



American College
of Radiology™

1892 Preston White Drive
Reston, VA 20191

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (BAA) is entered into by and between _____ (Covered Entity) and the **American College of Radiology** (Business Associate) as of the date of last signature below.

WHEREAS, Covered Entity has a business relationship with Business Associate as evidenced by a separate agreement (Underlying Agreement) under which Business Associate performs or assists Covered Entity with a function or activity involving the use or disclosure of Protected Health Information (PHI), as that term is defined under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). For purposes of this Agreement the definition of PHI includes electronic PHI.

WHEREAS, Covered Entity and Business Associate desire to comply with the requirements and regulations promulgated pursuant to HIPAA, which privacy regulations are codified at 45 CFR, Parts 160 and 164, and which security regulations are codified at 45 CFR, Parts 160, 162 and 164, and as amended by the American Recovery and Reinvestment Act of 2009 (ARRA), which pertinent provisions are found in Subtitle D of the Health Information Technology of Economic and Clinical Health Act (HITECH Act), 42 USC Sections 17921, 17931-17932 and 17934, further modified by 45 CFR Parts 160 and 164, dated January 25, 2013, and hereafter described as the HITECH Final Rule. In all other matters, so long as not inconsistent with HIPAA, the HITECH Act or attendant regulations, the provisions of the Underlying Agreement are binding.

WHEREAS, Covered Entity and Business Associate desire to enter into an agreement as required by 45 CFR 164.502(e) to provide satisfactory assurances to Covered Entity that Business Associate will appropriately safeguard PHI disclosed to it pursuant to any and all contracts with Covered Entity.

THEREFORE, in consideration of the mutual covenants contained herein, and for good and lawful consideration as set forth in the Underlying Agreement, Covered Entity and Business Associate enter into this Agreement for the purpose of ensuring compliance with the requirements of HIPAA, its implementing regulations, the HITECH Act and the Final Rule, and intending to be legally bound, the Parties hereby agree as follows:

1. **Definitions.** All terms and phrases in this Agreement shall have the same meanings as set forth in HIPAA, 45 CFR Parts 160, 162 and 164, Subparts A through E, and as amended by the HITECH Act and the Final Rule.

2. Permitted Uses and Disclosures by Business Associate

A. Except as otherwise limited in this BAA, Business Associate may use or disclose PHI 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, the Privacy or Security Rules or the HITECH Act if done by Covered Entity.

B. Except as otherwise limited in this BAA, Business Associate may use PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate, including reporting violations of the law to appropriate Federal and State authorities, consistent with CFR 164.502(j)(1).

C. Except as otherwise limited by this BAA, Business Associate may disclose PHI for the proper management and administration of Business Associate, provided that such disclosures are for the purpose of performing Business Associate's obligations under the Underlying Agreement or are required by law or Business Associate obtains reasonable assurances from any third party to whom PHI 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 third party and the third party notifies Business Associate within five (5) business days of any instances of which it becomes aware in which the confidentiality of the information has been breached.

D. Business Associate may use PHI to provide Data Aggregation services to Covered Entity as permitted by 45 CFR 164.504(e)(2)(i)(B) to the extent specifically required under the Agreement.

E. Business Associate shall not use or disclose PHI for fundraising or marketing purposes nor shall Business Associate receive indirectly or directly any remuneration in exchange for any PHI or any other purpose not permitted by this Agreement, the Underlying Agreement, the Privacy Rule or HITECH Act or the Final Rule.™

3. Obligations and Activities of Business Associate

A. Business Associate shall not use or further disclose PHI other than as permitted or required by this BAA or as required by law.

B. Business Associate shall use appropriate safeguards as required by HIPAA and the HITECH Act to prevent use or disclosure of PHI not provided for by this BAA or the Underlying Agreement, including but not limited to administrative, physical and technical safeguards as defined in the Security Rule, 45 CFR Part 164, Subpart C, including using appropriate safeguards for electronic PHI.

C. Business Associate shall ensure that any subcontractor to whom it provides PHI received from, or created or received by Business Associate on behalf of Covered Entity, agrees in writing to the same restrictions and conditions that apply through this BAA to Business Associate with respect to such information. In the event that Business Associate creates, maintains, receives or transmits electronic PHI on behalf of Covered Entity, Business Associate shall implement appropriate safeguards as mentioned in Section 3(B) above with respect to such electronic PHI.

D. Business Associate shall report to Covered Entity within five (5) business days any use or disclosure of PHI or an Individual's information not provided for by this BAA, including without limitation any Breach of PHI, Unsecured PHI or an Individual's information, and any Security Incident that compromises PHI or an Individual's information of which Business Associate becomes aware.

E. Business Associate shall, in consultation with the Covered Entity, take any action necessary to mitigate, to the extent practical, any harmful effect that is known to Business Associate of a Security Incident, and of any use or disclosure not provided for by this BAA.

F. If Business Associate maintains PHI in a Designated Record set, Business Associate shall:

- (1) Provide access, at the request of the Covered Entity, in a time and manner mutually agreed upon in good faith by both parties, to PHI in a Designated Record set, to Covered Entity, or as directed by Covered Entity, to an individual in order to meet the requirements under 45 CFR 164.524, including requirements relating to access to electronic PHI; and
- (2) Make any amendments to PHI in a designated Record Set that Covered Entity directs or agrees to pursuant to 45 CFR 164.526 at the request of Covered Entity or an individual, and in a time and manner mutually agreed upon in good faith by both parties.

G. Business Associate agrees to make its internal practices, books and records, including policies and procedures 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, for purposes of the Secretary determining Covered Entity's or Business Associate's compliance with HIPAA.

H. Business Associate shall make available to Covered Entity the information required to provide an accounting of disclosures to enable Covered Entity to fulfill its obligations under the Privacy Rule, the HITECH Act and the Final Rule. Such information for an accounting will be collected and maintained by Business Associate for at least six (6) years prior to the request. The accounting should include (1) the date of disclosure, (2) the name of the entity or person, and address if known, who received the PHI, (3) a brief description of PHI disclosed, and (4) a brief statement of the purpose of the disclosure. In the event that a

request for accounting is delivered directly to Business Associate, Business Associate will promptly forward the request to Covered Entity.

I. Business Associate acknowledges that if it violates any of the requirements provided under this BAA, Business Associate will be subject to the same civil and criminal penalties that a Covered Entity would be subject to if such Covered Entity violated the same requirements.

J. Business Associate shall implement and maintain safeguards as necessary to ensure that all PHI is used or disclosed only as authorized under HIPAA, the HITECH standards, the Final Rule and this BAA. Business Associate agrees to assess potential risks and vulnerabilities to PHI in its possession and develop, implement and maintain the administrative, physical and technical safeguards required by the HIPAA and HITECH standards that protect the confidentiality, availability and integrity of the PHI that Business Associate creates, receives, maintains or transmits on behalf of the Covered Entity. Business Associate also agrees to implement policies and procedures required under the Final Rule that address Business Associate's compliance with applicable HIPAA standards and its efforts to detect, prevent and mitigate the risks of identity theft from the improper use and/or disclosure of an Individual's information.

K. To the extent Business Associate is to carry out one or more of Covered Entity's obligations under Subpart E of 45 C.F.R. Part 164, Business Associate will comply with the requirements of Subpart E that apply to Covered Entity in the performance of such obligations.

L. Both Parties shall limit the request, disclosure and use of PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

4. Obligations of Covered Entity

A. It is the responsibility of Covered Entity to notify patients of any breach of PHI, including any breach of PHI involving more than 500 individuals. At no time is Business Associate to contact or speak directly to any of Covered Entity's patients/individuals who are the subject of a breach or to the media regarding any such breach. Business Associate shall cooperate with Covered Entity as necessary to provide notification and any details pertaining to any breach.

B. Covered Entity shall provide Business Associate with the Notice of Privacy Practices that Covered Entity produces in accordance with 45 CFR 164.520, as well as any changes to such Notice to the extent they may affect Business Associate's use or disclosure of PHI; Business Associate shall comply with such Notice of Privacy Practices.

C. Covered Entity shall provide Business Associate with any changes in, or revocation of, permission by individual to use or disclose PHI, if such changes affect Business Associate's permitted or required uses and disclosures. Business Associate shall act promptly upon notification of any such change to ensure that its future uses and disclosures

of PHI comply with such a change. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 CFR 164.522 to the extent such restriction relates to PHI used or disclosed by Business Associate. Business Associate shall act promptly upon notification of any such restriction to ensure that its future uses or disclosures of PHI comply with such restriction.

D. Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under HIPAA or the HITECH standards if done by Covered Entity.

5. Term and Termination

A. The obligations of Business Associate shall commence on the Effective Date and shall terminate when the Agreement terminates and 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 not feasible to return or destroy PHI, the terms of this Agreement are extended to cover such information and survive termination of this Agreement.

B. Upon Covered Entity's knowledge of a material breach by Business Associate to the terms of this Agreement, Covered Entity shall provide an opportunity for Business Associate to cure the breach or end the violation upon mutually agreeable terms. If Business Associate does not cure the breach or end the violation according to such terms, or if Covered Entity and Business Associate are unable to agree upon such terms, Covered Entity may terminate this Agreement and any Underlying Agreement between Covered Entity and Business Associate which is the subject of such breach.

C. In the event Business Associate has breached a material term of this Agreement and a cure is not possible, Covered Entity may immediately terminate this Agreement and any Underlying Agreement between Covered Entity and Business Associate which is the subject of such breach.

6. Effect of Termination

A. Except as provided in Section 6(B) of this BAA, upon termination of the Underlying Agreement or this BAA, for any reason, Business Associate shall return or destroy all PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to PHI that is in the possession of any subcontractors or agents of Business Associate. Business Associate shall retain no copies of PHI.

B. In the event that Business Associate determines that returning or destroying the PHI is not feasible and unless the Underlying Agreement already specifies that return or destruction of PHI is not feasible, Business Associate shall provide Covered Entity notification of the conditions that make return or destruction of PHI not possible. Upon mutual agreement of the parties that return or destruction is not feasible, Business Associate shall extend the

protections of this BAA to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction not feasible for so long as Business Associate maintains such PHI.

Notwithstanding the termination provisions of this BAA, the provisions of Section 6 shall survive termination of this BAA.

7. Miscellaneous

A. Business Associate acknowledges that Business Associate has no ownership rights with respect to Covered Entity's PHI.

B. The parties understand and agree that the terms of this BAA are reasonable and necessary to protect the interests of the Covered Entity and the Business Associate. The parties further agree that Covered Entity would suffer irreparable harm if the Business Associate breached this BAA. Thus, in addition to any other rights or remedies the Covered Entity may have, the Covered Entity shall be entitled to obtain injunctive relief to enforce the terms of this BAA.

C. Any ambiguity in the terms of this BAA shall be resolved in favor of a meaning that permits the parties to comply with the HIPAA, HITECH and the Final Rule.

D. This BAA is not intended to and does not create a private cause of action by any individual other than the parties to this BAA, as a result of any claim arising out of a breach of this BAA, the HIPAA or HITECH standards or any state or federal law or regulation relating to privacy or confidentiality.

E. In the event that any law or regulation is enacted or promulgated regarding the protection of health information that is in any way inconsistent with the terms of this BAA or that interferes with either party's obligations with respect to the protection of health information so as to warrant a modification of this BAA or in the event any HIPAA standard is amended or modified, either party shall have the right to amend this BAA so as to bring it into compliance with any such change by providing written notice to the other party, which notice shall allow the other party fifteen (15) business days to contest such amendment before implementation. If such proposed amendment(s) are contested, the Parties shall negotiate in good faith to amend the terms of this Agreement to comply with applicable law. If, following such good faith negotiations, the Parties cannot agree upon an amendment to implement the requirements of said law or final rule, then either Party may terminate this Agreement and the Underlying Agreement(s) upon written notice to the other Party. Except as set forth above in this Section 7(E), this BAA shall only be amended or modified upon written consent of the parties.

F. If any provision of this BAA shall be declared invalid or illegal for any reason whatsoever, then notwithstanding such invalidity or illegality, the remaining terms and provisions of this BAA shall remain in full force and effect in the same manner as if the

invalid or illegal provision had not been contained herein, and such remaining provisions shall be valid, enforceable and legal to the maximum extent permitted by law.

G. Any notice or other communication given pursuant to this BAA must be in writing and personally delivered or sent by registered or certified mail, postage prepaid, to the address as specified below:

Covered Entity: _____

Business Associate: Department of Quality and Safety
Attn: Q&S Operations
American College of Radiology
1892 Preston White Drive
Reston, VA 20191-4326

Center for Research and Innovation
Attn: Julie Zhao
American College of Radiology
50 S. 16th St., Suite 2800
Philadelphia, PA 19102

Notices pertaining to any unauthorized use or access to PHI or breach of PHI shall be submitted to the Covered Entity in accordance with the information provided below:

Contact Person: _____

Title: _____

Address: _____

Contact Phone: _____

Contact Email: _____

Signature: _____

Signature: Mythreyi Chatfield

Print Name: _____

Print Name: Mythreyi Chatfield

Title: _____

Title: Executive Vice President for Quality
& Safety

Date: _____

Date: September 4, 2024



American College
*of Radiology*TM

Please provide a list of all facility locations and ID numbers to which this Business Associate Agreement should be applied. If needed, make additional copies to ensure that information for all applicable facilities is provided.

Facility Name: _____
Facility Location Address: _____
City: _____ State: _____ Zip: _____
Accreditation ID Number(s) (Please specify the modality with the ID number such as MRAP 1234.): _____
NRDR Facility ID Number: _____

Facility Name: _____
Facility Location Address: _____
City: _____ State: _____ Zip: _____
Accreditation ID Number(s) (Please specify the modality with the ID number such as MRAP 1234.): _____
NRDR Facility ID Number: _____

Facility Name: _____
Facility Location Address: _____
City: _____ State: _____ Zip: _____
Accreditation ID Number(s) (Please specify the modality with the ID number such as MRAP 1234.): _____
NRDR Facility ID Number: _____