Fieldstone Health Master Business Associate Agreement

Sample copy. This is Fieldstone Health's Master Business Associate Agreement, version 1.0 of 27 October 2026, published for review before signing. Each customer signs its own copy, which records the revision signed. Questions: security@fieldstone-health.com.

This Master Business Associate Agreement (the "Agreement") is made as of the Effective Date on the signature page between **Fieldstone Health, LLC**, a Massachusetts limited liability company with its principal office at 14 Algonquian Drive, Natick, Massachusetts 01760 ("Fieldstone"), and the customer named on the signature page ("Customer").

Background

A. Fieldstone provides software and related services to Customer, as described in one or more Service Schedules signed by the parties (the "Services").

B. In providing the Services, Fieldstone may create, receive, maintain or transmit protected health information on Customer's behalf.

C. The parties enter into this Agreement to meet the business associate requirements of HIPAA and the HITECH Act. Where Customer is not subject to HIPAA, they enter into it so that Customer's information receives the same protection by contract.

1. Definitions

1.1 HIPAA terms. Capitalized terms used but not defined in this Agreement have the meanings given in 45 C.F.R. Parts 160 and 164, including Breach, Business Associate, Covered Entity, Designated Record Set, Disclosure, Individual, Minimum Necessary, Required by Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information and Use.

1.2 HIPAA Rules means the Privacy, Security, Breach Notification and Enforcement Rules at 45 C.F.R. Parts 160 and 164, as amended from time to time.

1.3 Protected Health Information or **PHI** has the meaning given in 45 C.F.R. § 160.103, limited to information that Fieldstone creates, receives, maintains or transmits on Customer's behalf in providing the Services. PHI includes Electronic Protected Health Information. It also includes PHI that reaches Fieldstone on Customer's behalf through a channel section 8.3 doesn't allow; that information is still protected under this Agreement.

1.4 Customer status. Customer may be a Covered Entity, a Business Associate of a Covered Entity, or an organization not subject to HIPAA. If Customer is not a Covered Entity or Business Associate:

1. information Fieldstone handles for Customer that would be PHI if Customer were a Covered Entity is treated as PHI under this Agreement; and
2. Fieldstone's obligations under this Agreement apply by contract as if Customer were a Covered Entity.

For information protected only by contract under this section, the HIPAA standards in this Agreement apply as contract terms. This Agreement does not make either party subject to HIPAA, give a regulator authority it would not otherwise have, or create an exemption from any other law. Customer remains bound by the obligations this Agreement places on Customer, and is responsible for having a lawful basis to collect and disclose the information and for any notices and consents the law requires. If Customer is a Business Associate of a Covered Entity, Fieldstone acts as Customer's Subcontractor, and this Agreement applies with that change. Customer states its role on the signature page and will tell Fieldstone promptly if it changes. Schedule C sets out the additional terms for health information this Agreement protects by contract rather than under HIPAA.

1.5 Service Schedule means a schedule to this Agreement that describes a Fieldstone product or plan and how PHI is handled in it, as signed by both parties and as later updated under section 10. Each version carries a version number and date. A reference to a signed Service Schedule includes updates validly adopted under section 10.

1.6 Subcontractor List means Fieldstone's list of its Subcontractors (Fieldstone document FH-LEG-006), given to Customer at signing and on request, as updated under section 5.2.

1.7 Business Day means a weekday other than a U.S. federal holiday. Any other period stated in "days" means calendar days.

1.8 Counting time. A period runs from the day after its starting event. A period measured from a notice starts when the notice becomes effective under section 12.5. A period measured from a request starts when the request is received: when it reaches the recipient's notice contact under section 12.5 or, for a request made through the Services, when it is submitted there. Every period is an outer limit. None overrides a requirement in this Agreement to act sooner, without unreasonable delay or immediately, and none extends a deadline set by law.

2. Permitted uses and disclosures

2.1 Services. Fieldstone may use and disclose PHI only as needed to perform the Services described in Customer's signed Service Schedules, or as Required by Law.

2.2 Fieldstone's management and administration. Fieldstone may use PHI for its proper management and administration or to carry out its legal responsibilities. It may disclose PHI for those purposes only if the disclosure is Required by Law, or if Fieldstone first obtains reasonable assurances from the recipient that the PHI will be kept confidential, used or further disclosed only as Required by Law or for the purpose for which it was disclosed, and that the recipient will notify Fieldstone of any instance in which the confidentiality of the PHI has been breached.

2.3 Minimum necessary. Fieldstone will limit its uses, disclosures and requests for PHI to the minimum necessary to accomplish their purpose.

2.4 HIPAA limits. Fieldstone will not use or disclose PHI in any way that would violate Subpart E of 45 C.F.R. Part 164 if done by Customer, except as permitted by section 2.2.

2.5 What Fieldstone will never do. Fieldstone will not sell PHI, use or disclose PHI for marketing, or use PHI to develop or train artificial-intelligence or machine-learning models.

Fieldstone may keep counts of form activity, such as forms viewed, started and submitted, that contain no PHI, to operate the Services and report on them to Customer.

3. Safeguards

3.1 Fieldstone will use appropriate administrative, physical and technical safeguards, and comply with Subpart C of 45 C.F.R. Part 164 for Electronic PHI, to prevent any use or disclosure of PHI other than as this Agreement provides.

3.2 How each product protects PHI is described in its Service Schedule.

4. Reporting and mitigation

4.1 What Fieldstone reports. Fieldstone will report to Customer:

1. any use or disclosure of PHI not provided for by this Agreement;
2. any Breach of Unsecured PHI, as required by 45 C.F.R. § 164.410; and
3. any Security Incident,

of which Fieldstone becomes aware.

4.2 When. Fieldstone will report in two steps:

1. **Initial notice** without unreasonable delay, and no later than 3 Business Days after discovering the event, saying what is known so far and naming a contact person.
2. **Full report** no later than 10 Business Days after discovery, with all the information in section 4.4 that is then known.

A Breach is treated as discovered as set out in 45 C.F.R. § 164.410(a)(2). An unfinished investigation does not delay either notice; Fieldstone will say what is still unknown and supplement the report as information becomes available. These are outer limits. They do not allow unreasonable delay, or delay beyond an earlier deadline set by law.

4.3 Unsuccessful attempts. This section is notice to Customer of routine, unsuccessful attempts against Fieldstone's systems, such as pings, port scans and failed sign-ins, that do not result in unauthorized access to, or Use or Disclosure of, PHI or affect its confidentiality, integrity or availability. No separate report of those attempts is required. An attack that succeeds, disrupts availability or otherwise compromises PHI is reported under sections 4.1 and 4.2.

4.4 Contents. A Breach report will identify each Individual whose Unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used or disclosed. It will give all other information then available that Customer needs for its notice under 45 C.F.R. § 164.404(c), including what happened, the relevant dates, the types of PHI involved, steps Individuals should take to protect themselves, what Fieldstone is doing to investigate and mitigate, and contact details. Fieldstone will promptly supplement the report. The initial notice by email and phone may leave out Individuals' identities; report contents that include PHI go through the secure channel Fieldstone designates under section 8.3(3), never by ordinary email.

4.5 Mitigation. Fieldstone will mitigate, to the extent practicable, any harmful effect known to it of a use or disclosure of PHI in violation of this Agreement.

4.6 Notices to Individuals. Customer is responsible for the notices to Individuals, regulators and the media that the law requires of Customer. Fieldstone will cooperate and promptly supply the information Customer reasonably needs. This does not excuse either party from its own duties under law or allow Fieldstone to delay a report the law requires, and the parties will coordinate notices where the law allows.

5. Subcontractors

5.1 Subcontractor agreements. Under 45 C.F.R. §§ 164.502(e)(1)(ii) and 164.308(b)(2), Fieldstone will ensure that any Subcontractor that creates, receives, maintains or transmits PHI on its behalf agrees in writing to the restrictions, conditions and requirements HIPAA requires for that information. A Subcontractor's standard business associate agreement or other binding written terms are acceptable if they meet those requirements and preserve this Agreement's restrictions on the use and disclosure of Customer's PHI, including the prohibitions in section 2.5 on sale, marketing and use to train artificial-intelligence or machine-learning models. They need not repeat every commercial or administrative provision of this Agreement word for word. Whatever a Subcontractor's terms provide, Fieldstone remains responsible for meeting its own obligations to Customer, including the reporting deadlines in section 4.

5.2 Subcontractor List. Fieldstone keeps a current Subcontractor List naming each Subcontractor that handles PHI, what it does, and where it processes PHI. Fieldstone gives Customer the current version at signing and on request. The version in effect at signing is part of this Agreement, and Fieldstone keeps every earlier version. Fieldstone will give Customer written notice at least 30 days before a new Subcontractor first handles Customer's PHI, counted from when the notice becomes effective. Customer may object on reasonable privacy or security grounds within 15 days after the notice becomes effective. If the parties can't resolve the objection before the new Subcontractor first has access, Customer may end the affected Service Schedule without penalty and take its export first. Listing a Subcontractor does not replace the written agreement section 5.1 requires.

5.3 Responsibility. Fieldstone is responsible to Customer under this Agreement for the services its Subcontractors perform and for their handling of Customer's PHI, as if Fieldstone had performed those services itself. This does not mean that any Subcontractor has signed, or is bound by, this Agreement.

6. Individuals' rights

6.1 Access. Without unreasonable delay, and no later than 10 Business Days after receiving Customer's request, or sooner if Customer tells Fieldstone a legal deadline requires it, Fieldstone will make PHI it holds in a Designated Record Set available to Customer, in the electronic form and format requested if readily producible or otherwise in a readable format agreed with Customer, so Customer can meet 45 C.F.R. § 164.524. In sections 6.1 to 6.3, each period is the time for completing the assistance described, not just for acknowledging the request, and no period extends a deadline set by law. Those sections apply for as long as Fieldstone holds the PHI, and Fieldstone will not withhold access because of a payment dispute or termination.

6.2 Amendment. No later than 10 Business Days after receiving Customer's request, or sooner if Customer tells Fieldstone a legal deadline requires it, Fieldstone will make PHI it holds in a Designated Record Set available for amendment and incorporate amendments as Customer directs, so Customer can meet 45 C.F.R. § 164.526. Where a record can't be changed, such as an archive copy, Fieldstone will attach or link the amendment and include it with every later access, export and disclosure of that record.

6.3 Accounting. Fieldstone will document the disclosures of PHI needed for an accounting under 45 C.F.R. § 164.528, including the date, the recipient and its address if known, a description of the PHI and the purpose, and keep that information for six years. No later than 10 Business Days after receiving Customer's request, or sooner if Customer tells Fieldstone a legal deadline requires it, Fieldstone will give Customer that information.

6.4 Requests made to Fieldstone. If an Individual asks Fieldstone directly for access, amendment or an accounting, Fieldstone will securely forward the request to Customer without unreasonable delay and no later than 2 Business Days after receiving it, or sooner if the law requires. Fieldstone may acknowledge the request and tell the Individual which Customer is responsible, but will not decide the request except as Customer directs or the law requires.

6.5 Restrictions. Fieldstone will comply with any restriction on the use or disclosure of PHI, or confidential-communication request, that Customer has agreed to and notified Fieldstone of in writing, to the extent it affects Fieldstone.

6.6 Customer's Privacy Rule duties. To the extent Fieldstone carries out any of Customer's obligations under Subpart E of 45 C.F.R. Part 164, it will comply with the requirements of Subpart E that apply to Customer in doing so.

7. Books and records

Fieldstone will make its internal practices, books and records relating to the use and disclosure of PHI available to the Secretary as required for determining compliance with the HIPAA Rules. For information protected only by contract under section 1.4, Fieldstone will disclose to a government authority only what that authority may lawfully require.

8. Customer's obligations

8.1 Notices and restrictions. Customer will tell Fieldstone in writing of any limitation in its notice of privacy practices, any change in an Individual's permission, and any restriction Customer agrees to, to the extent it affects Fieldstone's use or disclosure of PHI.

8.2 Permissible requests. Customer will not ask Fieldstone to use or disclose PHI in any way that would not be permitted under Subpart E of 45 C.F.R. Part 164 if done by Customer, except as section 2.2 allows.

8.3 Customer's side of the Services. Customer is responsible for:

1. the delivery addresses it sets for its forms, and the security of its own email accounts and systems once PHI is delivered to them;
2. who on its staff has accounts, including removing access promptly when someone leaves; and

3. sending PHI to Fieldstone only through the Services. Customer will not send PHI by ordinary email, support tickets or the Fieldstone websites. If a support issue requires sharing PHI, Customer will use the secure channel Fieldstone designates for that purpose.

8.4 Blank forms. When Customer sends Fieldstone a form to build, it will send a blank copy with no patient information on it.

8.5 Activation. Customer will not use the Services with real patient information until this Agreement, the applicable Service Schedule and the Fieldstone Health Services Agreement are signed and Fieldstone has expressly activated the Service for Customer. Any demo Fieldstone provides before activation is for fictional patient information and blank templates only. Fieldstone's demo controls enforce specific limits (demo marking, no uploads, a submission cap and expiry) and can't detect every entry of real patient information; Customer is responsible for keeping real patient information out of a demo.

9. Term and termination

9.1 Term. This Agreement starts on the Effective Date and continues until every Service Schedule has ended and Fieldstone has returned or destroyed all PHI as section 9.4 provides.

9.2 Termination for breach. If either party determines that the other has materially breached this Agreement, it will give written notice and may allow up to 30 days, counted from when the notice becomes effective, to cure a breach that can be cured. If the breach is not cured in that time, the non-breaching party may terminate this Agreement and the affected Services. It may terminate immediately if the breach can't reasonably be cured, or if continuing would put PHI at material risk or break the law. Either party may promptly suspend affected processing to contain a material security risk, while keeping Customer's lawful access and return rights. A party that learns of a pattern of activity or practice by the other that is a material breach will take reasonable steps to have it cured or ended and, if those steps fail, terminate where feasible.

9.3 Ending a Service Schedule. Either party may end a Service Schedule as the Fieldstone Health Services Agreement allows. This Agreement continues for any Service Schedule still in effect.

9.4 Return or destruction. When a Service Schedule ends, or when deletion of particular PHI becomes due under a Service Schedule, Customer's instruction or the law, Fieldstone will return or destroy that PHI as the Service Schedule describes and keep no copies, except that:

1. **Locked copies.** Fieldstone destroys locked archive copies and backups by deleting the data itself when each copy's lock or retention period ends. Fieldstone will first complete any return or export that this Agreement or the Service Schedule requires. Disabling an encryption key, deleting it or scheduling it for deletion is not a permitted way to destroy PHI. Until a locked copy is deleted, it remains PHI with every protection of this Agreement. Fieldstone places in a locked archive only the PHI Schedule B allows, and never information subject to a deletion right or duty that the lock could not meet (Schedule C, sections C.1 and C.8). While a locked copy remains after its Service Schedule has ended, Fieldstone keeps it only to complete the lock, uses it for nothing except a return Customer requests or a disclosure Required by Law, limits access to its

authorized administrator, and deletes it when the lock ends; each copy's deletion date is fixed when it is written, and Fieldstone tells Customer the date of the last one. If a copy can't be deleted when deletion becomes due, section 9.4(3) applies and Fieldstone tells Customer at once.

2. **Audit records.** Fieldstone keeps two kinds of record for 6 years under its written security policy, as documentation under 45 C.F.R. § 164.316(b)(2): (a) its audit log of access to PHI, recording the account and its role, the action, the time, the account's IP address, Customer's name, the form's name and the submission's number; and (b) a record of each form received, when, where it was delivered and the outcome. Neither record holds form answers, patient names or other patient identifiers, and a submission number identifies no one once the submission is deleted. After a Service Schedule ends, only Fieldstone's authorized administrator may use these records, and only for security investigation, Customer's or a regulator's lawful request, or a legal duty; they are deleted when the 6 years end. For Contract Health Data, section C.8 applies to any such record that identifies an individual. Any other PHI kept after termination stays protected under this Agreement and is deleted when the reason for keeping it ends.
3. **Infeasibility.** Where return or destruction is infeasible, Fieldstone will document the specific reason and tell Customer in writing what information is affected, why, and how long Fieldstone expects to keep it; extend this Agreement's protections to it; limit further uses and disclosures to the purposes that make return or destruction infeasible; and destroy it as soon as it can. This applies to backup, archive and Subcontractor copies too. An archive lock does not by itself make return or destruction infeasible, and neither an archive lock nor this Agreement overrides a legal duty to keep or delete information.

9.5 Survival. Section 9.4 and Fieldstone's obligations for any PHI it keeps survive termination.

10. Updates to Service Schedules

10.1 Updates that keep or improve protection. Fieldstone may update the operational or security descriptions in a Service Schedule, within the scope of the Services Customer signed for, without Customer's signature, as long as the update does not reduce protection. Fieldstone will compare each proposed update with the terms then binding on Customer. An update reduces protection if it weakens the confidentiality, integrity or availability of PHI, or narrows commitments on permitted purposes, retention, processing locations, access or support for Individuals' rights. An improvement in one protection does not offset a reduction in another.

10.2 Notice of updates. Fieldstone will send the revised Service Schedule, a clear summary of the changes and the effective date to Customer's notice contact under section 12.5, so that the notice becomes effective at least 30 days before the update's effective date. For an urgent security update, Fieldstone may give shorter notice, as soon as practicable. That exception shortens the notice period only; it does not permit any change that section 10.3 requires Customer to agree to. Changes the law requires are handled under section 12.1.

10.3 Changes that need Customer's written agreement. An update that reduces protection, adds a processing purpose, adds a Service, or changes monetary liability or fees takes effect for Customer only with Customer's affirmative written agreement. Silence or continued use of the Services is not agreement.

10.4 Effect and records. An update applies only from its effective date. It does not affect rights, obligations or claims that arose before then. Each update carries a new version number and date. Fieldstone will keep every version, each notice it sent with evidence of delivery, and a record of which version applies to each customer.

11. Order of precedence

This Agreement governs the parties' obligations to protect PHI and prevails over any conflicting Service Schedule or other agreement about those obligations. Each signed Service Schedule, including updates validly adopted under section 10, supplies its product's details consistently with this Agreement, and no update can change this Agreement. A limit on liability or remedies applies to claims under this Agreement only if a signed agreement says so expressly, and no such limit reduces either party's legal duties or required safeguards. This Agreement does not create an indemnity or a duty to reimburse Customer's notification or other breach-response costs.

12. General terms

12.1 Changes in law. The parties will amend this Agreement as needed to comply with changes in law by their compliance dates. Either party may propose a legally necessary amendment by written notice. If the parties can't agree on it within 60 days after the other party receives that notice, or sooner where needed to avoid breaking the law, either party may terminate the affected Services, with PHI returned or transferred under the protections of this Agreement. Negotiation does not postpone either party's legal duties.

12.2 Interpretation. Any ambiguity in this Agreement is resolved in favor of a meaning that complies with the HIPAA Rules. A reference to a regulation means that regulation as in effect or as amended.

12.3 Independent contractor. The parties intend Fieldstone to act as an independent contractor, not Customer's agent. This does not override any agency relationship that the law and the parties' actual conduct establish.

12.4 No third-party beneficiaries. Nothing in this Agreement gives any right to anyone other than the parties.

12.5 Notices. Notices go by email to the notice contacts on the signature page, which either party may change by notice. An email notice is effective on the day it is sent to the recipient's notice address, unless the sender receives an automated message that it was not delivered; the sender will then resend it or use another reasonable method, and the notice is effective when that succeeds. A Breach report under section 4 also goes by phone to Customer's notice contact.

12.6 Governing law and venue. This Agreement and disputes between the parties arising out of or relating to it are governed by the laws of the Commonwealth of Massachusetts, without regard to its conflict-of-laws rules, subject to applicable federal law and other nonwaivable law.

Subject to applicable nonwaivable law, any action between the parties arising out of or relating to this Agreement must be brought exclusively in the state courts of competent jurisdiction located in Middlesex County, Massachusetts or, where federal subject-matter jurisdiction

exists, the United States District Court for the District of Massachusetts. Each party consents to personal jurisdiction and venue in those courts.

This section does not restrict governmental enforcement authority or the rights of persons who are not parties to this Agreement.

12.7 Entire agreement and signatures. This Agreement and its signed Service Schedules, including updates validly adopted under section 10, are the parties' entire agreement about protecting PHI, together with any signed commercial terms that section 11 makes apply. They may be signed electronically and in counterparts.

Signatures

	Fieldstone Health, LLC	Customer
Legal name	Fieldstone Health, LLC	
HIPAA role	Business Associate	☐ Covered Entity ☐ Business Associate of a Covered Entity ☐ Not subject to HIPAA
Signed by		
Name and title	Russell Corsini, Member	
Date		
Notice contact (name, email, phone)	Russell Corsini, security@fieldstone-health.com, 617-237-0220	
Effective Date		

Service Schedules included:

- ☐ Schedule A: Secure Form Direct Delivery, version 1.0, 27 October 2026
- ☐ Schedule B: Secure Form Workflow Portal, version 1.0, 27 October 2026

Schedule C (Health Data Outside HIPAA) is part of this Agreement and applies automatically wherever it is relevant; it needs no separate signature.

Schedule A: Secure Form Direct Delivery

Version 1.0, 27 October 2026. This Service Schedule is part of the Master Business Associate Agreement between Fieldstone Health, LLC and Customer. On Direct Delivery, completed forms reach Customer by secure email and are deleted from Secure Form 30 days after the email provider accepts the delivery email.

Item	Terms
Service	Fieldstone hosts Customer's patient forms at Customer's own address on secure-form.com. When a patient submits a form, Fieldstone stores it, makes a PDF of it, and emails the PDF and any files the patient attached to the addresses Customer sets for that form.
PHI handled	Whatever Customer's forms ask for. This may include names, contact details, dates of birth, Social Security numbers, insurance details and card images, driver's license images, medical and dental history, and signatures. Customer decides what its forms collect. Patients do not have accounts.
Where it is processed and stored	In data centers in the United States, run by the hosting and storage providers on the Subcontractor List.
Shared and separate	All Secure Form customers share one application, one database and one file store. Access controls in the application and row-level security in the database limit each customer's staff to that customer's records, and Fieldstone tests and maintains those controls. Customers also share Fieldstone's code, its administration and its email provider.
Encryption in transit	Every connection that carries PHI is encrypted with TLS 1.2 or later. The email provider delivers over TLS. Where the recipient's mail server can't accept TLS, the provider holds the message in its secure portal, where the recipient signs in to read it.
Encryption at rest	Before storing a submission, the application encrypts its answers, signatures, files and PDF with a key unique to Customer. Customer's key is itself protected by a master key held in a separate key-management service. The storage underneath is also encrypted by the provider.
Email contents	The PDF and the patient's files are attached. The subject and body name only the form, Customer and the time.

Item	Terms
How long it is kept	Each submission is kept for 30 days after the email provider accepts its delivery email, so it can be sent again if an email is lost, and is then deleted. Acceptance by the email provider does not confirm the email arrived; Fieldstone watches for reported delivery failures, alerts Customer, and resolves each submission that can't be delivered with Customer, by resending it, correcting the address or returning it securely; a submission whose delivery failed is deleted 30 days after it is resolved, and is never kept indefinitely. Direct Delivery submissions are never added to a long-term archive. Backup copies held by Fieldstone and its Subcontractors expire within a further 30 days, subject to Master BAA section 9.4. Copies held by the email provider, including messages waiting in its secure portal, are deleted within 30 days after sending, and its backup copies expire within a further 30 days. Copies delivered to Customer's mailboxes are under Customer's control.
Once delivered	A delivered email is stored in Customer's mailbox under Customer's control. Its security there is Customer's responsibility (Master BAA, section 8.3).
Customer's access	Customer's administrators sign in with a password and a second step, or with a passkey. A device the user chooses to trust can skip the second step for up to 30 days. Administrators manage forms, delivery addresses and staff accounts, and see counts and a delivery log. On Direct Delivery they do not view stored submissions. They can see the full audit log, including every access by Fieldstone and its emergency contractor; audit entries may show which submission was accessed.
Fieldstone's access	Only Fieldstone's authorized administrator and its designated emergency contractor can open stored submissions, each with their own account, and only to deliver or resend them, to fix a problem, in a documented emergency, or as Customer directs. Every view and download, including privileged and emergency access, is recorded in an audit log kept for 6 years: the application attributes every decryption of a submission to a named account, so no access goes unrecorded.
Form pages	Patient form pages load no scripts from other services and run no analytics. Fieldstone does not store patient answers in the browser and tells browsers not to cache form pages. The patient's own downloads, and browser features such as autofill, are outside Fieldstone's control.

Item	Terms
Logs	Fieldstone keeps PHI out of its application logs, the hosting provider's service-generated logs and page addresses: its forms and portal are built so that patient answers never appear in them, and the hosting provider's rules forbid PHI in its logs. The hosting provider's request logs record each visitor's IP address and the page address, which names no patient, for 30 days. Any log found to contain PHI is protected under this Agreement and the cause corrected.
AI tools	Fieldstone may use an AI service to extract questions and field structure from Customer's approved blank forms to build web forms. An authorized person reviews each form before approving its submission, checking for patient information, filled-in answers and hidden or embedded data. A form containing PHI is never submitted to the AI service: Fieldstone asks for a clean blank replacement and returns or deletes the original. Fieldstone uses AI services only under terms and settings that bar training on what it sends. Any mistake is handled under Master BAA section 4.
Return or destruction	Because submissions are deleted 30 days after the email provider accepts their delivery email, there is normally little to return. If Customer asks before this Schedule ends or within 30 days after, Fieldstone will securely return any submission it still holds. Within 30 days after this Schedule ends, Fieldstone deletes all of Customer's submissions, forms and account data, and backup copies expire within a further 30 days, subject to Master BAA section 9.4. Fieldstone will tell Customer the deletion date in advance. Audit records, and the record of each form received and where it was delivered, are kept for 6 years (Master BAA, section 9.4).
Subcontractors	Hosting, file storage, backup and key management, secure email, Fieldstone's own email, and Fieldstone's emergency contractor, as named on the Subcontractor List.

Schedule B: Secure Form Workflow Portal

Version 1.0, 27 October 2026. This Service Schedule is part of the Master Business Associate Agreement between Fieldstone Health, LLC and Customer. On Workflow Portal, completed forms stay in Customer's secure portal, where Customer's staff search, view, download and track them.

Item	Terms
Service	Fieldstone hosts Customer's patient forms at Customer's own address on secure-form.com and stores each completed form in Customer's portal. Customer's staff search, view, download and track submissions there.
PHI handled	Whatever Customer's forms ask for. This may include names, contact details, dates of birth, Social Security numbers, insurance details and card images, driver's license images, medical and dental history, and signatures. Customer decides what its forms collect. The portal also holds staff accounts and their activity. Patients do not have accounts.
Where it is processed and stored	In data centers in the United States, run by the hosting and storage providers on the Subcontractor List.
Shared and separate	All Secure Form customers share one application, one database and one file store. Access controls in the application and row-level security in the database limit each customer's staff to that customer's records, and Fieldstone tests and maintains those controls. Customers also share Fieldstone's code, its administration and its email provider.
Encryption in transit	Every connection that carries PHI is encrypted with TLS 1.2 or later.
Encryption at rest	Before storing a submission, the application encrypts its answers, signatures, files and PDF with a key unique to Customer. Customer's key is itself protected by a master key held in a separate key-management service. The storage underneath is also encrypted by the provider.
Email	When a form arrives, Customer's chosen staff get a notice with a link to the portal and no patient details. At Customer's request, Fieldstone can also attach the PDF, which is then delivered as on Direct Delivery.

Item	Terms
How long it is kept	Active records: submissions stay in the portal while Customer is a client, unless Customer chooses a shorter retention period, after which older submissions are deleted from active systems. Backups: nightly backup copies expire 30 days after the record they hold is deleted. The locked archive below is a separate, limited exception. Customer's staff can't delete submissions; Fieldstone deletes junk, duplicate or other submissions when Customer asks, and whenever the law requires earlier deletion.
Archive	The locked archive holds only Regulated PHI, and only for a Customer that is a Covered Entity or Business Associate: each submission containing Regulated PHI is written once to a locked archive and kept for 1 year from the day it is written. Nobody, including Fieldstone, can change or delete an archive copy before then, which protects Customer's records against accidental deletion, changes and tampering. Fieldstone uses an archive copy only to restore Customer's record at Customer's request or as Required by Law, and limits access to its authorized administrator. Corrections are attached under Master BAA section 6.2. Contract Health Data, and any information subject to a deletion right or duty the lock could not meet, never goes into the archive (Schedule C, sections C.1 and C.8), so customers not subject to HIPAA have no locked archive. Each archive copy is deleted when its one-year lock ends, including after this Schedule ends (Master BAA, section 9.4(1)). Nightly backup copies are kept 30 days.
Customer's access	Each staff member has their own account and sees only Customer's records. Every account signs in with a password and a second step, or with a passkey. A device the user chooses to trust can skip the second step for up to 30 days; that option is not for shared or public computers, and removing the account ends it. Sessions end after 30 minutes without activity or 8 hours after sign-in. Customer's administrators add and remove staff.
Audit log	Every view and download of a submission, including privileged and emergency access, is recorded with the person and the time, and kept for 6 years; the application attributes every decryption of a submission to a named account, so no access goes unrecorded. Customer's administrators can see the full log, including every access by Fieldstone and its emergency contractor.
Fieldstone's access	Only Fieldstone's authorized administrator and its designated emergency contractor can open stored submissions, each with their own account, and only to support Customer, to fix a problem, in a documented emergency, or as Customer directs. Every view and download is recorded in the audit log.

Item	Terms
Form pages	Patient form pages load no scripts from other services and run no analytics. Fieldstone does not store patient answers in the browser and tells browsers not to cache form pages. The patient's own downloads, and browser features such as autofill, are outside Fieldstone's control.
Logs	Fieldstone keeps PHI out of its application logs, the hosting provider's service-generated logs and page addresses: its forms and portal are built so that patient answers never appear in them, and the hosting provider's rules forbid PHI in its logs. The hosting provider's request logs record each visitor's IP address and the page address, which names no patient, for 30 days. Any log found to contain PHI is protected under this Agreement and the cause corrected.
AI tools	Fieldstone may use an AI service to extract questions and field structure from Customer's approved blank forms to build web forms. An authorized person reviews each form before approving its submission, checking for patient information, filled-in answers and hidden or embedded data. A form containing PHI is never submitted to the AI service: Fieldstone asks for a clean blank replacement and returns or deletes the original. Fieldstone uses AI services only under terms and settings that bar training on what it sends. Any mistake is handled under Master BAA section 4.
Return or destruction	If Customer asks before this Schedule ends or within 10 days after, Fieldstone will, at no charge and within 10 Business Days, provide one export of all Customer's submissions: a ZIP file with a folder for each submission, named by its date, patient and form, holding its PDF and attached files, with a CSV index of patient name, date of birth, form, date submitted and status, plus any amendments and a copy of Customer's audit log. Customer downloads it from the portal. Fieldstone will tell Customer in advance when the export is available and when deletion will happen. Within 30 days after this Schedule ends, Fieldstone deletes all of Customer's submissions, forms and account data from its active systems, and backup copies expire within a further 30 days. The one exception is the locked archive: an archive copy can't be deleted before its lock ends, even by Fieldstone, so each one is deleted when its own one-year lock ends, at most one year after the last submission was archived, and stays PHI with every protection of this Agreement until then (Master BAA, section 9.4(1)). Fieldstone tells Customer the date the last archive copy will be deleted. Audit records, and the record of each form received and where it was delivered, are kept for 6 years (Master BAA, section 9.4).

Item	Terms
Subcontractors	Hosting, file storage, backup and key management, secure email, Fieldstone's own email, and Fieldstone's emergency contractor, as named on the Subcontractor List.

Schedule C: Health Data Outside HIPAA

Version 1.0, 27 October 2026. This Schedule is part of the Master Business Associate Agreement, not a Service Schedule, and changes only by written amendment. It applies automatically whenever Fieldstone handles Contract Health Data for Customer, in any product. For Contract Health Data it adds to the rest of the Agreement and prevails where they conflict, but it never reduces a protection the rest of the Agreement gives.

C.1 Two kinds of health information. This Agreement protects two kinds of information:

1. **Regulated PHI:** protected health information under 45 C.F.R. § 160.103 that Fieldstone handles as a Business Associate or Subcontractor. HIPAA applies to it by law.
2. **Contract Health Data:** any other information about an identifiable individual's health that Fieldstone handles for Customer in providing the Services, including information treated as PHI under section 1.4 and consumer health data under any applicable state law. It receives by contract every protection this Agreement gives PHI, plus this Schedule.

Customer's HIPAA role on the signature page is Fieldstone's starting point, not the deciding factor: the information's actual status governs. This Schedule applies whenever Fieldstone handles Contract Health Data, including for a Customer that is a Covered Entity or Business Associate. Before a form goes live, the parties record in writing which kind of information it collects, considering who the individuals are and why the information is collected. If that is unclear, Fieldstone treats the information as Contract Health Data for deletion and archiving, while giving it every protection PHI receives, until the parties resolve it.

C.2 Customer's instructions and Fieldstone's role. Customer decides why and how Contract Health Data is processed. Fieldstone acts as Customer's processor (or service provider, or the equivalent role under applicable law) and processes Contract Health Data only on Customer's documented instructions: this Agreement, Customer's signed Service Schedules and Customer's written instructions given through the Services. Fieldstone will tell Customer if it believes an instruction would break applicable law.

C.3 No independent use. Section 2.2 does not apply to Contract Health Data. Fieldstone may use it only to provide, secure and support the Services and to comply with law. Fieldstone will not sell it, share it for advertising, use it for its own purposes, combine it with information from other sources, or keep or use it outside its relationship with Customer, except the records section 9.4(2) permits, which remain subject to section C.8.

C.4 Notices and consents. Customer is responsible for the privacy notices, consumer health data privacy policies and consents that applicable law requires to collect Contract Health Data and to disclose it to Fieldstone. Fieldstone will give Customer the information about its processing that Customer reasonably needs for them.

C.5 Individuals' rights. Fieldstone will help Customer respond to requests from individuals to access, confirm, correct or delete their Contract Health Data, to withdraw consent, or to exercise any other right applicable law gives them. It will complete that help no later than 10 Business Days after receiving Customer's request, or sooner if Customer tells Fieldstone a legal deadline

requires it; acknowledging the request is not enough. A deletion request is the exception: Fieldstone will confirm it to Customer within 10 Business Days and complete the deletion within the periods in section C.8. If an individual sends such a request to Fieldstone, Fieldstone will forward it to Customer no later than 2 Business Days after receiving it. When consent is withdrawn, Fieldstone will stop the processing Customer identifies.

C.6 Subcontractors. Fieldstone will let a Subcontractor process Contract Health Data only under binding written terms that limit it to processing on Fieldstone's instructions, preserve this Schedule's restrictions on use and disclosure, and meet the requirements of applicable law. As with section 5.1, those terms need not repeat this Schedule word for word. Section 5, including the Subcontractor List, Customer's right to object and Fieldstone's responsibility under section 5.3, applies.

C.7 Security and incidents. The safeguards in section 3 apply to Contract Health Data. Fieldstone will report any unauthorized acquisition, access, use or disclosure of Contract Health Data, and any Security Incident affecting it, on the timetable in section 4.2, and will give Customer the information it needs to meet any notice duty under state breach or health-data law. Customer gives the notices the law requires of it.

C.8 Deletion everywhere it is kept. When Customer instructs Fieldstone to delete Contract Health Data, including to carry out an individual's request, Fieldstone will delete it from active systems no later than 30 days after receiving the instruction, or sooner if the law requires. Backup copies expire within the period the applicable Service Schedule states (30 days), or any shorter period the law requires; where the law would allow longer for backups or archives, Fieldstone still keeps to the Service Schedule's period. For consumer health data under Washington's My Health My Data Act, the permitted delay for archives and backups is in any case no more than six months after the request is authenticated, and it never extends the time for deleting from active systems. Fieldstone passes the deletion instruction to each Subcontractor that holds a copy within 5 Business Days, obtains its confirmation, and confirms completed deletion to Customer in writing on request. A request forwarded under section C.5 keeps its original receipt and authentication dates; forwarding does not restart any period. Fieldstone will not place Contract Health Data in the locked archive (Schedule B) or any other storage that would prevent deletion within these periods.

C.9 The law prevails over retention terms. If applicable law requires Fieldstone to delete, return or stop processing Contract Health Data sooner than a Service Schedule's retention terms provide, or to keep it longer, the law prevails and Fieldstone will tell Customer.

C.10 Showing compliance. Fieldstone will tell Customer promptly if it can no longer meet its obligations under this Schedule. On reasonable request, it will give Customer the information needed to show it is meeting them and will cooperate with reasonable assessments. Customer may take reasonable steps to stop and correct any unauthorized processing.