BUSINESS ASSOCIATE AGREEMENT

This BUSINESS ASSOCIATE AGREEMENT (the "BAA") is effective as of the date of the last signature below and is entered into by and between _____, a _____ organized under the laws of _____ ("Covered Entity"), and CriterionMD, Inc., a Delaware corporation ("Business Associate," in accordance with the meaning given to those terms at 45 CFR §164.501). Covered Entity and Business Associate are each a "Party" and, collectively, the "Parties."

BACKGROUND

I. Covered Entity is either a "covered entity" or a "business associate" of a covered entity, as each is defined under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, as amended by the HITECH Act (as defined below), and the related regulations promulgated by HHS (as defined below) (collectively, "HIPAA") and, as such, is required to comply with HIPAA provisions regarding the confidentiality and privacy of Protected Health Information (as defined below);

II. The Parties have entered into or will enter into one or more agreements, order forms, subscription agreements, statements of work, pilot or beta participation agreements, online terms, or similar agreements under which Business Associate provides or will provide certain specified services to Covered Entity (collectively, the "Agreement");

III. Business Associate provides current and future CriterionMD software, applications, browser-based tools, artificial-intelligence-enabled workflows, payer-policy and medical-necessity support, clinical-documentation review, coding support, customer support, implementation support, security monitoring, and related services made available under the Agreement, including the product currently known as Insurify and any successor, related, or additional CriterionMD products or modules (collectively, the "CriterionMD Services");

IV. In providing the CriterionMD Services pursuant to the Agreement, Business Associate may create, receive, maintain, transmit, or otherwise process Protected Health Information, including PHI included in user-submitted notes, clinical documentation, diagnoses, procedures, payer or insurance information, medical-necessity questions, prior-authorization-related information, and related support communications;

V. By providing the CriterionMD Services pursuant to the Agreement, Business Associate will become a "business associate" of Covered Entity as such term is defined under HIPAA;

VI. Both Parties are committed to complying with all federal and state laws governing the confidentiality and privacy of health information, including, but not limited to, the Standards for Privacy of Individually Identifiable Health Information found at 45 CFR Part 160 and Part 164, Subparts A and E (collectively, the "Privacy Rule"); and

VII. Both Parties intend to protect the privacy and provide for the security of Protected Health Information disclosed to or processed by Business Associate pursuant to the terms of this BAA, the Agreement, HIPAA, and other applicable laws.

AGREEMENT

NOW, THEREFORE, in consideration of the mutual covenants and conditions contained herein and the continued provision of PHI by Covered Entity to Business Associate under the Agreement in reliance on this BAA, the Parties agree as follows:

1. Definitions. For purposes of this BAA, the Parties give the following meaning to each of the terms in this Section 1 below. Any capitalized term used in this BAA, but not otherwise defined, has the meaning given to that term in the Privacy Rule, Security Rule, Breach Notification Rule, or other pertinent law.

A. "Affiliate" means a subsidiary or affiliate of Covered Entity that is, or has been, considered a covered entity, as defined by HIPAA.

B. "Breach" means the acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI, as defined in 45 CFR §164.402.

C. "Breach Notification Rule" means the portion of HIPAA set forth in Subpart D of 45 CFR Part 164.

D. "CriterionMD Services" means all current and future software, applications, browser-based tools, AI-enabled workflows, documentation review tools, medical-necessity and payer-policy support tools, coding support tools, customer support, implementation support, security monitoring, hosting, and related services provided by Business Associate under the Agreement, including Insurify and any successor, related, or additional CriterionMD product or module.

E. "Data Aggregation" means, with respect to PHI created or received by Business Associate in its capacity as the business associate under HIPAA of Covered Entity, the combining of such PHI by Business Associate with the PHI received by Business Associate in its capacity as a business associate of one or more other covered entities under HIPAA, to permit data analyses that relate to the Health Care Operations of the respective covered entities. The meaning of "data aggregation" in this BAA shall be consistent with the meaning given to that term in the Privacy Rule.

F. "Designated Record Set" has the meaning given to such term under the Privacy Rule, including 45 CFR §164.501.

G. "De-Identify" means to alter the PHI such that the resulting information meets the requirements described in 45 CFR §§164.514(a) and (b).

H. "Electronic PHI" means any PHI maintained in or transmitted by electronic media as defined in 45 CFR §160.103.

I. "Health Care Operations" has the meaning given to that term in 45 CFR §164.501.

J. "HHS" means the U.S. Department of Health and Human Services.

K. "HITECH Act" means the Health Information Technology for Economic and Clinical Health Act, enacted as part of the American Recovery and Reinvestment Act of 2009, Public Law 111-005.

L. "Individual" has the same meaning given to that term in 45 CFR §§164.501 and 160.103 and includes a person who qualifies as a personal representative in accordance with 45 CFR §164.502(g).

M. "Privacy Rule" means that portion of HIPAA set forth in 45 CFR Part 160 and Part 164, Subparts A and E.

N. "Protected Health Information" or "PHI" has the meaning given to the term "protected health information" in 45 CFR §§164.501 and 160.103, limited to the information created, received, maintained, transmitted, or otherwise processed by Business Associate from or on behalf of Covered Entity.

O. "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.

P. "Security Rule" means the Security Standards for the Protection of Electronic Health Information provided in 45 CFR Part 160 and Part 164, Subparts A and C.

Q. "Subcontractor" means a person or entity to whom Business Associate delegates a function, activity, or service, other than in the capacity of a member of Business Associate workforce, where the delegated function, activity, or service involves the creation, receipt, maintenance, transmission, or other processing of PHI.

R. "Unsecured Protected Health Information" or "Unsecured PHI" means any protected health information as defined in 45 CFR §§164.501 and 160.103 that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the HHS Secretary in guidance issued pursuant to the HITECH Act and codified at 42 USC §17932(h).

S. "User-Submitted Clinical Content" means clinical notes, patient history, examination findings, diagnosis information, procedure information, payer or insurance information, medical-necessity questions, prior-authorization-related information, documents, messages, prompts, attachments, or other content submitted to or processed through the CriterionMD Services by or on behalf of Covered Entity. User-Submitted Clinical Content shall be treated as PHI unless it has been De-Identified or otherwise falls outside the definition of PHI under HIPAA.

2. Use and Disclosure of PHI.

A. Except as otherwise provided in this BAA, Business Associate may use or disclose PHI as reasonably necessary to provide the CriterionMD Services described in the Agreement to Covered Entity, and to undertake other activities of Business Associate permitted or required by this BAA or as required by law.

B. Except as otherwise limited by this BAA or federal or state law, Covered Entity authorizes Business Associate to use the PHI in its possession for the proper management and administration of Business Associate business and to carry out its legal responsibilities. Business Associate may disclose PHI for its proper management and administration, provided that (i) the disclosures are required by law; or (ii) Business Associate obtains, in writing, prior to making any disclosure to a third party, (a) reasonable assurances from that third party that the PHI will be held confidential as provided under this BAA and used or further disclosed only as required by law or for the purpose for which it was disclosed to that third party and (b) an agreement from that third party to notify Business Associate promptly of any breach of the confidentiality of the PHI, to the extent it has knowledge of the breach.

C. Business Associate will not use or disclose PHI in a manner other than as provided in this BAA, as permitted under the Privacy Rule, or as required by law. Business Associate will use or disclose PHI, to the extent practicable, as a limited data set or limited to the minimum necessary amount of PHI to carry out the intended purpose of the use or disclosure, in accordance with Section 13405(b) of the HITECH Act (codified at 42 USC §17935(b)) and any implementing regulations adopted by HHS, for each use or disclosure of PHI.

D. Upon request, Business Associate will make available to Covered Entity any of Covered Entity PHI that Business Associate or any of its agents or subcontractors have in their possession, subject to Section 15.D and any limitations applicable to backup, archival, immutable security logs, or disaster recovery systems.

E. Business Associate may use PHI to report violations of law to appropriate federal and state authorities, consistent with 45 CFR §164.502(j)(1).

F. Business Associate may use and disclose PHI solely as necessary to provide, maintain, secure, monitor, troubleshoot, support, and improve the CriterionMD Services for Covered Entity, including: authenticating users; processing User-Submitted Clinical Content; generating medical-necessity, payer-policy, documentation-gap, clinical-decision-support, and coding-support outputs; providing customer support; maintaining audit logs; detecting, investigating, and preventing fraud, abuse, misuse, errors, downtime, and Security Incidents; performing quality assurance; and complying with law.

G. Business Associate will not sell PHI, use PHI for targeted advertising, use PHI to market third-party products or services to Individuals, or disclose PHI to data brokers. Business Associate will not use PHI to train, fine-tune, or improve any general-purpose artificial intelligence model or CriterionMD-hosted model. Information that has been De-Identified may be used as expressly permitted by Section 2.J.

H. Business Associate may use third-party AI, cloud, database, monitoring, logging, support, or infrastructure services only in accordance with this BAA and only where the service provider has entered into a written agreement imposing the same or substantially similar privacy and security obligations required by HIPAA and this BAA, to the extent such service provider creates, receives, maintains, transmits, or otherwise processes PHI.

I. Although CriterionMD may instruct users to avoid submitting direct patient identifiers when not necessary, Business Associate will treat all User-Submitted Clinical Content as PHI unless it has been De-Identified or is otherwise outside the definition of PHI under HIPAA. User instructions to redact identifiers do not reduce Business Associate obligations under this BAA.

J. Business Associate may De-Identify PHI in accordance with 45 CFR §§164.514(a) and (b). Business Associate may combine, use, and retain De-Identified or aggregated information for internal product analytics, benchmarking, payer-policy accuracy review, quality improvement, model and workflow evaluation, security improvement, and product development. Business Associate may publish or present aggregate findings provided that neither an Individual nor Covered Entity is reasonably identifiable and the underlying De-Identified dataset is not disclosed. Business Associate will not attempt to re-identify De-Identified information.

K. Unless expressly agreed otherwise in the Agreement, Business Associate does not act as Covered Entity system of record, electronic medical record, or legal medical record and does not independently determine medical necessity, payer coverage, or clinical appropriateness. Covered Entity remains responsible for clinical judgment, patient care, documentation, billing, coding, payer submissions, and compliance with payer and legal requirements. This Section does not limit Business Associate HIPAA obligations regarding PHI.

3. Safeguards Against Misuse of PHI. Business Associate will use appropriate safeguards to prevent the use or disclosure of PHI other than as provided by the Agreement or this BAA and Business Associate agrees to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Electronic PHI that it creates, receives, maintains, transmits, or otherwise processes on behalf of Covered Entity. Business Associate agrees to take reasonable steps, including providing adequate training to its workforce members, to ensure compliance with this BAA and to ensure that the actions or omissions of its workforce members, agents, or subcontractors do not cause Business Associate to breach the terms of this BAA.

A. Without limiting the generality of the foregoing, Business Associate security program for the CriterionMD Services shall include, as applicable and reasonable for the size, complexity, and risk profile of Business Associate operations: HIPAA security risk analysis and risk management; written privacy and security policies; workforce training; role-based access controls; least-privilege access; unique user identification; multi-factor authentication; encryption of Electronic PHI in transit and at rest where technically feasible; secure credential management; audit logging and monitoring; vulnerability

management; secure software development practices; backup and disaster recovery controls; incident response procedures; vendor and subcontractor risk management; and termination or access-revocation procedures for workforce members and contractors.

B. Business Associate will maintain reasonable technical and organizational measures designed to segregate PHI processed for Covered Entity from CriterionMD public marketing website systems and other systems that are not intended to process PHI. Covered Entity and its users should not submit PHI through public contact forms, public marketing pages, or non-HIPAA support channels unless Business Associate expressly designates the channel as approved for PHI.

C. Business Associate will maintain reasonable safeguards for logs, prompts, outputs, attachments, support tickets, screenshots, exports, and other artifacts that may contain PHI. Business Associate will use reasonable efforts to minimize PHI in diagnostic logs and monitoring tools while preserving information necessary for security, reliability, and support.

4. Reporting Disclosures of PHI and Security Incidents. Business Associate will report to Covered Entity in writing any use or disclosure of PHI not provided for by this BAA of which it becomes aware and any Security Incident affecting Electronic PHI of Covered Entity of which it becomes aware. Business Associate will report any such event without unreasonable delay and no later than fourteen (14) calendar days after becoming aware of the event. This Section does not require notice of unsuccessful, immaterial security events that do not result in unauthorized access, use, disclosure, modification, or destruction of PHI or material interference with systems containing PHI, including routine port scans, pings, unsuccessful login attempts, malware blocked by endpoint controls, or other routine events, provided such events are recorded and reviewed as appropriate by Business Associate.

5. Reporting Breaches of Unsecured PHI. Business Associate will notify Covered Entity in writing without unreasonable delay following discovery of any Breach of Unsecured PHI in accordance with 45 CFR §164.410, and in no case later than sixty (60) calendar days after discovery of the Breach. Business Associate will reimburse Covered Entity for reasonable costs incurred by Covered Entity in complying with Subpart D of 45 CFR Part 164 that are imposed on Covered Entity as a result of a Breach caused by Business Associate failure to comply with this BAA, subject to any limitations of liability in the Agreement to the extent such limitations are enforceable under applicable law and do not limit Business Associate obligations under HIPAA.

6. Mitigation of Disclosures of PHI. Business Associate will take reasonable measures to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of any use or disclosure of PHI by Business Associate or its agents or subcontractors in violation of the requirements of this BAA.

7. Agreements with Agents or Subcontractors. Business Associate will ensure that any agent or subcontractor that creates, receives, maintains, transmits, or otherwise processes PHI on behalf of Business Associate agrees in writing to restrictions, conditions, and safeguards that are the same as or substantially similar to those required by HIPAA and this BAA. Business Associate may add or replace subcontractors without Covered Entity prior approval, provided that Business Associate remains responsible for complying with this Section and gives Covered Entity commercially reasonable notice of a new subcontractor that may process PHI within thirty (30) calendar days after engagement, through a CriterionMD webpage or another written notice method.

A. Subcontractors may include, as applicable, hosting providers, cloud infrastructure providers, database providers, authentication providers, AI/model service providers, logging and monitoring tools, support ticketing systems, email or notification services, analytics services, backup/disaster recovery services, penetration testing or security vendors, and professional advisors, but only to the extent necessary to provide, secure, support, or improve the CriterionMD Services and only as permitted by this BAA and the Agreement.

B. Business Associate will maintain a current internal list of subcontractors that may create, receive, maintain, transmit, or otherwise process PHI for the CriterionMD Services and will make the list available to Covered Entity upon written request to legal@criterionmd.com. General security information may also be made available at criterionmd.com/security.

8. Audit Report and Security Documentation. Upon request, Business Associate will provide Covered Entity, or upstream Business Associate, with a copy of its most recent independent HIPAA compliance report (AT-C 315), SOC 2 report, HITRUST certification, penetration-test executive summary, or other mutually agreed upon independent standards-based third-party audit report, if available. If no such independent report is then available, Business Associate will provide a reasonable written summary of its HIPAA privacy and security program, risk analysis status, safeguards, and relevant security documentation, subject to reasonable confidentiality restrictions. Covered Entity agrees not to re-disclose Business Associate audit reports, security reports, risk analyses, penetration testing materials, or other confidential security documentation except as required by law.

9. Access to PHI by Individuals.

A. Upon request, Business Associate agrees to furnish Covered Entity with copies of the PHI maintained by Business Associate in a Designated Record Set in the time and manner designated by Covered Entity to enable Covered Entity to respond to an Individual request for access to PHI under 45 CFR §164.524. The Parties acknowledge that the CriterionMD Services are not intended to serve as Covered Entity designated record set unless expressly stated in the Agreement or unless Business Associate actually maintains PHI that forms part of a Designated Record Set.

B. In the event any Individual or personal representative requests access to the Individual PHI directly from Business Associate, Business Associate within ten business days will forward that request to Covered Entity. Any disclosure of, or decision not to disclose, the PHI requested by an Individual or a personal representative and compliance with the requirements applicable to an Individual right to obtain access to PHI shall be the sole responsibility of Covered Entity.

10. Amendment of PHI.

A. Upon request and instruction from Covered Entity, Business Associate will amend PHI or a record about an Individual in a Designated Record Set that is maintained by, or otherwise within the possession of, Business Associate as directed by Covered Entity in accordance with procedures established by 45 CFR §164.526. Any request by Covered Entity to amend such information will be completed by Business Associate within 15 business days of Covered Entity request.

B. In the event that any Individual requests that Business Associate amend such Individual PHI or record in a Designated Record Set, Business Associate within ten business days will forward this request to Covered Entity. Any amendment of, or decision not to amend, the PHI or record as requested by an Individual and compliance with the requirements applicable to an Individual right to request an amendment of PHI will be the sole responsibility of Covered Entity.

11. Accounting of Disclosures.

A. Business Associate will document any disclosures of PHI made by it to account for such disclosures as required by 45 CFR §164.528(a). Business Associate also will make available information related to such disclosures as would be required for Covered Entity to respond to a request for an accounting of disclosures in accordance with 45 CFR §164.528. At a minimum, Business Associate will furnish Covered Entity the following with respect to any covered disclosures by Business Associate: (i) the date of disclosure of PHI; (ii) the name of the entity or person who received PHI, and, if known, the address of such entity or person; (iii) a brief description of the PHI disclosed; and (iv) a brief statement of the purpose of the disclosure which includes the basis for such disclosure.

B. Business Associate will furnish to Covered Entity information collected in accordance with this Section 11 within ten business days after written request by Covered Entity, to permit Covered Entity to make an accounting of disclosures as required by 45 CFR §164.528, or in the event that Covered Entity elects to provide an Individual with a list of its business associates, Business Associate will provide an accounting of its disclosures of PHI upon request of the Individual, if and to the extent that such accounting is required under the HITECH Act or under HHS regulations adopted in connection with the HITECH Act.

C. In the event an Individual delivers the initial request for an accounting directly to Business Associate, Business Associate will within ten business days forward such request to Covered Entity.

12. Availability of Books and Records. Business Associate will make available its internal practices, books, agreements, records, and policies and procedures relating to the use and disclosure of PHI, upon request, to the Secretary of HHS for purposes of determining Covered Entity and Business Associate compliance with HIPAA and this BAA.

13. Responsibilities of Covered Entity. With regard to the use and/or disclosure of Protected Health Information by Business Associate, Covered Entity agrees to:

A. Notify Business Associate of any limitation(s) in its notice of privacy practices in accordance with 45 CFR §164.520, to the extent that such limitation may affect Business Associate use or disclosure of PHI.

B. 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 use or disclosure of PHI.

C. 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 that such restriction may affect Business Associate use or disclosure of PHI.

D. Except for data aggregation, De-Identification, or management and administrative activities of Business Associate as permitted by this BAA, Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under HIPAA if done by Covered Entity.

E. Use reasonable efforts to limit PHI submitted to the CriterionMD Services to the minimum necessary for the intended purpose, configure user access appropriately, maintain confidentiality of user credentials, promptly terminate access for workforce members no longer authorized to use the CriterionMD Services, and ensure that Covered Entity users follow Business Associate reasonable instructions regarding PHI submission channels and redaction of unnecessary direct identifiers.

F. Retain responsibility for the accuracy, completeness, and legal sufficiency of clinical documentation, payer submissions, prior authorization submissions, coding, billing, medical-necessity determinations, and patient care decisions, even when Covered Entity uses CriterionMD Services outputs as decision support.

14. Data Ownership. Business Associate data stewardship does not confer data ownership rights on Business Associate with respect to any PHI shared with it under the Agreement, including any and all forms thereof. Covered Entity retains ownership of PHI submitted by or on behalf of Covered Entity. Business Associate retains ownership of its software, workflows, algorithms, prompts, templates, payer-policy libraries, metadata structures, analytics methods, security tools, documentation, and other intellectual property, provided that Business Associate ownership rights do not grant Business Associate any right to use or disclose PHI except as permitted by this BAA and the Agreement. Business Associate may own and use De-Identified and aggregated information as provided in Section 2.J.

15. Term and Termination.

A. This BAA becomes effective on the date of the last signature below and continues in effect until all obligations of the Parties have been met under the Agreement and this BAA.

B. Covered Entity may terminate immediately this BAA, the Agreement, and any other related agreements if Covered Entity makes a determination that Business Associate has breached a material term of this BAA and Business Associate has failed to cure that material breach, to Covered Entity reasonable satisfaction, within 30 days after written notice from Covered Entity. Covered Entity may report the problem to the Secretary of HHS if termination is not feasible.

C. If Business Associate determines that Covered Entity has breached a material term of this BAA, then Business Associate will provide Covered Entity with written notice of the existence of the breach and shall provide Covered Entity with 30 days to cure the breach. Covered Entity failure to cure the breach within the 30-day period will be grounds for immediate termination of the Agreement and this BAA by Business Associate. Business Associate may report the breach to HHS.

D. Upon termination of the Agreement or this BAA for any reason, all PHI maintained by Business Associate will be returned to Covered Entity or destroyed by Business Associate, at Covered Entity direction, except that Business Associate may retain PHI as required by law, as necessary for legal defense, in routine backup or disaster recovery systems pending ordinary-course deletion, or where return or destruction is not feasible. Business Associate will not retain active production copies of such PHI except as permitted by this Section. This provision will apply to PHI in the possession of Business Associate agents and subcontractors. If return or destruction of the PHI is not feasible, in Business Associate reasonable judgment, Business Associate will furnish Covered Entity with notification, in writing, of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction of the PHI is infeasible, Business Associate will extend the protections of this BAA to such information for as long as Business Associate retains such information and will limit further uses and disclosures to those purposes that make the return or destruction of the information not feasible. The Parties understand that this Section 15.D will survive any termination of this BAA.

E. Business Associate may retain the original User-Submitted Clinical Content and the generated CriterionMD output for up to six (6) months from creation, unless an authorized user deletes the content earlier or retention is otherwise required by law. Authorized users may manually delete submitted content and outputs through available product functionality. Business Associate does not independently create or retain a replacement medical note as a separate legal medical-record document unless such content is expressly saved or submitted by an authorized user. Upon termination of the Agreement or a valid written deletion request, Business Associate will delete active production copies within thirty (30) calendar days, subject to Section 15.D. Backup, disaster-recovery, immutable security-log, and audit records may persist until ordinary-course rotation or deletion and will remain protected under this BAA while retained.

16. Effect of BAA.

A. This BAA is a part of and subject to the terms of the Agreement, except that to the extent any terms of this BAA conflict with any term of the Agreement, the terms of this BAA will govern with respect to the privacy, security, use, disclosure, retention, return, destruction, or other processing of PHI.

B. Except as expressly stated in this BAA or as provided by law, this BAA will not create any rights in favor of any third party.

17. Regulatory References. A reference in this BAA to a section in HIPAA means the section as in effect or as amended at the time.

18. Notices. All notices, requests, demands, and other communications under this BAA may be delivered by electronic mail to the applicable address below and will be effective when transmitted, provided the sender does not receive an automated failure or undeliverable notice. Either Party may also deliver notice by first-class mail, registered or certified mail, or express courier to the applicable mailing address below. A Party may update its notice information by written notice to the other Party.

A. If to Covered Entity, to:

Attn: _____

Address: _____

_____

E: _____

B. If to Business Associate, to:

Attn: Farhan Mustafa, Privacy and Security Officer

Address: 2248 Broadway

Suite 1981, New York, NY 10024

E: legal@criterionmd.com

19. Amendments and Waiver. This BAA may not be modified, nor will any provision be waived or amended, except in writing duly signed by authorized representatives of the Parties. A waiver with respect to one event shall not be construed as continuing, or as a bar to or waiver of any right or remedy as to subsequent events.

20. HITECH Act Compliance. The Parties acknowledge that the HITECH Act includes significant changes to the Privacy Rule and the Security Rule. The privacy subtitle of the HITECH Act sets forth provisions that significantly change the requirements for business associates and the agreements between business associates and covered entities under HIPAA, and these changes may be further clarified in regulations and guidance. Each Party agrees to comply with the applicable provisions of the HITECH Act and any HHS regulations issued with respect to the HITECH Act. The Parties also agree to negotiate in good faith to modify this BAA as reasonably necessary to comply with the HITECH Act and its regulations as they become effective, but in the event that the Parties are unable to reach agreement on such a modification, either Party will have the right to terminate this BAA upon 30 days prior written notice to the other Party.

21. Additional CriterionMD Service-Specific Terms.

A. Medical-Necessity and Payer-Policy Outputs. The CriterionMD Services may analyze clinical documentation and payer-policy materials to generate medical-necessity, prior-authorization, documentation-gap, and coding-support outputs. Such outputs may contain PHI and shall be protected under this BAA when created from, linked to, or maintained with PHI.

B. AI and Model Processing. The CriterionMD Services may use artificial intelligence, large language models, machine-learning models, retrieval systems, or similar technologies to process PHI. Current model services may include Anthropic HIPAA-eligible API services operating under an applicable business associate agreement and CriterionMD-hosted models. Business Associate will configure such technologies in a manner reasonably designed to protect PHI, prevent unauthorized retention or training by third-party model providers, and restrict access to PHI to the minimum necessary. Business Associate will not intentionally submit PHI to a third-party AI or model provider unless the provider has entered into an appropriate business associate or subcontractor agreement when required by HIPAA. Model providers may be added or replaced in accordance with Section 7.

C. Payer Policy Sources. Business Associate may retrieve, store, index, summarize, and display payer policies, medical policies, coverage criteria, local coverage determinations, national coverage determinations, and related materials. Such payer-policy materials generally are not PHI unless combined with, linked to, or generated from PHI.

D. Public Website Separation. CriterionMD public marketing website, blog, contact forms, demo-request pages, and non-authenticated webpages are not intended for PHI submission unless expressly labeled by Business Associate as HIPAA-approved channels. PHI submitted through unauthorized public website channels may create risk and should be reported promptly to Business Associate for mitigation.

E. Beta and Pilot Use. If Covered Entity uses CriterionMD Services in a beta, pilot, trial, or evaluation period, this BAA applies to PHI processed during the beta, pilot, trial, or evaluation period to the same extent as PHI processed during paid production use.

F. No Patient-Facing Portal. Unless expressly agreed otherwise, CriterionMD Services are not patient-facing portals and do not replace Covered Entity patient portal, medical records process, or HIPAA access obligations.

In light of the mutual agreement and understanding described above, the Parties execute this BAA, effective as of the date of the last signature below.

COVERED ENTITY

By: _____
Name: _____
Title: _____
Date: _____

BUSINESS ASSOCIATE

CriterionMD, Inc.

By: _____
Name: Farhan Mustafa
Title: Chief Executive Officer
Date: _____

EXHIBIT A

CriterionMD Services and Data Handling Summary

This Exhibit describes the expected CriterionMD Services and data-handling assumptions for purposes of the BAA. If this Exhibit conflicts with the BAA, the BAA controls with respect to PHI.

Item	CriterionMD information
Business Associate	CriterionMD, Inc., a Delaware corporation.
Primary product/service	All current and future CriterionMD products and modules provided under the Agreement, including Insurify and successor or related services for clinical-documentation review, payer medical-necessity criteria support, coding support, prior-authorization support, documentation-gap identification, and clinical-decision-support workflows.
Covered Entity users	Physicians, APPs, administrators, billing and coding staff, prior-authorization staff, and other workforce members or contractors authorized by Covered Entity.
Expected PHI categories	Patient notes, diagnoses, procedures, medication or injection requests, payer or insurance information, medical-necessity details, prior-authorization details, relevant history, examination, imaging summaries, and support communications that may contain PHI.
Redaction expectation	Users may be instructed to remove direct identifiers where not necessary. CriterionMD will treat submitted clinical content as PHI unless it has been De-Identified under HIPAA.
Storage assumption	CriterionMD stores the original user-submitted note or clinical content and the generated output. CriterionMD does not independently create or retain a replacement medical note as a separate legal medical-record document unless an authorized user expressly saves or submits it.
Retention period	Original user-submitted clinical content and generated outputs may be retained for up to six (6) months, unless deleted earlier by an authorized user or required longer by law. Active production copies will be deleted within thirty (30) calendar days after termination or a valid written deletion request, subject to backup, audit-log, legal, and technical exceptions described in the BAA.
Hosting/location	PHI is hosted and processed in United States environments. Current cloud, application, database, logging, monitoring, and other infrastructure details are maintained internally and are available upon written request, subject to reasonable confidentiality restrictions.
AI/model providers	Anthropic HIPAA-eligible API services operating under an applicable BAA and CriterionMD-hosted models. Third-party providers may be added or replaced in accordance with Section 7 and may not use PHI for unauthorized training or their own purposes.
Subprocessor list	CriterionMD maintains an internal current list and makes it available upon written request to legal@criterionmd.com. CriterionMD may provide notice of new PHI-processing subprocessors without customer preapproval as described in Section 7.
Security contact	Farhan Mustafa, Privacy and Security Officer — legal@criterionmd.com
Privacy contact	Farhan Mustafa, Privacy and Security Officer — legal@criterionmd.com