Creative Data Technologies, Inc.

2474 Pale Tiger Ct., Tallahassee, FL 32309
Phone: (850) 264-9065 http://www.creativedatatech.com

PSCS USER AGREEMENT FOR DATAVAULT™ SYSTEM

Please provide the following information to obtain account(s) on the DataVault System:

Facility Name _____

AHCA Facility ID _____ FEIN _____

Physical Address _____

City, State, Zip+4 _____

Mailing Address _____

City, State, Zip+4 _____

Facility Administrator's Name _____ _____
First Last

Facility Administrator's Phone (____) ____ - _____ Email Address _____

User 1 Name _____ _____ Phone (____) ____ - _____
First Last
Email Address _____

User 2 Name _____ _____ Phone (____) ____ - _____
First Last
Email Address _____

User 3 Name _____ _____ Phone (____) ____ - _____
First Last
Email Address _____

User 4 Name _____ _____ Phone (____) ____ - _____
First Last
Email Address _____

User 5 Name _____ _____ Phone (____) ____ - _____
First Last
Email Address _____

TERMS OF USER AGREEMENT

1. Facility Administrator must review & return signed attached HIPAA Business Associate Agreement.
2. Facility Administrator acknowledges receipt of DataVault User's Manual, including instructions on proper usage of system and instructions to back up data records.
3. Facility Administrator accepts full responsibility for performing regular backups of data records, and will hold Creative Data Technologies, Inc. harmless for any loss or corruption of data records, or periods of unavailability of DataVault system for whatever reason. Creative Data Technologies will perform due diligence to keep the system up and running 24/7, and recover as soon as possible from any unforeseen system failures.
4. Facility Administrator is aware and agrees that a separate customer account must be acquired for each separately registered Facility. Excessive transactional volume detected by a single facility deemed to be in significant excess of a typical 2 or 3 bed facility will be subject to additional subscription usage fees.

Signed _____ _____
Facility Administrator / Owner Date

Printed Name _____

Authorized Representative of _____ (facility name)

Signed _____ _____
Creative Data Technologies Rep. Date

Printed Name _____

Notice: Please email the signed agreement to smckennasr@gmail.com. We will sign and email you back an executed copy of the document(s).

HIPAA BUSINESS ASSOCIATE AGREEMENT

THIS AGREEMENT is made and entered into this day, _____ by and between Creative Consulting Co.

(COVERED ENTITY) and _____(BUSINESS ASSOCIATE).

RECITALS

WHEREAS, the Parties enter into this Agreement for the purposes of complying with the privacy, security and breach notification laws at 45 CFR Parts 160 and 164 under the Health Insurance Portability and Accountability Act of 1996, and regulations issued thereunder by the United States Department of Health and Human Services, as amended from time to time, and including as amended by Subtitle D of the Health Information Technology for Economic and Clinical Health Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (the "HITECH Act"), and its implementing regulations, as amended from time to time (these statutes and regulations are hereinafter collectively referred to as "HIPAA");

WHEREAS, Covered Entity possesses Individually Identifiable Health Information that is protected under HIPAA and is permitted to use and disclose such information only in accordance with such laws and regulations;

WHEREAS, Covered Entity has engaged Business Associate to provide certain services that will require or allow Business Associate to create, receive, maintain, access, use or transmit Protected Health Information on Covered Entity's behalf, including Electronic Protected Health Information, that is subject to protection under the Privacy and Security laws and regulations of HIPAA, and applicable guidance;

WHEREAS, HIPAA obligates Covered Entity to enter into a contract with Business Associate to ensure that Business Associate appropriately safeguards such information; and

NOW THEREFORE, for and in consideration of the recitals above, the benefits to Business Associate under the Underlying Agreement and the mutual covenants and conditions herein contained, Covered Entity and Business Associate agree to enter into this Agreement in order to provide a full statement of their respective responsibilities.

ARTICLE I – DEFINITIONS

Unless otherwise defined herein or in the recitals hereto, capitalized terms shall have the same meaning as ascribed to them in HIPAA. Although PHI and Protected Health Information will have the same meaning as defined by 45 C.F.R. § 160.103, the PHI referenced is limited to the PHI that Business Associate creates, receives, maintains, uses or transmits on behalf of Covered Entity. "HIPAA Privacy Rule" shall mean the regulations as set forth in 45 CFR Parts 160 and 164 Subparts A and E. "HIPAA Security Rule" shall mean the regulations as set forth in 45 CFR Parts 160 and 164, Subparts A and C. "HIPAA Breach Notification Rule" shall mean the regulations as set forth in 45 CFR Parts A and D.

ARTICLE II - PERMITTED USES AND DISCLOSURES OF PHI BY BUSINESS ASSOCIATE

2.1 **Access, Use or Disclosure to Provide Services.** Business Associate may access, use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in the Underlying Agreement, provided that such use or disclosure would not violate HIPAA if done by Covered Entity. Business Associate may provide data aggregation services relating to the health care operations of Covered Entity provided that Business Associate will not use or disclose the information other than as permitted or required by the underlying Agreement, this Agreement or as required by law. Business Associate shall not otherwise perform data aggregation and/or de-identify PHI except as expressly authorized by the Covered Entity and in compliance with HIPAA de-identification regulations and guidance.

2.2 **Use or Disclosure for Business Associate's Management and Administration.** Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate to the extent such use does not violate any provision of this Agreement and would not violate HIPAA if done by Covered Entity; and provided that (i) the disclosure is Required by Law, or (ii) Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as Required by Law or for the purposes for which it was disclosed to the person, and the person agrees to notify Business Associate immediately of any instances of which it is aware in which the confidentiality of the Protected Health Information has been breached.

ARTICLE III – PRIVACY AND SECURITY OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE

3.1 **Privacy.** Business Associate shall not use or disclose Protected Health Information other than as permitted or required by this Agreement and the Underlying Agreement or as Required By Law.

3.2 **Minimum Necessary Information**. Business Associate shall use reasonable efforts to limit uses, disclosures, and requests for Protected Health Information to a Limited Data Set (as defined in 45 CFR § 164.514(e)(2)) or to the minimum necessary to accomplish the intended purposes of such use, disclosure or request, in accordance with the minimum necessary standards at 45 CFR § 164.502(b) and in any guidance issued by the Secretary.

3.3 **Privacy and Security Safeguards.** Business Associate shall comply with the Security Rule, and adopt, implement and use reasonable and appropriate safeguards necessary to protect the privacy and security of PHI and such other reasonable and appropriate safeguards to protect the confidentiality, integrity, and availability of the Electronic PHI that Business Associate creates, receives, maintains, or transmits on behalf of Covered Entity. Business Associate shall report to Covered Entity any Security Incident[1] of which Business Associate becomes aware or, in the exercise of reasonable diligence, would be aware within the time set out below. Business Associate shall ensure that reasonable and appropriate measures are taken to secure electronic PHI as it is maintained, accessed and/or disclosed by Business Associate, including but not limited to implementation of the most current encryption standards published by the National Institute of Standards and Technology ("NIST").

3.4 **Policies and Procedures**. Business Associate shall implement and maintain reasonable and appropriate HIPAA Privacy and Security policies and procedures to ensure organizational compliance with the HIPAA and other requirements under this Agreement and shall maintain such policies as required under the statute. Upon reasonable request, Business Associate shall provide Covered Entity with a copy of such policies and procedures.

3.5 **Workforce**. Business Associate shall insure that its Workforce who are authorized to access, receive or disclose PHI agree in writing to the same restrictions and conditions that apply to Business Associate with respect to the privacy, security, and integrity of the PHI. Business Associate shall implement a security awareness training program for its Workforce, provide periodic updates or remedial training as needed and document such training as required under HIPAA. Business Associate shall implement appropriate disciplinary policies and procedures for Workforce with regard Workforce access, receipt, use or disclosure of PHI in a manner consistent with the purposes of this Agreement, the Business Associate policies and applicable federal and state law.

3.6 **Agents and Subcontractors.** Any agent or third party with which Business Associate contracts to provide services to Business Associate ("Subcontractor") and which requires Subcontractor receive, access, use or disclose PHI of the Covered Entity is considered a "Business Associate" under the HIPAA and is subject to the same laws and regulations and provisions in this Agreement as the Business Associate. Business Associate shall receive assurances from each Subcontractor in the form of a contract that it will comply with the same laws, regulations, restrictions and conditions with regard to the privacy. security, availability and integrity of PHI and the breach notification requirements that apply to Business Associate through this Agreement.

3.7 **Risk Assessment**. Business Associate shall perform an annual security HIPAA Security Risk Assessment and maintain documentation as required by HIPAA. Business Associate shall provide to Covered Entity a copy of such Risk Assessment or assurances by an independent Certified Public Accountant or independent third-party information security analyst that such a Risk Assessment has been performed and any deficiencies corrected or subject to a corrective action plan.

[1] With respect to the reporting of a security incident, as referenced above, the parties stipulate and agree that Business Associate will furnish the required report to Covered Entity in all cases involving a "Successful Security Incident," which is defined for purposes of this Business Associate Agreement as any security incident that results in or is suspected to have resulted in unauthorized access, use, disclosure, modification or destruction of electronic protected health information of Covered Entity or interference with system operations adversely affecting, or which the Business Associate suspects may adversely affect, the ability of Business Associate to maintain, process or safeguard electronic protected health information of Covered Entity. The parties further stipulate and agree that this paragraph constitutes notice by Business Associate to Covered Entity with respect to any Unsuccessful Security Incident, which is defined for purposes of this Business Associate Agreement as any security incident that does not result in unauthorized access, use, disclosure, modification or destruction of electronic protected health information of Covered Entity, interference with system operations adversely affecting the ability of Business Associate to maintain, process or safeguard electronic protected health information of Covered Entity. By way of example, such Unsuccessful Security Incidents may include: (i) pings on the firewall of Business Associate; (ii) port scans; (iii) attempts to log on to a system or enter a database with an invalid password or username; (iv) denial-of-service attacks that do not result in a server being taken off-line; or (v) malware that does not pass through a firewall (worms, viruses, etc.). The parties further stipulate and agree that with respect to any such Unsuccessful Security Incident, no further or more detailed report to Covered Entity is needed or required under this Business Associate Agreement.

3.8 **Mitigation.** Business Associate shall mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement.

3.9 **Access.** Business Associate shall provide access, or a copy to Covered Entity, at the request of Covered Entity and in the time, method and manner reasonably designated by Covered Entity, to Protected Health Information maintained by Business Associate in a Designated Record Set in order to enable Covered Entity to meet the requirements under 45 C.F.R. § 164.524. To the extent that a copy of records has been requested by an Individual and Covered Entity has requested that Business Associate provide the copy, such copy shall be provided in accordance with the requirements of 45 C.F.R. § 164.524 the most current HIPAA guidance with regard to fees charged for copies or access. Any request for access received by Business Associate from an Individual or representative of Individual shall be immediately, but no later than five (5) business days, forwarded to Covered Entity. Except as Required by Law, and in accordance with HIPAA regulations, no request for access from an Individual or third party, including any federal or state regulatory agency or commission, shall be given by Business Associate prior to notice to the Covered Entity and an opportunity for Covered Entity response.

3.10 **Amendment.** Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that Covered Entity directs or agrees to pursuant to 45 C.F.R. § 164.526, and in the time and manner reasonably designated by Covered Entity. Any request for amendment received by Business Associate from an Individual or representative of Individual shall be immediately, but no later than five (5) business days, forwarded to Covered Entity.

3.11 **Books and Records.** Except for information or matters subject to the attorney-client or other legal privilege, Business Associate shall make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of, Covered Entity available to the Secretary of the Department of Health and Human Services for purposes of determining Covered Entity's compliance with HIPAA. Business Associate shall provide Covered Entity with notice of any request by the Secretary for access to records of Covered Entity and with a log of any PHI that Business Associate provides to the Secretary concurrently with providing such PHI to the Secretary.

3.12 **Accounting of Disclosures .** Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of access and disclosures of Protected Health Information in accordance with 45 C.F.R. § 164.528 and to maintain such documentation as required under HIPAA. Business Associate agrees to provide to Covered Entity, in a time and manner reasonably designated by Covered Entity, information collected in accordance with this section to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. § 164.528.

3.13 **Restrictions**. Business Associate shall comply with any communicated restrictions in the use or disclosure of Protected Health Information to which Covered Entity has agreed pursuant to 45 CFR 164.522, and shall further comply with any Individual's request for restrictions on Protected Health Information disclosures that Covered Entity or Business Associate is required by law to honor, including without limitation, requests for restrictions on disclosures to a health plan if the disclosure is for payment or health care operations and pertains solely to a health care item or service for which the Individual has paid his or her health care provider out of pocket in full, unless disclosure is otherwise required by law. Business Associate shall forward any request for restrictions by an Individual to Covered Entity within five (5) business days of such request. Covered Entity shall determine whether to grant or deny an Individual's request for restrictions.

3.14 **Marketing/Fundraising/Sale of Protected Health Information**. Business Associate shall not use or disclose protected Health Information for purposes of Marketing or fundraising. Business Associate shall not sell Protected Health Information or otherwise receive remuneration, directly or indirectly, in exchange for Protected Health Information; provided, however, that this prohibition shall not affect payment to Business Associate by Covered Entity for performance of the services set forth in the Underlying Arrangement or transfer of PHI in a merger or acquisition.

3.15 **Encryption**. Hard drives on any servers, desktops, laptops or mobile devices that are used to access, receive, transmit, or maintain Covered Entity's Electronic Protected Health Information must be Encrypted. All transmissions of PHI or use of shared-files outside of Business Associate's secured network must be Encrypted. Mobile devices (such as tablets and smart phones) or external or removable media, including, without limitation, USB drives and backup tapes, used for sending, receiving, or storing Electronic Protected Health Information must be Encrypted and password protected with double authentication. For the purposes of this section, "Encrypted" or "Encryption" shall mean any encryption standards that meet the U.S. Department of Health and Human Services Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements under Section 13402 of the HITECH Act.

3.16 **Mobile Device Security and Remote Access**. To the extent that PHI is received, accessed, used, transmitted, or maintained on any mobile device, such as but not limited to a smart phone, tablet, external hard drive, DVD/CD or flash drive, Business Associate shall follow the most current security guidelines recommended and published by HHS and/or NIST. To the extent that the Business Associate permits teleworking or remote access of PHI through a portable device or out-of-network computer, Business Associate

shall insure that such access or disclosure is performed only through a secure method in compliance with the most current encryption standards published by the NIST, that the device is adequately protected by anti-virus and malware software, and that the Workforce is trained on virus and malware detection and prevention. Business Associate shall ensure that no PHI is maintained on any mobile devices, laptops or other authorized out-of-network computer and that the Business Associate has appropriate safeguards in the event of loss or theft or workforce member termination.

ARTICLE IV - BUSINESS ASSOCIATE NOTICE OBLIGATIONS AND INDEMNIFICATION

4.1 Reporting

a. **Notification.** Business Associate shall notify Covered Entity as soon as practicable and in no event later than one (1) business day of any suspected or actual Successful Security Incident, impermissible Use or Disclosure of PHI, or Breach of Unsecured PHI of which Business Associate becomes aware and/or any actual or suspected Use or Disclosure of PHI in violation of any applicable federal or state laws or regulations, including Breaches of Unsecured PHI, as required by 45 C.F.R. § 164.410 (collectively "Impermissible Use or Disclosure"). Notwithstanding anything to the contrary above, in the event of a ransomware incident or other cyber-security incident involving malware or unauthorized access to systems, Business Associate shall provide Covered Entity with immediate notice of such Security Incident whether or not PHI has been encrypted or exfiltrated and whether or not it has been determined that such action is malicious.

b. **Mitigation**. Business Associate shall take prompt corrective action to mitigate any harm, cure any deficiencies leading to the successful Security Incident and/or Impermissible Use or Disclosure and any other action pertaining to such Impermissible Use or Disclosure required by applicable federal and state laws and regulations and this Agreement.

c. **Preliminary Risk Assessment and Investigation.** Without unreasonable delay and, in any event, no more than five (5) business days after discovery, Business Associate shall notify Covered Entity of any Impermissible Use or Disclosure, and shall commence conducting a preliminary risk assessment in order to determine if the Impermissible Use or Disclosure is a violation of any applicable federal or state laws or regulations. Business Associate shall deliver the initial notification of such Impermissible Uses or Disclosures, in writing, which must include a reasonably detailed description of the Impermissible Uses or Disclosures and the steps Business Associate is taking and would propose to mitigate or terminate the successful Security Incident and/or Impermissible Uses or Disclosures and a copy of the initial Risk Assessment. Furthermore, Business Associate shall supplement the initial notification no more than ten (10) days following discovery (or following the date additional information becomes reasonably available to Business Associate) with information including:

(i) the identification of each individual whose PHI was or is believed to have been involved;

(ii) a reasonably detailed description of the types of PHI involved;

(iii) all other information reasonably requested by Covered Entity, including all information necessary to enable Covered Entity to perform and document a risk assessment in accordance with 45 C.F.R. § 164 subpart D; and

(iv) all other information necessary for Covered Entity to provide notice to individuals, the U.S. Department of Health and Human Services and any applicable federal or state regulatory body, or the media, if required.

An initial notification to Covered Entity shall not be delayed because Business Associate has not confirmed an Impermissible Use or Disclosure, has not completed an investigation or does not have all the information needed to provide a complete report. Business Associate shall also notify Covered Entity, in writing, within the timeframes and in the manner outlined in this Agreement, of any use or disclosure of PHI by its subcontractor(s) (or subcontractors' agent(s)) not provided for by this Agreement or the Underlying Agreement.

d. Timing of Discovery of Breach. **An Impermissible Use or Disclosure shall be treated as discovered by Business Associate as of the first day on which such Impermissible Use or Disclosure is known to the Business Associate, or by exercising reasonable diligence would have been known to the Business Associate.**

4.2 **Cooperation.** With regard to any Breach or Successful Security Incident occurring at Business Associate or related to Business Associate services, Business Associate shall cooperate fully with Covered Entity in any investigation or forensic review without regard to any claim of the attorney-client privilege. Cooperation may include, but is not limited to, data analysis to determine appropriate mitigation steps in the event of a Breach, access to Business Associate's systems, logs, audit records and other information technology records for purposes of Breach data analysis, and access to and cooperation of Business Associate IT staff.

4.3 Indemnification for Breach. Business Associate agrees to indemnify and hold harmless Covered Entity and any Covered Entity affiliate, officer, director, employee or agent ("Indemnified Party") from and against any claim, cause of action, liability, damage, fine or penalty, settlement or resolution agreement, cost or expense (including attorneys' and consultants' fees and forensic investigation), administrative proceeding (including government agency investigation) or court costs, arising out of or in connection with any Impermissible Use or Disclosure of PHI or other medical, health or personal information, Breach, security incident, by Business Associate or any subcontractor, agent, person or entity contracted by or under the control of Business Associate. This indemnification shall specifically provide for: (a) the costs incurred by Covered Entity in complying with its legal obligations relating to such Breach or security incident, and (b) in addition to other damages for which Business Associate may be liable, the following reasonable expenses incurred by Covered Entity in responding to such Breach: (i) mitigation of any Breach, Security Incident, or other non-permitted use or disclosure of PHI or medical, health or personal information protected by other federal or state law, including, without limitation, the following: credit monitoring and account monitoring services for impacted individuals for a reasonable period (which shall be no less than 12 months); and such other mitigation action required of Covered Entity by federal or state regulators, and other reasonable mitigation steps taken by Covered Entity; (ii) Notice of Breach, including preparation and mailing of notification(s) of Breach to impacted individuals, the media and regulators; costs associated with proper handling of inquiries from individuals and other entities about Breach (such as the establishment of toll-free numbers, maintenance of call centers for intake, preparation of scripts, questions/answers, and other communicative information about the Breach), and other notice requirements under state laws; and (iii) costs and expenses associated with any subsequent investigation, requests for data or proceeding by the Office of Civil Rights of HHS or any other federal or state agency. This provision is applicable whether or not Business Associate has insurance coverage for such indemnification. With regard to matters arising under this Agreement, this provision supersedes any provision for indemnification in any other agreement between the parties.

ARTICLE V – OBLIGATIONS OF COVERED ENTITY

5.1 Notice of Privacy Practices. Covered Entity will either provide Business Associate with a copy of its notice of privacy practices developed in accordance with 45 C.F.R. § 164.520 or will notify Business Associate of any limitation(s) in Covered Entity's notice of privacy practices, to the extent that such limitation may affect Business Associate's use or disclosure of Protected Health Information.

5.2 Change or Revocation of Permission. Covered Entity shall promptly notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information.

5.3 Restrictions on Use or Disclosure. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.

5.4 Permissible Requests. Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under this Agreement or permitted or required by HIPAA.

ARTICLE VI – TERM AND TERMINATION

6.1 Term. This Agreement is effective on the date set forth on the signature page and shall remain effective for the entire term of the Underlying Agreement, or until terminated as set forth herein.

6.2 Termination.

a. Termination upon Material Breach. Covered Entity may immediately terminate this Agreement in the event that Business Associate breaches any provision of this Agreement, including any Breach or violation of HIPAA or applicable state privacy or security law. In its sole discretion, Covered Entity may offer Business Associate the ability to cure or to take substantial steps to cure such material breach to Covered Entity's satisfaction within thirty (30) days after receipt of written notice from Covered Entity. Covered Entity may additionally report any Breaches to the Secretary.

Business Associate may immediately terminate this Agreement in the event that Covered Entity fails to cure any material breaches of any provision of this Agreement within thirty (30) days after receipt of written notice from Business Associate.

b. Termination upon Expiration of Underlying Agreement. This Agreement shall automatically terminate without any further action of the parties upon the termination of the underlying services agreement; provided, however, to the extent that Business Associate maintains any PHI of Covered Entity beyond such termination or expiration of the Underlying Agreement this Agreement shall remain in full force and effect as required for the protection of the privacy, security and integrity of the PHI.

c. Return or Destruction of PHI. Upon termination, if feasible, Business Associate shall return or destroy all PHI received from, or created or received by Business Associate on behalf of, Covered Entity that Business Associate still maintains in any form and shall retain no copies of such information. Prior to doing so, Business Associate further agrees to recover any PHI in

the possession of its subcontractors or agents. If it is infeasible to return or destroy PHI, including retention is required by law, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction of PHI infeasible. Business Associate shall continue to extend the protections of this Agreement to such PHI, and limit further use of such PHI to those purposes that make the return or destruction of such PHI infeasible.

At no additional cost to the Covered Entity, data shall be returned in a structurally interoperable format that protects the security, integrity and availability of the PHI and other Covered Entity data and permits migration to Covered Entity systems.

ARTICLE VII – LEGAL PRIVILEGES

Except as provided in paragraph 4.2, nothing in this Agreement is intended to or shall be deemed to constitute or require any waiver of any privilege or other legal protection (such as the attorney-client privilege, the work product doctrine and the quality assurance privilege) applicable to, relating to or arising out of (i) the relationship between Covered Entity and Business Associate, (ii) the PHI, or (iii) any summaries, analyses, reports and the like related thereto. The provisions of this section shall survive termination of this Agreement.

ARTICLE VIII - INJUNCTION; DISCLAIMER; DATA OWNERSHIP AND INDEMNIFICATION; INSURANCE

8.1. **Injunction**. Business Associate hereby recognizes that irreparable harm may result to Covered Entity, and to the business of Covered Entity, in the event of a breach by Business Associate of any of the covenants and assurances contained in this Agreement. As such, in the event of a breach of any material covenants and assurances contained herein, Covered Entity shall be entitled to enjoin and restrain Business Associate from any continued violation of such covenants and assurances.

8.2. **Disclaimer**. PROTECTED HEALTH INFORMATION IS PROVIDED TO BUSINESS ASSOCIATE SOLELY ON AN "AS IS" BASIS. COVERED ENTITY DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE.

8.3. **Data Ownership**. As between Covered Entity and Business Associate, any Protected Health Information disclosed, delivered or provided to Business Associate in connection with this Agreement, shall be deemed to be the exclusive property of Covered Entity. In no event shall Business Associate or its Business Associates claim any rights with respect to such Protected Health Information. Any de-identified data created from PHI subject to this Agreement shall be the exclusive property of Covered Entity.

8.4. Insurance. Business Associate shall maintain adequate insurance coverage for the purposes of the indemnifications contained herein. Business Associate shall comply with all notice and compliance requirements of its insurer, including notice of claim requirements. Upon execution of this Agreement, and annually, Business Associate shall provide Covered Entity with a Certificate of Insurance demonstrating its compliance with this provision.

ARTICLE IX - STATE PRIVACY AND SECURITY LAWS

9.1 State Privacy, Security and Breach Notification Laws. To the extent that there is no safe-harbor provision or to the extent an applicable State privacy, security and/or breach notification law is more stringent than HIPAA, Business Associate shall comply, and shall insure that its subcontractors agree to comply, with the more stringent requirements under the applicable State law. Business Associate shall be subject to liability under such State law in addition to any liability under HIPAA.

ARTICLE X – MISCELLANEOUS PROVISIONS

10.1 Amendment to Comply with Law. The parties acknowledge that it may be necessary to amend this Agreement to comply with modifications to HIPAA, including but not limited to statutory or regulatory modifications or interpretations by a regulatory agency or court of competent jurisdiction. No later than sixty (60) days after the effective date of any such modifications, the parties agree to use good faith efforts to develop and execute any amendments to this Agreement as may be required for compliance with HIPAA.

10.2 Amendment. This Agreement may be amended or modified only in writing signed by the parties.

10.3 Relationship of the Parties and No Third Party Beneficiaries. The parties are independent contractors of each other. Nothing in this Agreement shall be construed to create an employer/employee, joint venture, partnership or other similar relationship between the parties. Neither party shall have the right to exercise control or direction over the business of the other party with respect to this Agreement. Nothing expressed or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than Covered Entity, Business Associate and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

10.4 **Governing Law.** This Agreement shall be governed by and construed in accordance with HIPAA and the laws of the State of Florida without regard to conflicts of law principles.

10.5 **Conflicts.** In the event of any conflict between the terms of this Agreement and the terms of the Underlying Arrangement or any such later agreement(s), the terms of this Agreement shall control unless the terms of such Underlying Arrangement are more strict with respect to Protected Health Information and comply with the HIPAA Regulations, or the parties specifically otherwise agree in writing.

10.6 **Paragraph Headings.** The paragraph headings in this Agreement are for convenience only. They form no part of this Agreement and shall not affect its interpretation.

10.7 **Survival.** Article IV and VIII shall survive termination of this Agreement.

10.8 **Entire Agreement.** This Agreement and the Underlying Arrangement constitute the complete agreement between the parties relating to the matters specified in this Agreement, and supersedes all prior representations or agreements, whether oral or written, with respect to such matters. This Agreement is for the benefit of, and shall be binding upon the parties, their affiliates and respective successors and assigns.

10.9 **Notices**. All notices, request, approvals demands or other communications required or permitted to be given under this Agreement shall be in writing and delivered either personally, or by email and certified mail with postage prepaid and return receipt requested or by overnight courier to the party to be notified. All communications will be deemed given when received. The addresses of the Parties , and person to whom notice shall be given are:

ACCEPTED BY BUSINESS ASSOCIATE:

Signed: _____

Name: _____

Title: _____

Company: _____

Date: _____

ACCEPTED BY COVERED ENTITY: Creative Consulting Co.:

Signed: _____

Name: _____

Title: _____

Date: _____