BUSINESS ASSOCIATE AGREEMENT

(HIPAA Subcontractor Business Associate Agreement)

between

_____ ("Representative")

and

Catalyst MedTech LLC, a Texas limited liability company, dba CaseClose ("CaseClose")

Effective Date: _____, 20____

This Business Associate Agreement is intended to be read together with the Master Subscription Agreement, HIPAA Security Addendum, and Data Processing Addendum between the same parties. In the event of a conflict specifically concerning the handling of Protected Health Information, this Agreement controls.

Table of Contents

Recitals

1. Definitions

2. Purpose and Scope

3. Permitted Uses and Disclosures

4. Responsibilities of CaseClose

5. Responsibilities of the Representative/Customer

6. Safeguards Required by HIPAA

7. AI Processing Provisions

8. Email Transmission Requirements

9. Security Incident and Breach Notification

10. Subcontractors

11. Audit Rights

12. Data Retention and Destruction

13. Term and Termination

14. Indemnification

15. Limitation of Liability

16. Miscellaneous

Exhibit A — Description of Services

Exhibit B — Security Controls

Exhibit C — Approved Subprocessors

Signature Page

Recitals

This Business Associate Agreement ("Agreement") is entered into as of the Effective Date between **Representative (as identified on the signature page) ("Representative")** and **Catalyst MedTech LLC, a Texas limited liability company, dba CaseClose ("CaseClose")**.

WHEREAS, Representative provides sales and case-support services to hospitals and other healthcare providers (each, a "Covered Entity") and holds a direct business associate agreement with each such Covered Entity (each, an "Upstream BAA") governing Representative's creation, receipt, maintenance, and transmission of Protected Health Information on that Covered Entity's behalf;

WHEREAS, Representative uses the CaseClose mobile application and backend services (the "Services") to capture and process surgical case sheets, track implant/device inventory, and generate and transmit restock and billing communications, and in doing so discloses Protected Health Information to CaseClose for creation, receipt, maintenance, and transmission on Representative's behalf;

WHEREAS, under 45 C.F.R. § 160.103 and the HIPAA Omnibus Rule, a person that creates, receives, maintains, or transmits PHI on behalf of a business associate is itself a subcontractor business associate, and CaseClose is such a subcontractor of Representative;

NOW, THEREFORE, the parties agree as follows:

1. Definitions

Capitalized terms not otherwise defined here have the meanings given in the HIPAA Rules (defined below); in a conflict, the HIPAA Rules control.

1.1 "Agreement" means this Business Associate Agreement, including all Exhibits, as amended from time to time.

1.2 "Breach" has the meaning given in 45 C.F.R. § 164.402.

1.3 "Business Associate" / "Subcontractor" has the meaning given in 45 C.F.R. § 160.103; CaseClose is a subcontractor business associate of Representative and these terms refer to CaseClose in that capacity.

1.4 "Case-Sheet Data" means the photograph(s) of a surgical case sheet or implant log captured through the Services, and all data extracted from those photographs, including patient identifiers, hospital/surgeon identifiers, device/lot/serial numbers, procedure information, and pricing.

1.5 "Covered Entity" has the meaning given in 45 C.F.R. § 160.103, and refers to the hospital(s) or other healthcare provider(s) with which Representative has a direct business associate relationship and Upstream BAA.

1.6 "Designated Record Set" has the meaning given in 45 C.F.R. § 164.501.

1.7 "ePHI" has the meaning given in 45 C.F.R. § 160.103, and includes all PHI processed through the Services.

1.8 "HIPAA Rules" means the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Parts 160 and 164, as amended by HITECH and the Omnibus Rule.

1.9 "Minimum Necessary" means the standard at 45 C.F.R. § 164.502(b) and § 164.514(d).

1.10 "OCR Extraction" means the automated process by which the Services use AI/ML models, accessed through the Bedrock Environment (Section 7), to extract structured data from Case-Sheet Data.

1.11 "PHI" has the meaning given in 45 C.F.R. § 160.103, limited to information CaseClose creates, receives, maintains, or transmits on Representative's behalf, including Case-Sheet Data.

1.12 "Representative" / "Customer" means the individual or entity identified on the signature page, an independent contractor sales representative and business associate of one or more Covered Entities who uses the Services in that capacity. The terms "Representative" and "Customer" are used interchangeably in this Agreement and in the related Master Subscription Agreement.

1.13 "Required by Law" has the meaning given in 45 C.F.R. § 164.103.

1.14 "Secretary" means the Secretary of the U.S. Department of Health and Human Services or designee.

1.15 "Security Incident" has the meaning given in 45 C.F.R. § 164.304.

1.16 "Services" means the CaseClose mobile application and backend infrastructure described in Exhibit A.

1.17 "Subprocessor" means any third party engaged by CaseClose to create, receive, maintain, process, or transmit PHI in connection with the Services, including those listed in Exhibit C.

1.18 "Unsecured PHI" has the meaning given in 45 C.F.R. § 164.402.

1.19 "Upstream BAA" means the business associate agreement directly between Representative and a Covered Entity referenced in the Recitals.

1.20 "Bedrock Environment" means the AWS Bedrock service environment, or any successor server-side AI processing environment adopted under Section 7.6, through which OCR Extraction is performed.

2. Purpose and Scope

2.1 This Agreement satisfies the subcontractor business associate agreement requirements of 45 C.F.R. §§ 164.308(b)(2), 164.314(a)(2)(iii), and 164.504(e), and is the exclusive chain-of-trust agreement between Representative and CaseClose with respect to PHI processed through the Services.

2.2 The parties acknowledge that Representative, not CaseClose, holds the direct relationship and Upstream BAA with each Covered Entity, and that CaseClose's obligations to any Covered Entity, if any, run solely through Representative and this Agreement, except to the extent applicable law independently imposes direct obligations on subcontractors.

2.3 This Agreement governs PHI handling only. It does not itself establish or modify the commercial, subscription, fee, or licensing terms between the parties, which are governed by the Master Subscription Agreement ("MSA") between the same parties. In the event of a conflict specifically concerning PHI, this Agreement controls over the MSA and any other agreement between the parties, including the Data Processing Addendum, to the extent the Data Processing Addendum addresses PHI.

2.4 This Agreement applies to all PHI that CaseClose creates, receives, maintains, or transmits on Representative's behalf in connection with the Services, regardless of the specific Covered Entity to which the PHI relates, unless a specific Covered Entity's Upstream BAA imposes additional requirements of which Representative has notified CaseClose in writing under Section 5.3.

3. Permitted Uses and Disclosures

3.1 Permitted Uses and Disclosures Generally

Except as otherwise limited in this Agreement, CaseClose may use and disclose PHI to perform the Services on behalf of Representative, provided that such use or disclosure would not violate the HIPAA Rules if done by Representative, or the Minimum Necessary policies of Representative or the applicable Covered Entity of which CaseClose has been made aware in writing.

3.2 Enumerated Permitted Uses

3.2.1 To capture, store, and process Case-Sheet Data, including OCR Extraction, to populate case records within the Services.

3.2.2 To track implant/device inventory associated with a case for restock communications.

3.2.3 To generate and transmit restock and billing communications through Representative's own connected email account (Section 8).

3.2.4 To generate case-sheet PDFs and related billing/restock documentation for transmission to the manufacturer, distributor, hospital billing contact, or other recipient designated by Representative in the ordinary course of a case.

3.2.5 To maintain case history, send logs, and audit trails for Representative's own reference and correction workflow.

3.2.6 For CaseClose's proper management and administration or to carry out CaseClose's legal responsibilities, subject to the third-party confidentiality/notification assurances required by 45 C.F.R. § 164.504(e)(4).

3.2.7 For data aggregation services relating to Representative's operations, if requested in writing by Representative, per 45 C.F.R. § 164.504(e)(2)(i)(B).

3.2.8 To report violations of law to appropriate authorities, consistent with 45 C.F.R. § 164.502(j)(1).

3.3 Prohibited Uses and Disclosures

CaseClose shall not, and shall not permit any Subprocessor to:

- Use or disclose PHI in a manner that would violate the HIPAA Rules if done by Representative, except for the limited purposes in Sections 3.2.6 and 3.2.7.
- Sell PHI, as defined at 45 C.F.R. § 164.502(a)(5)(ii), without prior written authorization.
- Use PHI for marketing purposes without the authorization required by 45 C.F.R. § 164.508.
- Use or disclose PHI to train, fine-tune, or otherwise improve any general-purpose or third-party AI/ML model outside the scope of performing OCR Extraction for the specific case to which the data relates, except in de-identified form meeting 45 C.F.R. § 164.514(a)-(c).

- De-identify PHI except in accordance with 45 C.F.R. § 164.514(a)-(c), and not use de-identified data to re-identify any individual.
- Disclose PHI to any law enforcement, immigration, or other governmental authority except as Required by Law, under Section 11, or with Representative's prior written consent.

4. Responsibilities of CaseClose

4.1 General Compliance

4.1.1 CaseClose shall not use or disclose PHI other than as permitted or required by this Agreement or as Required by Law.

4.1.2 CaseClose shall implement appropriate safeguards, and comply with the Security Rule (45 C.F.R. Part 164, Subpart C) with respect to ePHI, as detailed in Section 6.

4.1.3 CaseClose shall report to Representative any use or disclosure of PHI not provided for by this Agreement, including any Security Incident or Breach, per Section 9.

4.1.4 CaseClose shall comply, to the extent it carries out an obligation of Representative under the Privacy Rule, with the requirements of 45 C.F.R. Part 164, Subpart E applicable to Representative in performing that obligation.

4.2 Access, Amendment, and Accounting

4.2.1 Upon written request, CaseClose shall make PHI in a Designated Record Set available to Representative within ten (10) business days, so Representative can meet its obligations under 45 C.F.R. § 164.524.

4.2.2 CaseClose shall make requested amendments to PHI in a Designated Record Set within ten (10) business days, per 45 C.F.R. § 164.526.

4.2.3 CaseClose shall maintain and provide, within ten (10) business days of request, the information needed for an accounting of disclosures under 45 C.F.R. § 164.528.

4.3 Government and Regulator Access

4.3.1 CaseClose shall make its internal practices, books, and records relating to PHI available to Representative or the Secretary, in a time and manner reasonably requested, to determine HIPAA compliance.

4.4 Minimum Necessary

4.4.1 CaseClose shall request, use, and disclose only the minimum PHI necessary to accomplish the intended purpose.

5. Responsibilities of the Representative/Customer

5.1 Independent Contractor Status

5.1.1 Representative is an independent contractor, not an employee, partner, or agent of CaseClose. This Agreement addresses PHI obligations only and does not itself establish engagement, compensation, or commercial terms, which are governed by the MSA and any separate agreements between Representative and third parties (hospitals, manufacturers, distributors).

5.2 Representative's Covered Entity Relationships

5.2.1 Representative represents and warrants that it holds a direct, currently effective Upstream BAA with each Covered Entity for which it uses the Services to process PHI, and that it is authorized under each such Upstream BAA to engage subcontractors, including CaseClose, subject to Section 5.2.2.

5.2.2 Before first using the Services to process PHI relating to a given Covered Entity, Representative shall confirm whether that Covered Entity's Upstream BAA requires prior written approval before subcontracting PHI-handling to a new vendor, and, if so, shall obtain that approval before doing so. Representative shall promptly notify CaseClose in writing if a Covered Entity restricts or revokes Representative's authorization to use CaseClose, and CaseClose shall cease processing that Covered Entity's PHI upon notice.

5.3 Notice of Heightened Requirements

5.3.1 If a specific Covered Entity's Upstream BAA imposes obligations more stringent than this Agreement (for example, a shorter breach-notification window or a longer retention period), Representative shall notify CaseClose of the specific heightened term in writing, and CaseClose shall comply with that heightened term with respect to that Covered Entity's PHI going forward, subject to good-faith discussion of any operational impact.

5.4 Representative's Own Compliance Obligations

5.4.1 Nothing in this Agreement relieves Representative of its own obligations under the HIPAA Rules or any Upstream BAA, including using PHI only as permitted by the applicable Covered Entity, obtaining any required patient authorization, and independently evaluating whether use of the Services is consistent with Representative's own compliance obligations.

5.5 Data Accuracy

5.5.1 Representative is responsible for reviewing, correcting, and confirming case data (including OCR-extracted data) before it is finalized, sent, or billed, consistent with Section 7.4.

5.6 Multiple Representatives / Onboarding

5.6.1 This Agreement is intended to be executed in substantially the same form with each Representative/Customer who uses the Services, once at onboarding. CaseClose may make immaterial administrative updates to the form for future signers without affecting Representatives who already executed a prior form; any change to Sections 1–13 or 14/15 shall require thirty (30) days' written notice and an opportunity to object under Section 16.5.

6. Safeguards Required by HIPAA

6.1 General Security Rule Compliance

CaseClose shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of ePHI, consistent with 45 C.F.R. §§ 164.308, 164.310, and 164.312, and as further detailed in the HIPAA Security Addendum and Exhibit B.

6.2 Encryption

6.2.1 All ePHI in transit between the CaseClose mobile application, CaseClose's backend, and any Subprocessor shall be encrypted using TLS 1.2 or higher.

6.2.2 All ePHI at rest — case-sheet photographs, extracted case data, generated PDFs, and logs — shall be encrypted using AES-256 or stronger, with database-level encryption enabled from creation of the data store.

6.2.3 Encryption keys shall be managed through a dedicated key-management service and shall not be embedded in client-side application code.

6.3 Access Controls

6.3.1 CaseClose shall implement real, individual per-Representative authentication, and role/row-level access restrictions limiting each Representative to that Representative's own case data absent a legitimate administrative or support need.

6.3.2 CaseClose personnel access to production PHI systems shall be limited to individuals with a legitimate operational need, using unique credentials and, where supported, multi-factor authentication.

6.4 Workforce Security and Training

6.4.1 CaseClose shall implement a sanctions policy for workforce members who violate CaseClose's security policies, and shall provide periodic HIPAA/security training to workforce members with PHI access.

6.5 Physical Safeguards

6.5.1 Because CaseClose's infrastructure is hosted on third-party cloud platforms, physical security is provided by those platforms under their respective BAAs and industry-standard certifications; CaseClose shall not maintain PHI on any on-premises server not covered by such a BAA.

6.6 Device and Application Security

6.6.1 The CaseClose mobile application shall not store PHI in unencrypted local storage beyond what is technically necessary; any locally cached PHI shall be encrypted at rest on the device and cleared upon logout or reasonable inactivity.

6.6.2 CaseClose shall maintain a documented process for evaluating and remediating known vulnerabilities in the Services, including third-party dependencies, on a reasonable periodic basis.

7. AI Processing Provisions

7.1 Description of AI Processing

The Services use OCR Extraction to convert a photograph of a case sheet, implant log, or similar source document into structured case data (patient identifiers, hospital, surgeon, device/lot/serial numbers, procedure type, pricing). OCR Extraction is performed by a large language model accessed exclusively through the Bedrock Environment, and not through any direct, client-side, or public-internet call to a third-party AI API outside CaseClose's HIPAA-eligible processing boundary.

7.2 No Training on PHI

7.2.1 CaseClose shall not use, and shall contractually prohibit its AI Subprocessor from using, any PHI processed through OCR Extraction to train, fine-tune, evaluate, or otherwise improve any AI/ML model made available to any party other than CaseClose in connection with the Services.

7.2.2 CaseClose represents that, as of the Effective Date, its AI Subprocessor's standard commercial terms for the Bedrock Environment provide that customer content submitted through the API is not used to train underlying foundation models, and shall promptly notify Representative in writing if this ceases to be true.

7.3 Transient Processing and Data Minimization

7.3.1 The case-sheet image and extracted data are transmitted to the Bedrock Environment solely to perform the extraction for the specific case being captured, and are not retained by the AI Subprocessor beyond the time reasonably necessary to complete and return the extraction and satisfy any short-term abuse-monitoring window offered under the AI Subprocessor's own BAA.

7.3.2 Extracted structured data and the underlying case-sheet photograph shall be stored only in CaseClose's encrypted backend, subject to Section 12.

7.4 Human Review and Accuracy

7.4.1 OCR Extraction is a data-entry aid, not a substitute for Representative's own review. The Services present all extracted fields to Representative for review, correction, and confirmation before a case is finalized, sent, or billed.

7.4.2 CaseClose shall maintain reasonable technical controls so that OCR Extraction output is clearly editable/correctable and is not automatically transmitted to any third party without an intervening Representative review-and-send action, except for internal storage within the Services.

7.5 AWS Bedrock — HIPAA-Eligible Service

7.5.1 CaseClose represents that Amazon Web Services ("AWS") and Amazon Bedrock are covered under a HIPAA Business Associate Addendum executed via AWS Artifact, and that Bedrock appears on

AWS's list of HIPAA-eligible services. CaseClose shall maintain this BAA for as long as Bedrock is used to process PHI and shall promptly notify Representative if it lapses.

7.5.2 All calls to the Bedrock Environment shall originate from CaseClose's backend, not from the mobile application directly; no AI API key or credential capable of submitting PHI to an AI model shall be embedded in the mobile application binary.

7.5.3 PHI submitted to the Bedrock Environment shall be encrypted in transit (TLS 1.2+) and remain within AWS's HIPAA-eligible boundary; CaseClose shall not route PHI through any non-HIPAA-eligible AWS service or through a public consumer AI API.

7.5.4 CaseClose shall process PHI through the Bedrock Environment using U.S.-based AWS region(s) only, and shall not enable cross-border inference routing for PHI without Representative's prior written consent.

7.6 Model or Provider Changes

7.6.1 CaseClose shall provide at least thirty (30) days' advance written notice before materially changing the AI model, model provider, or processing architecture used for OCR Extraction, other than routine version upgrades within the same HIPAA-eligible boundary, and shall confirm any replacement is bound by a BAA meeting Section 10 before PHI is processed through it.

8. Email Transmission Requirements

8.1 Representative's Own Business Email Account

The Services allow Representative to connect Representative's own Google Workspace or Microsoft 365 business email account via OAuth (Gmail API "gmail.send" scope or Microsoft Graph API "Mail.Send" scope), so restock/billing communications are transmitted from Representative's own authenticated business address rather than a shared or CaseClose-controlled account.

8.2 Representative's Obligations

8.2.1 Representative represents that any email account it connects is a paid, business-tier Google Workspace or Microsoft 365 account for which an appropriate BAA is maintained directly with Google LLC or Microsoft Corporation, as applicable.

8.2.2 Representative shall not connect a personal, free-tier account (including @gmail.com, @outlook.com, or @hotmail.com) to send PHI-containing communications, and acknowledges a personal account cannot carry a BAA regardless of authentication method.

8.3 CaseClose's Obligations

8.3.1 CaseClose shall implement a reasonable technical control at connection time to detect and reject known personal-tier consumer email domains, as a compliance aid that does not relieve Representative of Section 8.2.1.

8.3.2 CaseClose shall store Representative's OAuth refresh token(s) in encrypted form, accessible only to the backend process(es) that send email on Representative's behalf, and shall use the connected account only for communications initiated by Representative through the Services.

8.3.3 CaseClose shall support both Google Workspace and Microsoft 365 and shall not require a CaseClose-provisioned or CaseClose-paid email account or license.

8.3.4 CaseClose shall allow Representative to disconnect a connected email account at any time, immediately revoking CaseClose's stored token.

8.4 Scope of BAA Coverage for Email

The BAA covering a Representative's connected email account is between Representative's own organization and Google or Microsoft; CaseClose is not a party to, and assumes no obligation under, that agreement. This Agreement governs CaseClose's handling of the OAuth token and its role in initiating transmission; Representative remains independently responsible for maintaining the underlying provider BAA.

8.5 Google Sensitive-Scope Verification

8.5.1 CaseClose shall pursue and maintain any Google security assessment required to request the "gmail.send" scope from external Workspace accounts once required by user count, and shall notify Representative of any material change in Gmail connectivity resulting from that process.

9. Security Incident and Breach Notification

9.1 Notification of Security Incidents

9.1.1 CaseClose shall report to Representative, without unreasonable delay and in no event later than five (5) business days after discovery, any Security Incident of which it becomes aware, whether or not it resulted in a Breach. This Section 9.1 constitutes CaseClose's standing notice under 45 C.F.R. § 164.314(a)(2)(i)(C) of routine, unsuccessful, immaterial attempted intrusions common to internet-connected systems, for which no further notice of each individual occurrence is required, provided CaseClose shall report any attempt it reasonably believes may indicate a targeted or successful compromise.

9.2 Notification of Breach

9.2.1 CaseClose shall notify Representative in writing of any Breach of Unsecured PHI without unreasonable delay, and in no event later than thirty (30) calendar days after discovery (as defined at 45 C.F.R. § 164.410), notwithstanding that the HITECH Act permits up to sixty (60) days; the shorter internal target preserves Representative's time to meet its own notification obligations to the affected Covered Entity within the outer sixty (60) day statutory limit.

9.2.2 Notification shall include, to the extent known and supplemented as information develops: what happened and when; the types of Unsecured PHI involved; identities (or number/type) of affected individuals; recommended steps for individuals; CaseClose's investigation, mitigation, and remediation actions; and contact information for a CaseClose representative.

9.3 Mitigation

9.3.1 CaseClose shall mitigate, to the extent practicable, any harmful effect known to it of a use or disclosure of PHI in violation of this Agreement.

9.4 Cooperation and Costs

9.4.1 CaseClose shall reasonably cooperate with Representative and, through Representative, any affected Covered Entity in investigating a Breach and preparing required notifications under 45 C.F.R. §§ 164.404–164.408.

9.4.2 As between the parties, CaseClose shall bear the reasonable direct costs of notifying individuals, the Secretary, and (if applicable) the media of a Breach caused by CaseClose's or a Subprocessor's acts or omissions, including reasonable state-law-required credit monitoring costs, without limiting Representative's remedies under Sections 14 and 15.

10. Subcontractors

10.1 Omnibus Chain-of-Trust Acknowledgment

The parties acknowledge that, under the HIPAA Omnibus Rule's amendment to the definition of "business associate" at 45 C.F.R. § 160.103, the BAA requirement extends down the contracting chain to any subcontractor that creates, receives, maintains, or transmits PHI on behalf of a business associate, regardless of privity with the covered entity. CaseClose is such a subcontractor with respect to Representative, and this Agreement is the written contract required by 45 C.F.R. §§ 164.308(b)(2), 164.314(a)(2)(iii), and 164.502(e)(1)(ii).

10.2 CaseClose's Own Subcontractors

10.2.1 Under 45 C.F.R. §§ 164.308(b)(2) and 164.502(e)(1)(ii), CaseClose shall ensure that any Subprocessor that creates, receives, maintains, or transmits PHI on CaseClose's behalf agrees, in writing, to restrictions and conditions at least as stringent as those applicable to CaseClose under this Agreement.

10.2.2 As of the Effective Date, CaseClose's primary backend (database, authentication, encrypted file storage, audit logging) is hosted on Supabase under Supabase's Team plan with HIPAA add-on, pursuant to a BAA between CaseClose and Supabase. AWS Bedrock is used for OCR Extraction regardless of the underlying database platform, because Supabase does not itself provide AI extraction; both Supabase and AWS are Subprocessors independently subject to this Section 10.

10.2.3 CaseClose shall maintain and, upon written request (no more than once per calendar year absent a Security Incident or Breach), make available to Representative the current Subprocessor list in Exhibit C, together with confirmation of each Subprocessor's applicable BAA or equivalent assurance.

10.3 Changes to Subcontractors

10.3.1 CaseClose shall provide at least thirty (30) days' advance written notice (email to Representative's address of record is sufficient) before engaging a new Subprocessor that will handle PHI, or materially changing an existing Subprocessor's role, and shall update Exhibit C accordingly.

10.3.2 If Representative reasonably objects in writing within fifteen (15) days based on a good-faith compliance or security concern, the parties shall discuss in good faith; if unresolved after a further fifteen (15) days, either party may treat the objection as grounds for termination under Section 13.3 as to the affected functionality, or the whole Agreement if not reasonably severable.

10.4 Liability for Subcontractor Acts

10.4.1 CaseClose remains fully responsible for the acts and omissions of its Subprocessors with respect to PHI to the same extent as if CaseClose had performed the function directly.

11. Audit Rights

11.1 Audit Logging

11.1.1 CaseClose shall maintain audit logs sufficient to identify, for each item of PHI: the identity of the user or process that created, accessed, modified, or transmitted it; date and time; the nature of the action; and, for transmissions, the destination or recipient system.

11.1.2 Audit logs shall be retained not less than six (6) years from creation, consistent with 45 C.F.R. § 164.316(b)(2)(i), independent of the case-data retention period in Section 12.

11.1.3 Audit logs shall be protected against unauthorized access, modification, or deletion, including by restricting write access to the automated processes that generate them.

11.2 Representative's Right to Audit

11.2.1 No more than once per calendar year, or promptly following a Security Incident or Breach, Representative may request that CaseClose (a) provide relevant audit log excerpts pertaining to Representative's own data in a reasonably usable format, (b) complete a written security questionnaire, or (c) provide a current summary of CaseClose's and its Subprocessors' relevant compliance certifications and BAAs, subject to reasonable confidentiality protections for information not pertaining to Representative's own data or for CaseClose's proprietary system information.

11.2.2 If Representative reasonably believes, based on a documented Security Incident or Breach, that a deeper review is warranted, CaseClose shall permit Representative (or a mutually agreeable independent third-party auditor bound by confidentiality obligations) to conduct a reasonable on-site or remote audit of the specific systems and controls relevant to the incident, at Representative's expense (unless the audit confirms a material violation by CaseClose, in which case CaseClose shall bear reasonable audit costs), upon reasonable advance notice and during normal business hours, and subject to CaseClose's reasonable security and confidentiality requirements.

11.3 Third-Party Certifications in Lieu of Audit

11.3.1 Where CaseClose or a Subprocessor maintains a current third-party audit report or certification reasonably responsive to Representative's audit request (for example, a SOC 2 report, once obtained, or an AWS/Supabase compliance attestation), CaseClose may satisfy the applicable portion of Representative's request by providing that report or certification in lieu of a duplicative independent audit of the same control.

12. Data Retention and Destruction

12.1 General Retention Standard

HIPAA itself does not set a retention period for case records; retention is governed by the law of the state(s) in which the applicable Covered Entity and Representative operate, which varies by state. Absent a shorter or longer period confirmed by counsel for the relevant jurisdiction(s), the parties agree to the following default schedule as a conservative baseline pending that confirmation:

12.1.1 Case data (patient labels, line items, pricing, and associated PHI) shall be retained for ten (10) years from the date of the applicable case, unless a longer period is required by the law of a state in which the applicable Covered Entity or patient is located, in which case the longer period controls for that record.

12.1.2 Audit logs and send logs shall be retained not less than six (6) years from creation, per Section 11.1.2, independent of the case-data retention period.

12.1.3 The parties shall revisit and, if necessary, amend this Section 12.1 upon confirmation by counsel of the specific state-law retention periods applicable to Representative's actual states of operation.

12.2 Destruction Standard

12.2.1 Upon expiration of the applicable retention period, or a valid destruction request under Section 13.4, CaseClose shall destroy PHI (including copies and backups, subject to standard backup-cycle rollover) using a method consistent with the Secretary's guidance for rendering PHI unusable, unreadable, or indecipherable, such as cryptographic erasure or secure deletion.

12.2.2 Destruction of case-sheet photographs and generated PDFs in encrypted object storage shall follow the lifecycle policy in Exhibit B and the Data Retention Policy, including any interim transition to lower-cost archival storage before final destruction, provided the same encryption and access controls continue to apply while archived.

12.3 Minors and Extended Retention

12.3.1 Where case data relates to a minor patient, CaseClose shall apply the longer retention period required by applicable state law for minors upon written notice from Representative identifying the record as subject to minor-patient retention rules.

13. Term and Termination

13.1 Term

13.1.1 This Agreement is effective as of the Effective Date and remains in effect until terminated under this Section 13, or until all PHI provided by Representative to CaseClose, or created or received by CaseClose on Representative's behalf, is destroyed or returned under Section 13.4, whichever is later.

13.2 Termination for Cause

13.2.1 Representative may terminate this Agreement immediately upon written notice if it determines CaseClose has violated a material term and such violation is not or cannot be cured within thirty (30) days after written notice describing the violation in reasonable detail. If neither termination nor cure is feasible, Representative may report the violation to the Secretary.

13.3 Termination for Convenience

13.3.1 Either party may terminate this Agreement, or Representative's access to the Services, for convenience upon thirty (30) days' prior written notice, subject to the separate termination provisions of the MSA governing the underlying commercial relationship.

13.4 Effect of Termination

13.4.1 Upon termination, CaseClose shall, at Representative's election and to the extent feasible, return or destroy all PHI it still maintains that was received from, or created or received on behalf of, Representative, retaining no copies except as provided in Section 13.4.2.

13.4.2 If return or destruction is not feasible (for example, because PHI must be retained under Section 12, applicable law, or standard backup-cycle limitations), CaseClose shall notify Representative in writing of the conditions making return or destruction infeasible, extend this Agreement's protections to the retained PHI, and limit further use or disclosure to the purposes that make return or destruction infeasible for as long as CaseClose retains it.

14. Indemnification

14.1 Indemnification by CaseClose

Subject to Section 15, CaseClose shall indemnify, defend, and hold harmless Representative, and, to the extent Representative is contractually obligated to extend such protection under an Upstream BAA, the applicable Covered Entity, from third-party claims, losses, liabilities, fines, penalties, and reasonable costs and expenses (including reasonable attorneys' fees) arising from: (a) CaseClose's or a Subprocessor's breach of this Agreement; (b) a Breach of Unsecured PHI caused by CaseClose's or a Subprocessor's negligence, willful misconduct, or failure to implement the safeguards required by Section 6; or (c) any use or disclosure of PHI by CaseClose or a Subprocessor not permitted by this Agreement.

14.2 Indemnification by Representative

Representative shall indemnify, defend, and hold harmless CaseClose from third-party claims, losses, liabilities, fines, penalties, and reasonable costs and expenses (including reasonable attorneys' fees) arising from: (a) Representative's breach of this Agreement, including the representations in Sections 8.2, and 5.2.1; (b) Representative's connection of a non-compliant email account in violation of Section 8.2; or (c) Representative's use of the Services inconsistent with its Upstream BAA(s) or the HIPAA Rules.

14.3 Procedure

14.3.1 The party seeking indemnification shall promptly notify the indemnifying party in writing of any claim, provided that delay does not relieve the indemnifying party except to the extent materially prejudiced.

14.3.2 The indemnifying party shall control the defense and settlement with counsel of its choosing, provided it shall not settle in a manner admitting fault by, or imposing a non-monetary obligation on, the indemnified party without that party's prior written consent, not unreasonably withheld.

14.3.3 The indemnified party shall reasonably cooperate, at the indemnifying party's expense, in the defense.

14.4 Aggregate Cap on Indemnification

Each party's aggregate indemnification obligations under this Section 14 shall not exceed $_____, as specified in the applicable Order Form under the MSA.

15. Limitation of Liability

15.1 General Limitation

EXCEPT FOR (A) A PARTY'S INDEMNIFICATION OBLIGATIONS UNDER SECTION 14 ARISING FROM A THIRD-PARTY CLAIM, (B) A PARTY'S BREACH OF SECTIONS 3 (PERMITTED USES), 6 (SAFEGUARDS), OR 9 (BREACH NOTIFICATION), (C) A PARTY'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT, OR (D) A PARTY'S BREACH OF ITS CONFIDENTIALITY OBLIGATIONS REGARDING PHI, IN NO EVENT SHALL EITHER PARTY BE LIABLE TO THE OTHER FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, OR PUNITIVE DAMAGES ARISING OUT OF OR RELATING TO THIS AGREEMENT, REGARDLESS OF THE THEORY OF LIABILITY, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

15.2 Aggregate Cap

Except for the exclusions set forth in Section 15.1, each party's aggregate liability under this Agreement shall not exceed the fees paid or payable under the MSA in the twelve (12) months preceding the claim, or $_____, as specified in the applicable Order Form.

15.3 Basis of the Bargain

The parties acknowledge that the limitations in this Section 15 are an essential basis of the bargain and that, absent them, the economic terms of the Services would be different.

16. Miscellaneous

16.1 Relationship to Other Agreements

16.1.1 This Agreement, the MSA, the HIPAA Security Addendum, and the Data Processing Addendum between the same parties are intended to be read together. As to PHI specifically, this Agreement controls in the event of conflict; as to commercial terms, the MSA controls; as to non-PHI personal data, the Data Processing Addendum controls.

16.2 Insurance

CaseClose represents that it maintains: (a) Cyber Liability / Technology Errors & Omissions insurance, including data breach response costs and regulatory fines/penalties to the extent insurable, with a per-occurrence limit of not less than $_____; and (b) Commercial General Liability insurance with a per-occurrence limit of not less than $_____. Upon written request, CaseClose shall furnish a certificate of insurance.

16.3 Interpretation and Regulatory References

16.3.1 A reference to a HIPAA Rules section means that section as in effect or amended, for which compliance is required. Any ambiguity shall be interpreted to permit HIPAA compliance.

16.4 Survival

16.4.1 Obligations under Sections 11 (Audit Rights, as to retained logs), 9 (Breach Notification, as to Breaches discovered before termination), 13.4 (Effect of Termination), 12 (Retention and Destruction), 14 (Indemnification), and 15 (Limitation of Liability) survive termination or expiration.

16.5 Amendment

16.5.1 This Agreement may be amended only by a written instrument signed by both parties, except the parties agree to amend as necessary to comply with changes in the HIPAA Rules; CaseClose may propose such amendments on thirty (30) days' written notice, effective unless Representative reasonably objects in writing within that period.

16.6 No Third-Party Beneficiaries

16.6.1 Except as provided in Section 14.1 regarding an applicable Covered Entity's indemnification rights, nothing in this Agreement confers rights on any person other than the parties and their permitted successors and assigns.

16.7 Assignment

16.7.1 Neither party may assign this Agreement without the other's prior written consent, except CaseClose may assign it without consent in connection with a merger, acquisition, or sale of substantially all assets, provided the assignee agrees in writing to be bound.

16.8 Notices

16.8.1 All notices shall be in writing and delivered by email (with confirmation of receipt for notices under Sections 9, 13, or 14) to the addresses on the signature page, or such other address as a party designates in writing.

16.9 Entire Agreement; Severability; Counterparts

16.9.1 This Agreement, including its Exhibits, is the entire agreement between the parties as to PHI handling and supersedes prior understandings on that subject, without superseding the MSA or other agreements as to matters outside the scope of PHI handling. If a provision is held invalid, the remainder continues in effect, and the parties shall negotiate in good faith to replace it with a valid provision reflecting the original intent. This Agreement may be executed in counterparts, including electronic or digital signature.

16.10 Governing Law and Dispute Resolution

This Agreement is governed by the laws of the State of Texas, without regard to conflict-of-laws principles, except to the extent preempted by the HIPAA Rules or other federal law. Subject to a good-faith direct-negotiation period of thirty (30) days following written notice of a dispute, the parties consent to the exclusive jurisdiction and venue of the state and federal courts located in _____ County, Texas.

Exhibit A — Description of Services

This Exhibit describes the Services as of the Effective Date. CaseClose shall update this Exhibit upon any material change affecting PHI handling.

Component	Description
Case Capture	Representative photographs a case sheet or implant log; the image is uploaded to CaseClose's backend, which performs OCR Extraction through the Bedrock Environment to populate structured case fields.
Case Review	Representative reviews, corrects, and confirms extracted case data, including an optional per-line-item notes field, before the case is finalized.
Inventory Tracking	Tracks manufacturer device/implant inventory, deducts inventory upon case confirmation, and forecasts shortages based on scheduled/tagged upcoming cases.
Schedule / Add Case	Representative may tag calendar events or manually add upcoming cases (date, time, manufacturer, case template, hospital, surgeon, patient) for planning/forecasting, distinct from the confirmed case record.
Send Center	Generates and transmits restock and billing communications via Representative's connected email account, and maintains an independently resendable send log.
Case History	Maintains a trimmed historical record (date, patient, hospital, surgeon) of closed cases, reopenable in Review to correct and resend.
Case-Sheet PDF Generation	Generates a PDF case sheet, including a Notes column when applicable, for transmission alongside restock/billing communications.
Authentication	Real per-Representative login/authentication (Section 6.3).

Exhibit B — Security Controls

This Exhibit summarizes the controls referenced in Section 6 and the HIPAA Security Addendum. CaseClose may update specific implementation details without amending this Agreement, provided the control objective and protection level are maintained or improved.

Control Area	Implementation
Encryption at rest	AES-256 (or stronger); database-level encryption at creation; encrypted object storage for case-sheet photos and PDFs.
Encryption in transit	TLS 1.2+ for client-backend, backend-Subprocessor, and backend-Bedrock communications.
Key management	Managed key-management service native to the backend platform; no keys embedded in client-side code.
Authentication	Real per-Representative login; role/row-level restrictions limiting each Representative to their own data.
Audit logging	Access/transmission logging retained 6+ years, protected against tampering.
Backup / lifecycle	Encrypted backups; lifecycle policy to archival storage while maintaining encryption/retention.
AI processing boundary	Server-side-only OCR Extraction within AWS's HIPAA-eligible boundary; no client-side/public-API AI calls with PHI.
Email token security	Encrypted OAuth refresh tokens; used solely for Representative-initiated sends; revocable anytime.
Vulnerability management	Periodic review/remediation of known vulnerabilities.
Incident response	Documented plan; investigation on discovery; notification per Section 9.
Workforce controls	Least-privilege access; unique credentials; periodic training; sanctions policy.
Physical security	Provided by underlying HIPAA-eligible cloud platforms under their BAAs/certifications.

Exhibit C — Approved Subprocessors

Consistent with Section 10, this Exhibit lists CaseClose's Subprocessors as of the Effective Date. See also the standalone Subprocessor Schedule, which CaseClose shall keep current and which controls in the event of conflict with this Exhibit as to the identity of current Subprocessors.

Subprocessor	Role / Data Processed	BAA Status
Amazon Web Services, Inc. (AWS Bedrock)	Server-side OCR Extraction from case-sheet photographs; underlying cloud infrastructure supporting the Bedrock Environment.	HIPAA BAA via AWS Artifact; Bedrock is HIPAA-eligible.
Supabase, Inc. (and/or affiliates)	Primary backend: Postgres database, authentication, encrypted storage, audit logging, auto-generated APIs.	HIPAA BAA under Supabase's Team plan with HIPAA add-on.
Google LLC (Google Workspace)	Per-Representative email transmission where Representative connects a Workspace account via OAuth.	BAA is between Representative's organization and Google; CaseClose is not a party (Section 8.4).
Microsoft Corporation (Microsoft 365)	Per-Representative email transmission where Representative connects a Microsoft 365 account via OAuth.	BAA is between Representative's organization and Microsoft; CaseClose is not a party (Section 8.4).
Additional Subprocessor (if any)	_____	_____

Signature Page

IN WITNESS WHEREOF, the parties have executed this Business Associate Agreement as of the Effective Date.

REPRESENTATIVE / CUSTOMER:

_____

Signature: _____

Name: _____

Title: _____

Date: _____

Notice Address: _____

_____

Email for Notices: _____

CASECLOSE:

Catalyst MedTech LLC, a Texas limited liability company, dba CaseClose

Signature: _____

Name: _____

Title: _____

Date: _____

Notice Address: _____

_____

Email for Notices: _____