to the following Mobile Apps published by Business Data Applications, Inc., including white-labeled deployments for client organizations:

- Healthy Contracts Timesheets (iOS, Android)
- Healthy Contracts Timecards (iOS, Android)

2. Information the Mobile Apps Collect

The Mobile Apps collect and process only the information necessary to provide time-entry, submission-review, and proxy-authorization features:

- Identity information: email address, name, organization affiliation, and role, as provisioned by the client organization. The Mobile Apps do not enroll users directly; user accounts are created by client administrators.
- Authentication credentials: access tokens and refresh tokens issued by Amazon Web Services Cognito for the duration of an active session. Tokens are stored on the device using platform-provided secure storage (iOS Keychain, Android Keystore).
- User-entered work data: time entries, hour counts, contract references, comments, and submission status. This information is transmitted to the client organization's data tier and is retained according to the client's record-retention policy.
- Device information: the Mobile Apps record only the device model and operating-system version sufficient to diagnose technical issues. They do not collect device advertising identifiers, precise or coarse geolocation, browsing history, contacts, calendar entries, photos, microphone audio, or camera images.

3. Information the Mobile Apps Do Not Collect

For clarity, the Mobile Apps do not:

- Use third-party advertising software development kits
- Use third-party analytics software development kits (including Google Analytics, Firebase Analytics, Mixpanel, Amplitude, or similar)
- Track users across other applications or websites
- Share user information with data brokers
- Sell user information

4. How Information Is Used

Information collected by the Mobile Apps is used solely to:

- Authenticate the user against the client organization's authorized user directory
- Submit and retrieve work-hour records on behalf of the user
- Notify the user of the status of their submissions
- Enable authorized proxies to log time on behalf of designated principals
- Diagnose and repair technical issues with the Mobile Apps

5. Data Storage and Transmission

- In transit: all communications between the Mobile Apps and Company servers occur over Transport Layer Security (TLS) version 1.2 or higher.
- At rest on the device: authentication tokens are stored in platform secure storage. PHI is not cached on the device beyond the current session.
- At rest on Company infrastructure: information is stored in Amazon Web Services within the United States. Access is governed by the HIPAA Policies described in the base Privacy Policy.

6. Your Rights

If you are an end user of a Mobile App, you have the following rights with respect to information the Mobile Apps collect about you.

6.1 Right to Access Your Information

You have the right to receive a copy of the personal information the Mobile Apps hold about you. To make a request, contact your client organization administrator or the Company Privacy Officer using the contact information in Section 9 below.

6.2 Right to Delete Your Account

You have the right to request deletion of your account and the personal information associated with it, subject to legal and regulatory retention obligations.

The Mobile Apps provide an in-app account-deletion feature. To use it:

1. Open the Mobile App and sign in.
2. Open the user menu and select "Settings."
3. Select "Delete My Account."
4. Confirm the deletion when prompted.

When you delete your account through the Mobile App, the following occurs:

- Your authentication credentials are disabled within minutes.
- Your user record is marked for deletion.
- Your historical time entries and submissions are retained as required by the client organization's record-retention policy and applicable law; they are no longer associated with an active user account but may remain in audit logs.
- You are signed out of the Mobile App and your local data is cleared from the device.

If you are unable to access the in-app feature, you may also request account deletion by emailing the Company Privacy Officer at info@businessdataapps.com.

6.3 Right to Correct Your Information

You have the right to request correction of inaccurate information. Corrections to identity information are typically made by your client organization administrator. Corrections to time-entry data are made through the Mobile App's standard editing workflow before submission, or by contacting your reviewer for re-routing after submission.

6.4 Right to Know

You have the right to know what personal information has been collected about you, the categories of sources, the business purposes for collection, and the categories of third parties (if any) with whom

information has been shared. The Mobile Apps share information only with the client organization that provisioned your account and with Company subcontractors operating under written Business Associate Agreements as required by HIPAA.

7. Children's Privacy

The Mobile Apps are intended for use by healthcare workforce personnel and are not directed to children under the age of thirteen (13). The Mobile Apps do not knowingly collect personal information from children under 13.

8. Changes to This Addendum

The Company may update this addendum from time to time. The effective date at the top of this document indicates the most recent revision. Material changes will be communicated through the Mobile Apps or through the client organization.

9. Contact

For privacy questions, access requests, deletion requests, or to report a concern:

Privacy Officer
Business Data Applications, Inc.
24 Front Street, Exeter, New Hampshire 03833
(877) 821-5393
info@businessdataapps.com