Business Associate Agreement

Version 3.1.0 — Effective upon electronic acceptance recorded in ForensicShield's audit log.

This copy is provided for review — share it with your attorney or compliance team before accepting. The agreement is executed electronically within the ForensicShield application; this document is not an executed instrument.

BUSINESS ASSOCIATE AGREEMENT

Effective Date: The date of electronic acceptance recorded in ForensicShield's audit log.

This Business Associate Agreement ("Agreement" or "BAA") is entered into by and between the organization accepting this Agreement ("Covered Entity") and ForensicShield LLC ("Business Associate"), collectively referred to as the "Parties."

RECITALS

WHEREAS, the Covered Entity is a healthcare provider or other entity subject to the Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health Act (collectively, "HIPAA");

WHEREAS, the Business Associate provides a software-as-a-service platform that analyzes forensic evaluation reports for courtroom defensibility, which requires the Business Associate to create, receive, maintain, or transmit Protected Health Information ("PHI") on behalf of the Covered Entity;

WHEREAS, the Parties wish to comply with the requirements of the HIPAA Privacy Rule (45 CFR Part 160 and Part 164, Subparts A and E), the HIPAA Security Rule (45 CFR Part 160 and Part 164, Subparts A and C), and the HIPAA Breach Notification Rule (45 CFR Part 164, Subpart D);

NOW, THEREFORE, in consideration of the mutual promises and covenants contained herein, the Parties agree as follows:

1. DEFINITIONS

Terms used but not otherwise defined in this Agreement shall have the same meaning as those terms in HIPAA, including but not limited to:

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

(b) "Designated Record Set" means a group of records maintained by or for a Covered Entity, as defined in 45 CFR 164.501.

(c) "Electronic Protected Health Information" or "ePHI" means PHI that is transmitted or maintained in electronic media, as defined in 45 CFR 160.103.

(d) "Protected Health Information" or "PHI" means individually identifiable health information transmitted or maintained in any form or medium, as defined in 45 CFR 160.103.

(e) "Required by Law" has the same meaning as the term "required by law" in 45 CFR 164.103.

(f) "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, as defined in 45 CFR 164.304.

(g) "Unsecured Protected Health Information" means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary of HHS, as defined in 45 CFR 164.402.

2. PERMITTED USES AND DISCLOSURES OF PHI

(a) The Business Associate may use or disclose PHI only as permitted or required by this Agreement or as Required by Law.

(b) The Business Associate is permitted to use and disclose PHI to perform the following functions, activities, and services ("Services") on behalf of the Covered Entity:
(i) Receiving, storing, and processing forensic evaluation reports containing PHI;
(ii) Performing AI-assisted analysis of reports for courtroom defensibility vulnerabilities;
(iii) Generating cross-examination preparation materials based on report content;
(iv) Verifying legal citations referenced in or relevant to the reports;
(v) Providing report comparison and portfolio analysis features; and
(vi) Maintaining audit logs and compliance records related to the above.

(c) The Business Associate may use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate, provided that:
(i) Such uses are necessary for the proper management and administration of the Business Associate; and
(ii) The disclosures are Required by Law, or the Business Associate obtains reasonable assurances from any person or entity 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 purpose for which it was disclosed, and the person or entity notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(d) The Business Associate may de-identify PHI in accordance with 45 CFR 164.514(a)-(c) and may use de-identified data for quality improvement, aggregate analytics, and service improvement purposes.

3. PROHIBITION ON UNAUTHORIZED USE OR DISCLOSURE

(a) The Business Associate shall not use or disclose PHI other than as permitted or required by this Agreement or as Required by Law.

(b) The Business Associate shall not use or disclose PHI in a manner that would violate Subpart E of 45 CFR Part 164 if done by the Covered Entity, except as expressly permitted in Section 2(c) and 2(d) above.

(c) The Business Associate shall not sell PHI as that term is defined in 45 CFR 164.502(a)(5)(ii).

(d) The Business Associate shall not use PHI for marketing purposes without the prior written authorization of the Covered Entity.

4. SAFEGUARDS

(a) The Business Associate shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of ePHI that it creates, receives, maintains, or transmits on behalf of the Covered Entity, as required by 45 CFR 164.306 and 45 CFR 164.314(a).

(b) Without limiting the generality of the foregoing, the Business Associate implements the following specific safeguards:
(i) Encryption: All PHI is encrypted at rest using AES-256-GCM with AWS Key Management Service (KMS) envelope encryption. Each data field containing PHI uses application-layer encryption before database storage.
(ii) Access Controls: Multi-factor authentication (MFA) is required for all users. Sessions time out after 15 minutes of inactivity. Role-based access controls restrict PHI access to authorized users within the Covered Entity's organization.
(iii) Audit Logging: All access to PHI is logged in an immutable, append-only audit log, including the identity of the accessor, the resource accessed, the action performed, and the timestamp.
(iv) Data Isolation: Multi-tenant data isolation is enforced at the application layer through organization scoping applied to every database query, verified by automated cross-organization isolation tests. PostgreSQL row-level security (RLS) policies are additionally defined on org-scoped tables as a forward-compatible second layer; because the application currently connects through a privileged database role that bypasses RLS, application-layer scoping is the operative enforcement mechanism. Each organization's data is logically separated so that no organization can access another's PHI.
(v) AI Processing: All AI inference is processed through AWS Bedrock within the AWS security boundary. PHI is not transmitted to any third-party AI provider outside the Business Associate's contracted AWS environment.
(vi) Transport Security: All data in transit is encrypted using TLS 1.2/1.3.
(vii) Malware Protection: All uploaded files are scanned for malware before processing.

5. REPORTING OF SECURITY INCIDENTS AND BREACHES

(a) The Business Associate shall report to the Covered Entity any Security Incident of which it becomes aware. The Business Associate shall report successful Security Incidents within five (5) business days of discovery. The Parties acknowledge that unsuccessful Security Incidents (such as pings, port scans, unsuccessful log-on attempts, or denial-of-service attacks) occur routinely and that no additional notice to the Covered Entity of such unsuccessful

incidents is required under this Agreement.

(b) The Business Associate shall report to the Covered Entity any Breach of Unsecured PHI without unreasonable delay and in no case later than thirty (30) calendar days after discovery of the Breach, as required by 45 CFR 164.410.

(c) The Business Associate's notification shall include, to the extent possible:
(i) The identification of each individual whose Unsecured PHI has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, used, or disclosed during the Breach;
(ii) A description of the nature of the Breach, including the types of Unsecured PHI involved;
(iii) A description of what the Business Associate is doing to investigate the Breach, mitigate harm, and protect against further Breaches; and
(iv) Contact information for the Business Associate, including a toll-free telephone number, e-mail address, postal address, or web address.

(d) The Business Associate shall cooperate with the Covered Entity in meeting the Covered Entity's obligations under 45 CFR 164.404 (notification to individuals) and 45 CFR 164.408 (notification to HHS).

6. SUBCONTRACTORS

(a) In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), the Business Associate shall ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate under this Agreement.

(b) The Business Associate currently uses the following subcontractors and subprocessors:
(i) Amazon Web Services (AWS) — cloud infrastructure, including RDS (database), S3 (file storage), KMS (encryption), SES (transactional email delivery — no PHI in message bodies), and Bedrock (AI inference). AWS processes ePHI and operates under a BAA with the Business Associate.
(ii) Clerk — authentication and identity management. Clerk processes user identity information (name, email) only. Clerk does not process clinical PHI.
(iii) Stripe — payment processing for subscription billing. Stripe processes payment and billing information only. Stripe does not receive, store, or process clinical PHI. Stripe is PCI-DSS Level 1 certified.
(iv) Sentry — error monitoring and application performance. Provisioned in code but not currently active in production (no DSN is configured); any future activation requires an executed Sentry BAA and the Business Associate's SENTRY_BAA_CONFIRMED configuration gate. The Business Associate implements server-side PHI scrubbing filters that remove identifiable health information before any error report would be transmitted. Sentry does not receive PHI.
(v) Mailchimp — marketing email communications. Mailchimp processes subscriber email addresses and names for marketing purposes only. Mailchimp does not receive clinical PHI.
(vi) CourtListener (Free Law Project) — case-law citation verification. Receives only case names, citations, and legal references; no PHI is included in lookup queries. Listed for transparency rather than as a PHI-handling subcontractor.
(vii) Cloudflare — DNS management and certificate DNS-validation only; not in the application data path (the CDN/edge is AWS CloudFront). Listed for transparency rather than as a PHI-handling subcontractor.

(c) The Business Associate shall maintain a current list of subcontractors and subprocessors that process PHI and shall make this list available to the Covered Entity upon request.

7. ACCESS TO PHI BY INDIVIDUALS

(a) To the extent the Business Associate maintains PHI in a Designated Record Set, the Business Associate shall, within fifteen (15) business days of a request from the Covered Entity, make available to the Covered Entity such PHI as is necessary for the Covered Entity to fulfill its obligations to provide individuals with access to their PHI under 45 CFR 164.524.

(b) The Business Associate provides a data export feature that allows the Covered Entity to download all PHI stored on the platform at any time, in compliance with the individual's right of access under HIPAA.

8. AMENDMENT OF PHI

(a) To the extent the Business Associate maintains PHI in a Designated Record Set, the Business Associate shall, within fifteen (15) business days of a request from the Covered Entity, make any amendments to PHI as directed by the Covered Entity pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy the Covered Entity's obligations under 45 CFR 164.526.

(b) The Covered Entity may modify case data and associated records through the platform's standard interface. The

Business Associate shall not independently modify PHI without instruction from the Covered Entity.

9. ACCOUNTING OF DISCLOSURES

(a) The Business Associate shall document disclosures of PHI and information related to such disclosures as would be required for the Covered Entity to respond to a request by an individual for an accounting of disclosures of PHI in accordance with 45 CFR 164.528.

(b) Within fifteen (15) business days of a request from the Covered Entity, the Business Associate shall provide to the Covered Entity information collected in accordance with this section to permit the Covered Entity to respond to a request by an individual for an accounting of disclosures.

(c) The Business Associate maintains a comprehensive audit log of all PHI access and disclosures, which serves as the basis for any accounting of disclosures.

10. AVAILABILITY OF BOOKS AND RECORDS

The Business Associate shall make its internal practices, books, and records relating to the use and disclosure of PHI available to the Secretary of the U.S. Department of Health and Human Services ("HHS") for purposes of determining compliance with HIPAA, as required by 45 CFR 164.504(e)(2)(ii)(I).

11. OBLIGATIONS OF COVERED ENTITY

(a) The Covered Entity shall notify the Business Associate of any limitations in the Covered Entity's notice of privacy practices under 45 CFR 164.520, to the extent that such limitation may affect the Business Associate's use or disclosure of PHI.

(b) The Covered Entity shall notify the Business Associate of any changes in, or revocation of, the permission by an individual to use or disclose their PHI, to the extent that such changes may affect the Business Associate's use or disclosure of PHI.

(c) The Covered Entity shall notify the Business Associate of any restriction on the use or disclosure of PHI that the Covered Entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect the Business Associate's use or disclosure of PHI.

(d) The Covered Entity warrants that it has obtained any necessary authorizations, consents, or other permissions required under applicable law for the disclosure of PHI to the Business Associate for the purposes described in this Agreement.

12. TERM AND TERMINATION

(a) Term. This Agreement shall be effective as of the date of electronic acceptance and shall terminate when all PHI provided by the Covered Entity to the Business Associate, or created or received by the Business Associate on behalf of the Covered Entity, is destroyed or returned to the Covered Entity, or, if it is infeasible to return or destroy PHI, protections are extended to such information in accordance with Section 12(e) below.

(b) Termination for Cause. Upon the Covered Entity's knowledge of a material breach of this Agreement by the Business Associate, the Covered Entity shall provide an opportunity for the Business Associate to cure the breach or end the violation within thirty (30) calendar days. If the Business Associate does not cure the breach or end the violation within the specified time period, the Covered Entity may terminate this Agreement and the underlying service agreement.

(c) Termination by Business Associate. Upon the Business Associate's knowledge of a material breach of this Agreement by the Covered Entity, the Business Associate shall provide an opportunity for the Covered Entity to cure the breach or end the violation within thirty (30) calendar days. If the Covered Entity does not cure the breach or end the violation within the specified time period, the Business Associate may terminate this Agreement and the underlying service agreement.

(d) Obligations on Termination. Upon termination of this Agreement for any reason, the Business Associate shall:
(i) Return or destroy all PHI received from the Covered Entity, or created, maintained, or received by the Business Associate on behalf of the Covered Entity, within thirty (30) calendar days of termination. This includes deleting all database records, uploaded files, and associated metadata. Encrypted backups will expire per the Business Associate's standard retention schedule (not to exceed ninety (90) calendar days after termination). Audit log entries will be retained for the HIPAA-required period (six (6) years from the date of creation) but will be anonymized to remove identifying information.
(ii) The Business Associate shall not retain any copies of PHI except as necessary for compliance with applicable law, including HIPAA's record retention requirements.

(e) Survival. If return or destruction of PHI is infeasible, the Business Associate shall extend the protections of this Agreement to the PHI and limit further uses and disclosures to those purposes that make return or destruction infeasible, for as long as the Business Associate retains the PHI.

13. LIMITATION OF LIABILITY

(a) TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, NEITHER PARTY SHALL BE LIABLE TO THE OTHER PARTY FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES ARISING OUT OF OR RELATING TO THIS AGREEMENT, INCLUDING BUT NOT LIMITED TO LOSS OF PROFITS, REVENUE, DATA, USE, OR GOODWILL, REGARDLESS OF THE THEORY OF LIABILITY AND EVEN IF THE PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

(b) EXCEPT FOR A PARTY'S BREACH OF ITS OBLIGATIONS UNDER SECTIONS 3 (PROHIBITION ON UNAUTHORIZED USE OR DISCLOSURE) OR 5 (REPORTING OF SECURITY INCIDENTS AND BREACHES), THE TOTAL AGGREGATE LIABILITY OF EITHER PARTY UNDER THIS AGREEMENT SHALL NOT EXCEED THE TOTAL FEES PAID BY THE COVERED ENTITY TO THE BUSINESS ASSOCIATE DURING THE TWELVE (12) MONTHS PRECEDING THE EVENT GIVING RISE TO THE CLAIM.

(c) Nothing in this Section shall limit either Party's liability for willful misconduct, gross negligence, or violations of applicable law, including HIPAA.

14. INDEMNIFICATION

(a) Each Party (the "Indemnifying Party") shall indemnify, defend, and hold harmless the other Party and its officers, directors, employees, and agents (the "Indemnified Party") from and against any third-party claims, damages, losses, liabilities, and reasonable expenses (including attorneys' fees) arising from the Indemnifying Party's material breach of this Agreement or its obligations under HIPAA, provided that such breach directly caused the damages at issue.

(b) The Indemnified Party shall promptly notify the Indemnifying Party in writing of any claim for which indemnification is sought and shall cooperate with the Indemnifying Party in the defense of such claim. Failure to provide prompt notice shall not relieve the Indemnifying Party of its obligation except to the extent such failure materially prejudices its ability to defend.

15. DISPUTE RESOLUTION

(a) Informal Resolution. Before initiating any formal proceeding, the Parties agree to first attempt to resolve any dispute arising under this Agreement through good-faith negotiation for a period of at least thirty (30) calendar days. Notices shall be directed to the contact information provided during account registration or to legal@forensicshield.net.

(b) Governing Law. This Agreement shall be governed by and construed in accordance with federal law, including HIPAA. To the extent that state law applies, the laws of the State of Georgia shall govern, without regard to conflict-of-law principles.

(c) Jurisdiction. Any disputes arising under this Agreement that cannot be resolved through informal negotiation shall be resolved exclusively in the state or federal courts located in the State of Georgia. Both Parties consent to the personal jurisdiction of such courts.

16. MISCELLANEOUS

(a) Regulatory References. A reference in this Agreement to a section in HIPAA means the section as in effect or as amended from time to time.

(b) Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with HIPAA and its implementing regulations. The Business Associate may update this Agreement by publishing a new version on the platform and requiring re-acceptance. The new version's effective date, version number, and cryptographic hash will be recorded in the audit log upon acceptance.

(c) Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with HIPAA.

(d) No Third-Party Beneficiaries. Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than the Covered Entity, the Business Associate, and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.

(e) Entire Agreement. This Agreement constitutes the complete agreement between the Parties with respect to the subject matter hereof and supersedes all prior agreements and understandings, whether written or oral, relating to its subject matter. This Agreement is supplemental to the ForensicShield Terms of Service and Privacy Policy, and all

three documents together govern the relationship between the Parties.

(f) Severability. If any provision of this Agreement is found to be invalid or unenforceable, the remaining provisions shall continue in full force and effect.

(g) Notices. Any notices required or permitted under this Agreement shall be sent to the contact information provided during account registration or to legal@forensicshield.net.