BUSINESS ASSOCIATE AGREEMENT (BAA)

This Business Associate Agreement (Hereinafter "**Agreement**") is entered into by and between _____ (Hereinafter "**Covered Entity**") and Canfield Scientific, Inc. (Hereinafter "**BusinessAssociate**").

1. Introduction

This Agreement governs the terms and conditions under which Business Associate will access Protected Health Information (PHI) belonging to patients of Covered Entity when performing services for, or on behalf of, Covered Entity. Specifically, this Agreement governs the terms and conditions under which Business Associate will provide [description of contracted services] (Hereinafter "**Services**").

Covered Entity and Business Associate intend to work together to ensure the following requirements are met (under the terms of the aforementioned contracted Services):

a) Protect the privacy and provide the proper security for PHI disclosed pursuant to this Agreement.

b) Comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), public law 104-191, as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH), public law 111-5, and the regulations promulgated thereunder by the U.S. Department of Health and Human Services and other applicable federal and state laws.

2. Definitions

- **Breach:** The unauthorized acquisition, access, use, or disclosure of PHIthat compromisesthe security or privacy of affected PHI
- **Business Associate:** A person or entity that creates, receives, maintains, or transmits PHI for a function or regulated activity on behalf of, or when providing services to, a Covered Entity
- **Covered Entity:** Any organization or corporation that directly handles and electronically transmits PHI. The most common examples include hospitals, doctors' offices, and health insurance providers
- **Electronic Protected Health Information (ePHI):** Individually identifiable health information that can be linked to a particular individual and is produced, saved, transferred, or received in an electronic form
- **HHS:** Department of Health and Human Services (also known as the Health Department): A cabinet-level department of the U.S. federal government with the goal of protecting the health of all Americans and providing them with essential human services
- **Individual:** A single human being, with the right to access, review, and update their PHI at any time
- **Protected Health Information (PHI):** Individually identifiable health information that can be linked to a particular individual
- **Secretary:** Secretary of the U.S. Department of Health and Human Services (HHS): A member of the President's cabinet whose main concern is health matters. Duties revolve

around human conditions and concerns in the U.S. including advising the President on matters of health, welfare, and income security programs

- **Secure PHI:** Protected Health Information (PHI) that is made unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology (encryption) or methodology(destruction)
- **Unsecured PHI:** Protected Health Information (PHI) that is not secured through the use of a technology or methodology and therefore can be used, read, or deciphered by unauthorized individuals

3. Governing Regulations

- **HIPAA:** *Health Insurance Portability and Accountability Act of 1996*: Federal law enacted to address the security and privacy of health data. Created to improve the efficiency and effectiveness of the nation's health care system by encouraging widespread use of electronic data interchange in the U.S. health care system. Appointed the HHS responsible for enforcing the rules, accountability, and standards for patient information in the internet age
- **HIPAA Security Rule:** Established national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a Covered Entity. Requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of ePHI
- **HIPAA Privacy Rule:** Established national standards to protect individuals' medical records and other health information including information stored or transmitted electronically. Requires appropriate safeguards be put in place to protect the privacy of individual health information and sets limits and conditions on the uses and disclosures that may be made with such information without patient authorization. It also gives patients the right to review and obtain copies of their medical records and request changes to incorrect data
- **HITECH:** *Health Information Technology for Economic and Clinical Health (HITECH Act)*: Legislation created to promote and expand the adoption of health information technology (electronic health records and supporting technology) in the United States by the HHS. Considered to be the most important piece of health care legislation to be passed in the last 30 years and the foundation for health care reform in the United States
- **45 CFR Part 160:** 45 CFR = Public Welfare; Part 160 = General Administrative Requirements
- **45 CFR Part 164:** 45 CFR = Public Welfare; Part 164 = Security and Privacy

4. Obligations and Activities of Business Associate

HIPAA COMPLIANCE

Business Associate agrees to:

a) Not use or disclose PHI other than as permitted or required by this Agreement or as required by law.

b) Use the appropriate physical, technical, and administrative safeguards to prevent use or disclosure of PHI other than as permitted by this Agreement or as required by law.

c) Reasonably and appropriately protect the confidentiality, integrity, and availability of the Electronic Protected Health Information (ePHI) that Business Associate creates, receives, maintains, or transmits on behalf of Covered Entity.

d) Report in writing to Covered Entity within 10 business days after discovery and suspected or actual access, use, or disclosure of PHI not permitted by this Agreement; breach of unsecured PHI; security breach or intrusion; use or disclosure of PHI in violation of any applicable federal or state laws or regulations.

e) Implement a reasonable system for breach identification and assessment.

f) Mitigate to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement.

g) Ensure that any agent, including subcontractors that create, receive, maintain, or transmit PHI on behalf of Business Associate agrees to the same restrictions, conditions, and requirements that apply through this Agreement to Business Associate with respect to such information.

h) Provide access to PHI (upon request from Covered Entity) within 10 businessdays from the day the request is received in the time and manner designated by Covered Entity, to Covered Entity, or to an Individual as instructed.

i) Document any disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request from an Individual for an accounting of disclosures of PHI.

j) Make its internal practices, books, and records relating to the use and disclosure of PHI received from, created, or received by Business Associate on behalf of Covered Entity available to the Secretary for purposes of determining Covered Entity's compliance with the HIPAA Rules. In the event of such request, Business Associate agrees to notify Covered Entity immediately.

k) Allow Covered Entity to conduct a reasonable inspection (with at least 30 business days' notice) of its facilities, systems, books, records, agreements, policies, and procedures relating to the use and disclosure of PHI pursuant to this Agreement to determine whether or not Business Associate has complied with this Agreement. However, Business Associate and Covered Entity must mutually agree in advance upon the scope, location, and timing of such inspection; and Covered Entity must agree to protect the confidentiality of all confidential and proprietary information of Business Associate to which Covered Entity is exposed to during the inspection. Such inspection will be available to Covered Entity no more than annually unless Covered entity has an articulable concern that forms the basis for the request.

l) Understand and comply with state privacy laws to the extent that such state privacy laws are not preempted by HIPAA or HITECH.

HITECH COMPLIANCE

Business Associate agrees to:

a) Not receive (directly or indirectly) any impermissible remuneration in exchange for PHI or ePHI except as permitted by HIPAA or HITECH Regulations.

b) Comply with the marketing and other restrictions applicable to Business Associates contained in HITECH and HIPAA Regulations.

c) Fully comply with the applicable requirements of 45 CFR 164 for each use and disclosure of PHI to the extent required under HITECH.

d) Fully comply with 45 CFR 164 to the extent required under HITECH.

e) Comply with the additional privacy and security requirements (to the extent required under HITECH) that apply to Covered Entities in the same manner and to the same extent as Covered Entity is required to do so.

f) Comply with the privacy and security requirements that apply to Business Associates to the extent required under the HIPAA Regulations.

5. Permitted Uses and Disclosures by Business Associate

Except as otherwise limited in this Agreement:

a) Business Associate may use or disclose PHI as necessary to perform the services set forth in the [Service Agreement Name].

b) Business Associate may use or disclose PHI as required by law.

c) Business Associate agrees to perform functions for uses, disclosures, or requests for PHI on behalf of Covered Entity, provided that such use, disclosure, or request would not violate the Privacy Rule if done by Covered Entity.

d) Business Associate may not use or disclose PHI in a manner that would violate [Subpart E of 45 CFR Part 164] if done by Covered Entity except for the specific uses and disclosures set forth below.

e) Business Associate may disclose PHI for the proper management and administration of the Business Associate, provided that disclosures are required by law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notified Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

6. Obligations of Covered Entity

a) Covered Entity shall provide Business Associate with its notice of privacy practices as well as any changes to such notice.

b) Covered Entity shall notify Business Associate of any limitations in the notice of privacy practices of Covered Entity to the extent that such limitation may affect Business Associate's use or disclosure of PHI.

c) Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible if done by Covered Entity.

d) Covered Entity will indemnify and hold harmless Business Associate and any of its officers, directors, employees, or agents from and against any third party claim, cause of action, liability, damage, cost or expense, including reasonable attorneys' fees and court or proceeding costs ("Losses"), attributable to any material breach of the terms of this Agreement by Covered Entity, any incident involving PHI under the control of Covered Entity or its agents or subcontractors, or any failure to perform its obligations with respect to PHI by Covered Entity, it officers, employees, agents or any person or entity under Business Associate's direction or control. The indemnity obligations hereunder shall only apply so long as Business Associate has complied with all of its obligations under this Agreement and so long as Business Associate's actions or omissions are not responsible for the violations/breaches or losses.

7. Term and Termination

a) The Terms of this Agreement are effective as of [insert effective date]/or [insert execution date of contract of services]. These terms will terminate when all of the PHI provided by Covered Entity to Business Associate or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or if it is infeasible to return or destroy PHI, protections are extended to such information, in accordance with this Agreement.

b) Business Associate authorizes termination of this Agreement by Covered Entity, if covered entity determines Business Associate has violated a material term of this Agreement and Business Associate has not cured the breach or ended the violation with the time specified by Covered Entity.

- **Obligations of Business Associate upon Termination of this Agreement**

Upon termination of this Agreement (for any reason), Business Associate, with respect to PHI received, created, or maintained by Business Associate on behalf of Covered Entity shall:

i. Only retain the PHI that is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities.

ii. Return to Covered Entity (or if agreed to by Covered Entity, destroy) the remaining PHI (in any form) that the Business Associate still maintains.

iii. Continue to use appropriate safeguards and comply with Regulations with respect to ePHI to prevent use or disclosure of PHI, other than as provided for in this Section, for as long as Business Associate retains the PHI.

iv. Not use or disclose the PHI retained by Business Associate other than for the purposes for which such PHI was retained and subject to the same condition permitted by this Agreement.

v. Return to Covered Entity (or if agreed to by Covered Entity, destroy), the PHI retained by Business Associate when it is no longer needed by Business

Associate for its proper management and administration or to carry out its legal responsibilities.

c) In the event that Business Associate determines returning or destroying PHI is infeasible, Business Associate will provide Covered Entity with notification of the conditions that make return or destruction infeasible. If Covered Entity approves these conditions, Business Associate will extend its protections of this Agreement to such PHI and limit further use and disclosure of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.

d) The obligations of Business Associate under this Section survive the termination of this Agreement.

8. Miscellaneous

a) Covered Entity makes no warranty or representation that compliance by Business Associate with this Agreement, HIPAA, HITECH, or the HIPAA Regulations will be adequate or satisfactory for Business Associate's own purposes. Business Associate is solely responsible for all decisions made by Business Associate regarding the safeguarding of PHI.

b) Covered Entity holds all right, title, and interest in and to the PHI. Business Associate does not hold and will not acquire by virtue of this Agreement or by virtue of providing goods or services to Covered Entity, any right, title, or interest in or to PHI or any portion thereof.

c) Both parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary in compliance with the requirements of the HIPAA Rules and any other applicable law.

d) Any ambiguity in this Agreement will be interpreted to permit compliance with the HIPAA Rules.

e) In the event any part or parts of this Agreement are held to be unenforceable, the remainder of this Agreement will continue in effect.

f) Business Associate agrees to indemnify, defend, and hold harmless Covered Entity against and in respect of, any and all claims, losses, expenses, costs, damages, obligations, penalties, and liabilities which Covered Entity may incur by reason of Business Associate's breach of or failure to perform any of its obligations pursuant to this Agreement.

g) Business Associate agrees to indemnify, defend, and hold harmless Covered Entity against all costs and expenses, including but not limited to, reasonable legal expenses, which are incurred by or on behalf of Business Associate in connection with the defense of such claim.

h) The terms and conditions of this Agreement shall override and control any conflicting term or condition of the Services Agreement. All non-conflicting terms and conditions of the Services Agreement remain in full force and effect.

i) Relationship of Parties. It is expressly agreed that Business Associate, its divisions, and its affiliates, including its employees and subcontractors, are performing the services under this Agreement as independent contractors for Covered Entity. Neither Business Associate nor of its affiliates, officers, directors, employees or subcontractors is an employee or agent of Covered Entity. Nothing in this Agreement shall be construed to create (i) a partnership,

joint venture or other joint business relationship between the parties or any of their affiliates, or (ii) an agency relationship for purposes of the HITECH Act.

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be executed by their respective duly authorized officers or agents as of [insert effective date].

COVERED ENTITY:	**BUSINESS ASSOCIATE:**
Signature:_____	Signature:_____
Printed Name:_____	PrintedName: _____
Title:_____	Title:_____
Date:_____	Date:_____