

This Business Associate Agreement (“Agreement”) entered into by and between _____ (hereinafter “Business Associate”) and **Steinberg Diagnostic Medical Imaging** (hereinafter “Covered Entity”) on _____ to comply with privacy and security standards adopted by the U.S. Department of Health and Human Services, and any applicable state confidentiality laws, the terms of this Agreement shall govern:

Obligations of Covered Entity If deemed applicable by Covered Entity, Covered Entity shall:

1. provide Business Associate with any changes in, or revocation of, authorizations by Individuals relating to the use and/or disclosure of protected health information, if such changes affect Business Associate’s permitted or required uses and/or disclosures;
2. notify Business Associate of any restriction to the use and/or disclosure of protected health information to which Covered Entity has agreed in accordance with 45 CFR 164.522;
3. notify Business Associate of any amendment to protected health information to which Covered Entity has agreed that affects a Designated Record Set maintained by Business Associate; and
4. if Business Associate maintains a Designated Record Set, provide Business Associate with a copy of its policies and procedures related to an Individual’s right to: access protected health information; request an amendment to protected health information; request confidential communications of protected health information; revocation of permission by an individual to use protected health information; restriction on the use and disclosure of protected health information; or request an accounting of disclosures of protected health information.
5. shall not request Business Associate to use or disclose protected health information in any manner that would not be permissible under Subpart E of 45 CFR Part 164 if done by the Covered Entity.

Obligations of Business Associate:

1. **Permitted Uses and Disclosures.** Business Associate shall not use or disclose any protected health information received from or on behalf of Covered Entity except as permitted or required by the Agreement, or as required by law;
 - a) Business Associate may only use or disclose protected health information such as “necessary to perform the services” set forth in all Contractual Agreements;
 - b) Business Associate will get authorization from Covered Entity to use de-identified protected health information and must de-identify the information in accordance with 45 CFR 164.514(a)-(c).
 - c) Business Associate may use or disclosure protected health information as required by law;
 - d) Business Associate agrees to make uses and disclosures and requests for protected health information consistent with Covered Entity’s minimum necessary policies and procedures.
 - e) Business Associate may not use or disclose protected health information 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 (f) and (g).
 - f) Business Associate may use protected health information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.
 - g) Business Associate may disclose protected health information for the proper management and administration of Business Associate or to carry out the legal responsibilities of the Business Associate, provided the disclosures are required by law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential 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 notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.
 - h) Business Associate shall not use or disclose PHI for fundraising or marketing purposes no shall Business Associate receive indirectly or directly any remuneration in exchange for PHI or any other purpose not permitted by this Agreement, the Privacy Rule, or HITECH Act.

2. **Safeguarding of ePHI:** If Business Associate receives or maintains Electronic Protected Health Information (ePHI), Business Associate (and any subcontractor or agent) will comply with subpart C of 45 CFR Part 164 to prevent use or disclosure of protected health information other than as provided for by the Agreement;

3. **Subcontractors and Agents:** In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to Business Associate with respect to such information.

4. **Inspection of Books and Records** Business Associate (and any subcontractor or agent) will make its internal practices, books and records, relating to its use and disclosure of the protected health information it creates or receives for or from Covered Entity, available to the U.S. Department of Health and Human Services to determine Covered Entity's compliance with 45 CFR Parts 160 and 164.

5. **Protected Health Information Access, Amendment and Disclosure Accounting.**

a) **Access:** At the direction of Covered Entity, Business Associate agrees to provide access to any protected health information held by Business Associate, which Covered Entity has determined to be part of Covered Entity's Designated Record Set, in the time and manner designated by Covered Entity. This access will be provided to Covered Entity or, as directed by Covered Entity, to an Individual, in order to meet the requirements under the Privacy Rule 45 CFR 164.524.

b) **Amendment:** At the direction of Covered Entity, Business Associate agrees to amend or correct protected health information held by Business Associate, which Covered Entity has determined to be part of Covered Entity's Designated Record Set, in the time and manner designated by Covered Entity, in order to meet the requirements under the privacy rule 45 CFR 164.526.

c) **Accounting of Disclosures:** At the direction of Covered Entity, Business Associate agrees to maintain and make available the information required to provide an Accounting of Disclosure to the Covered Entity to meet its accounting obligations under the Privacy Rule 45 CFR 164.528.

d) **Restriction Agreements and Confidential Communications.** Business Associate (and any subcontractor or agent) will comply with any agreement that Covered Entity makes that either:

- Restricts use or disclosure of Covered Entity's protected health information pursuant to 45 CFR 164.522(a), or
- Requires confidential communication about Covered Entity's protected health information pursuant to 45 CFR 164.522(a), provided that the Covered Entity notifies Business Associate in writing of the restriction or confidential communication.

6. **Breach of Privacy Obligations:**

a) **Reporting of an Incident/Breach,** Business Associate shall report to Covered Entity including those occurrences reported to Business Associate by its subcontractors or agents, a discovery of breach or any use or disclosure of protected health information which is not in compliance with the terms of this Agreement. An occurrence of protected health information shall be treated as "discovered" as of the first day on which such occurrence is known to the Business Associate, or, by exercising reasonable diligence would have been known to the Business Associate.

- The Business Associate shall provide notice to the Covered Entity of the occurrence. Business Associate will contact Covered Entity within **Five (5)** business days of the discovery, the Business Associate shall notify the Covered Entity's Privacy Officer.
- Investigation of Occurrence. The Business Associate shall immediately conduct an investigation and report in writing the following information:
 - Each individual whose protected health information has been or is reasonably believed to have been accessed, acquired, or disclose during the occurrence.
 - A brief description of what happened, including the date of the occurrence and the date of the discovery of

the occurrence, if known.

- A description of the types of protected health information that were involved in the occurrence (such as full name, social security number, date of birth, home address, account number, etc.).
- A brief description of what the Business Associate is doing to investigate the occurrence, to mitigate losses and to protect against further occurrences.
- The actions the Business Associate has undertaken or will undertake to mitigate any harmful effect of the occurrence, and a corrective action plan that includes the steps the Business Associate has taken or shall take to prevent future similar occurrences.

- b) **Notification to Individuals:** Covered Entity will be responsible for notifying individuals of the occurrence Business Associate agrees to pay all cost of such notifications, as well as any costs associated with the breach, including but not limited to credit monitoring.
- c) **Mitigating Effect of an Incident/Breach:** Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a misuse or unauthorized disclosure of protected health information by Business Associate in violation of the requirements of this Agreement. The Business Associate shall reasonably cooperate with the Covered Entity's efforts to seek appropriate injunctive relief or otherwise prevent or curtail such threatened or actual breach, or to recover its protected health information, including complying with a reasonable Corrective Action Plan.
- d) **Security Incidents:** If a security incident results in a disclosure of Covered Entity's ePHI not permitted by this Agreement, Business Associate will promptly report such incident to Covered Entity.
- Business Associate will report unauthorized access, disclosure, modification or destruction of Covered Entity's ePHI of which Business Associate becomes aware, or
 - Interference with system operations in Business Associate's information systems involving Covered Entity's ePHI of which Business Associate becomes aware.

7. **Termination of Agreement.**

- a) **Term.** The term of this Agreement shall be effective as of date on First Page of this Agreement, and shall terminate when Contractual Obligations are no longer utilized or on the date Covered Entity terminates for cause as authorized in paragraph (b) of this Section.
- b) **Termination for Cause.** Business Associate agrees that Covered Entity has the right to terminate the Agreement if Covered Entity determines that Business Associate (and any subcontractor or agent) has violated a material term of this Agreement and such violation continues for ten (10) days after written notice of such violation has been given to Business Associate by Covered Entity 45 CFR 164.504 (e).
- c) **Obligations of Business Associate upon Termination.** Upon termination, cancellation, expiration, or other conclusion of the Agreement, Business Associate with respect to protected health information received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity shall:
- Retain only that protected health information which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;
 - Return to Covered Entity or, if return is not feasible, destroy all protected health information in whatever form or medium that Business Associate received from or created on behalf of Covered Entity within a thirty (30) day period, Business Associate shall certify in writing to Covered Entity that such return or destruction has been completed. If Business Associate destroys protected health information, it shall be done with the use of technology or methodology that renders the protected health information unusable, unreadable, or undecipherable to unauthorized individuals as specified by HHS in HHS guidance. Within such thirty (30) day period, Business Associate shall certify in writing to Covered Entity that such return or destruction has been completed;
 - Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information to prevent use or disclosure of the protected health information, other than as provided for in this Section, for as long as Business Associate retains the protected health information;
 - Not use or disclose the protected health information retained by Business Associate other than for the purposes for which such protected health information was retained and subject to the same conditions set out at Permitted

- Uses and Disclosures by Business Associate paragraph (f) and (g) which applied prior to termination; and
- Returned to Covered Entity or, if return is not feasible, destroy all protected health information 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.

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

The parties agree that, in the event that any documentation of the arrangement pursuant to which Business Associate provides services to Covered Entity contains provisions relating to the use or disclosure of Protected Health Information which are more restrictive than the provisions of this Agreement, the provisions of the more restrictive documentation will control. The provisions of this Agreement are intended to establish the minimum requirements regarding Business Associate's use and disclosure of Protected Health Information.

In the event that any provision of this Agreement is held by a court of competent jurisdiction to be invalid or unenforceable, the remainder of the provisions of this Agreement will remain in full force and effect. In addition, in the event a party believes in good faith that any provision of this Agreement fails to comply with the then-current requirements of the HIPAA Security and Privacy Rule, such party shall notify the other party in writing, For a period of up to thirty days, the parties shall address in good faith such concern and amend the terms of this Agreement, if necessary to bring it into compliance. If, after such thirty-day period, the Agreement fails to comply with the HIPAA Security and Privacy Rule, then either party has the right to terminate upon written notice to the other party.

IN WITNESS WHEREOF, the Parties have executed this Agreement to be effective full upon execution, as indicated by the last date written below.

Covered Entity:

Business Associate:

Sign

Sign

Print

Print

Title

Title

Date

Date