



End User License Agreement

BUSINESS CUSTOMER SUBSCRIPTION TERMS

Version Web 1.0 | Effective date October 10, 2026

Provider: AFH Care Portal LLC, a Wisconsin limited liability company, doing business as AFH Care Portal, with its address at 2917 International Ln, Suite 101, Madison, WI 53704 (Company, we, or us). Website: <https://www.afhcareportal.com>. Legal notices: support@afhcareportal.com and the address above. Privacy and security reporting: support@afhcareportal.com, (608) 512-8190.

1. Parties and acceptance

This Agreement is between Company and the adult family home or other business identified in the checkout acceptance record (Customer). Before checkout, an authorized representative must enter Customer's legal name, their own full name, title, and business email, review the displayed Agreement and subscription summary, affirmatively check the required boxes, and select Sign Agreement and Continue to Checkout. By doing so, that representative intends to electronically sign this Agreement on Customer's behalf and confirms authority to bind Customer. Company offers these terms through its authorized checkout process; a separate Company signature is not required. The Agreement is accepted when Company's system successfully records the signature and confirms acceptance. Service activation remains subject to completion of the order and any required BAA. Each person accessing the Service for Customer is an Authorized User and must comply with these terms. A staff user without contracting authority must refer acceptance to an authorized representative.

The Service is licensed for business use. Resident or guardian access, if offered, must be covered by an appropriate separate access agreement. Nothing here binds a resident, guardian, regulator, or other person who has not validly accepted applicable terms, or limits their rights under law.

2. Service scope and document priority

Service means the hosted AFH Care Portal software and the features purchased in the order. An order identifies the subscription period, fees, user or facility limits, included support, and any service levels. No unpurchased feature or custom service is promised. The Service assists with recordkeeping and administrative workflows; it does not provide resident care.

For PHI and HIPAA duties, the signed Business Associate Agreement (BAA) controls over conflicting terms. For other data processing matters, a signed data protection addendum controls. A signed negotiated amendment controls other conflicts, followed by the order, this Agreement, and expressly incorporated policies. A privacy notice does not authorize a use prohibited by the BAA or law.

3. License and acceptable use

During the subscription, Company grants Customer a limited, nonexclusive, nontransferable right to let its Authorized Users access the Service for Customer's lawful internal business purposes within purchased limits. Customer may not resell access, copy or distribute the software, defeat security controls, access another customer's information, upload malware, or reverse engineer the Service except to the extent a nonwaivable legal right permits it. Authorized security testing requires prior written coordination, except where law prohibits that restriction.

Customer must not falsify records, conceal abuse or reportable events, use the Service for unlawful discrimination or unlawful surveillance, or upload information it lacks authority to process. Company may investigate misuse while protecting confidentiality and complying with the BAA.

4. Accounts and customer responsibilities

Customer manages user authorization, uses unique accounts and required multifactor authentication, promptly removes access when staff leave, and protects devices and credentials. Customer must report suspected unauthorized access promptly through the security contact. Neither party is relieved of responsibility for its own systems or conduct by a shared responsibility arrangement.

Customer is responsible for the lawful collection and submission of its information, required notices and permissions, and the accuracy of records it creates or approves. Customer must verify entries, imports, calculations, reports, and reminders before using them for care, billing, regulatory submissions, or employment decisions. Customer retains responsibility for facility licensing, staffing, resident rights, record retention, and care obligations. Company remains responsible for duties applicable to Company under law and its agreements.

5. Care decisions and continuity

The Service does not provide medical, nursing, pharmacy, legal, tax, or compliance advice. Templates and alerts do not guarantee compliance, proper medication administration, reimbursement, inspection results, or any resident outcome. Qualified personnel must verify clinical information, medication orders, schedules, and care plans against appropriate authoritative sources.

The Service is not an emergency response system and is not continuously monitored for emergencies. Customer must use appropriate emergency services when necessary. Customer must maintain a practical downtime procedure and securely available records needed for essential care during outages. These responsibilities do not excuse Company's breach of an express service or data protection obligation.

6. Data ownership and permitted processing

As between the parties, Customer retains its rights in submitted resident, staff, and facility information (Customer Data), subject to individuals' rights and applicable law. Customer grants Company only the rights needed to host, secure, transmit, support, and otherwise provide the purchased Service as permitted by this Agreement, the BAA, and law. This grant does not transfer ownership of Customer Data.

Company will not sell Customer Data, use identifiable resident information for advertising, or train general purpose AI models on Customer Data. Identifiable health information may not be reused for unrelated product development. Any proposed deidentification, research, analytics beyond service delivery, or separate AI

processing requires an express written agreement and a lawful basis; the BAA and applicable law control. Customer may provide nonconfidential feedback without including resident or staff information; Company may use that feedback without payment.

7. Health information and required agreements

PHI means protected health information under HIPAA. Before Customer submits PHI for which Company acts as a business associate or business associate subcontractor, the parties must execute an appropriate BAA and confirm the contracted environment is approved for that processing. A signup checkbox, resident consent, cloud subscription, or this Agreement alone does not replace a required BAA. Company's legal duties can apply based on its actual activities even if a BAA was not signed.

Customer must accurately disclose its HIPAA role and intended data categories. If a customer is not HIPAA regulated, confidential resident information remains subject to applicable privacy and confidentiality laws and contractual safeguards. Substance use disorder records, specially protected state records, biometric data, and other specially regulated information require advance written review of applicable requirements and an appropriate addendum before upload.

For data already held without required agreements, both parties will promptly cooperate on lawful remediation, preserve relevant evidence, and maintain safeguards. Signing this Agreement does not retroactively authorize past processing or waive potential obligations to individuals or authorities.

8. Security and subcontractors

Company will maintain reasonable administrative, physical, and technical safeguards appropriate to the sensitivity of Customer Data and will comply with security requirements applicable to it. Company will maintain a documented risk assessment and risk management process, access controls, appropriate encryption, logging, backup and recovery procedures, workforce confidentiality obligations, and incident response procedures. Specific technical commitments and allocation of responsibilities belong in the signed security schedule.

Company may use qualified hosting and support subcontractors subject to confidentiality and appropriate data protection agreements. Where required, Company will obtain subcontractor BAAs before PHI processing and use services within the scope of those agreements. Company remains accountable for its contractual obligations and will make its current material data processing providers available to Customer on request. Customer does not authorize tracking or advertising technologies to receive resident information merely by accepting these terms.

9. Incidents and cooperation

Each party will promptly notify the other of a suspected compromise affecting Customer Data or Service access and cooperate in containment, investigation, evidence preservation, and remediation. Company will provide required reports without unreasonable delay and within any shorter period imposed by law or the BAA. Company will not delay a required initial notice solely because the investigation is incomplete.

The BAA governs PHI incident reporting, breach assessment, and notification responsibilities. Each party retains its own statutory reporting duties. Neither party may prevent legally required reporting, lawful complaints, or cooperation with authorities. Reasonable response costs will be allocated according to the BAA, any applicable addendum, legal responsibility, and proven causation; Customer is not automatically

responsible for Company caused incidents.

10. Fees, subscription, and support

Fees, billing frequency, subscription term, any renewal mechanism, cancellation process, and refund policy must be expressly stated in the order and disclosed before acceptance. No automatic renewal or charge for an additional term is authorized unless Customer expressly agrees to the renewal arrangement and applicable notice requirements are met. No pricing or renewal change applies retroactively.

Customer may dispute an invoice in good faith by promptly providing the reason; the parties will work to resolve it, and Customer must pay undisputed amounts. Company will give at least 15 days' written notice and an opportunity to cure before suspending solely for undisputed overdue fees. Support hours and response commitments are those in the order. No round the clock support or uptime guarantee applies unless expressly purchased. Health record access must not be improperly withheld as leverage for payment.

11. Availability and warranty disclaimer

Company will use commercially reasonable efforts to provide the purchased Service and support. Scheduled maintenance, security work, outages, and third party failures can affect availability. Any express service level commitment and remedy are those in the order; they do not displace mandatory legal duties.

TO THE MAXIMUM EXTENT PERMITTED BY LAW, EXCEPT FOR EXPRESS COMMITMENTS IN THE ORDER, THIS AGREEMENT, THE BAA, OR AN APPLICABLE ADDENDUM, THE SERVICE AND GENERAL INFORMATION ARE PROVIDED AS IS AND AS AVAILABLE. COMPANY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT. COMPANY DOES NOT GUARANTEE ERROR FREE OPERATION, UNINTERRUPTED ACCESS, COMPLETE DETECTION OF SECURITY THREATS, OR A PARTICULAR CARE, BUSINESS, OR REGULATORY RESULT.

These disclaimers do not negate express security or confidentiality promises, permit misleading statements, or exclude rights or duties that applicable law does not allow the parties to exclude. Third party integration terms apply to that third party's services, but do not remove Company's responsibility for its own integration or processing obligations.

12. Limits on contractual liability

SUBJECT TO THE EXCEPTIONS BELOW AND TO THE MAXIMUM EXTENT PERMITTED BY LAW, COMPANY'S TOTAL AGGREGATE LIABILITY TO CUSTOMER ARISING OUT OF THIS AGREEMENT OR THE SERVICE WILL NOT EXCEED THE GREATER OF USD 1,000 OR THE FEES PAID OR PAYABLE BY CUSTOMER FOR THE SERVICE DURING THE 12 MONTHS IMMEDIATELY BEFORE THE FIRST EVENT GIVING RISE TO THE CLAIM. RELATED EVENTS ARE TREATED AS ONE EVENT FOR THIS PURPOSE.

FOR COMPANY'S BREACH OF CONFIDENTIALITY, DATA PROTECTION, OR BAA OBLIGATIONS, THE PROPOSED AGGREGATE CAP IS THE GREATER OF USD 25,000 OR TWO TIMES THOSE 12 MONTH FEES, INSTEAD OF THE GENERAL CAP. REASONABLE, DOCUMENTED FORENSIC, REQUIRED NOTIFICATION, DATA RESTORATION, AND LEGALLY REQUIRED CREDIT MONITORING COSTS CAUSED BY THAT BREACH ARE DIRECT DAMAGES UNDER THIS CAP.

SUBJECT TO THE SAME EXCEPTIONS, COMPANY WILL NOT BE LIABLE TO CUSTOMER FOR INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES, OR LOST PROFITS, ARISING FROM

THE SERVICE, EVEN IF ADVISED OF THEIR POSSIBILITY. THE SPECIFIC RESPONSE COSTS IDENTIFIED ABOVE ARE NOT EXCLUDED MERELY BECAUSE THEY ARISE FROM A DATA INCIDENT.

Neither cap nor exclusion applies to Company's fraud, willful misconduct, gross negligence, death or bodily injury caused by its negligence, or liability that law forbids limiting. These terms do not cap regulatory fines or enforcement liability owed to authorities, restrict a nonparty's statutory rights, or excuse performance of mandatory HIPAA obligations. They allocate legally limitable contractual monetary remedies between the parties only. The BAA controls any conflict concerning PHI remedies. Customer's payment obligations and indemnity obligations are not subject to Company's liability caps.

13. Protection of owners and representatives

Customer agrees that Company alone is the provider and contracting party. No member, owner, manager, director, officer, employee, or authorized representative personally guarantees Company's performance or debts by signing or acting in a representative capacity. To the extent permitted by law, Customer will pursue contractual claims against Company rather than these individuals solely because of their role in Company.

Those individuals are intended third party beneficiaries solely of this section and applicable protections in Sections 12 and 14, subject to the same exceptions. This section does not release an individual from liability for their own fraud, willful misconduct, independently actionable conduct, an express personal guarantee, or duties or liability imposed by law. It does not prevent veil piercing where legally justified or bind regulators, residents, or other nonparties.

14. Customer indemnity

To the extent permitted by law, Customer will defend Company and its owners and representatives against third party claims arising from Customer's unlawful submission or disclosure of Customer Data, infringement by Customer supplied material, unauthorized use of the Service, or resident care acts or omissions attributable to Customer rather than Company. Customer will indemnify them for resulting final judgments and reasonable approved settlements and defense costs, but only to the extent caused by that conduct.

This indemnity does not cover Company's or an indemnified individual's own breach, negligence, fraud, willful misconduct, or violation of law. It does not transfer nondelegable legal duties or fines that law prohibits indemnifying. The indemnified party must give prompt notice, provide reasonable cooperation at Customer's expense, and allow Customer to control the defense with competent counsel. Delay reduces the obligation only to the extent materially prejudicial. No settlement may admit wrongdoing, impose nonmonetary duties, or fail to release an indemnified party without that party's written consent, not unreasonably withheld.

15. Suspension, termination, and data return

Company may promptly restrict access reasonably necessary to address an active security threat, unlawful use, or material risk to residents or other customers, with notice as soon as reasonably practicable. Other material breaches require written notice and 30 days to cure unless incapable of cure. Either party may terminate for an uncured material breach. Any additional BAA termination right remains effective.

On termination, Company will provide a secure, reasonably usable export of Customer Data upon an authorized request and a reasonable transition opportunity, ordinarily 30 days unless the BAA, law, or an agreed transition plan requires otherwise. Necessary access must not be unlawfully blocked because of a payment dispute. Customer must arrange compliant ongoing record retention; using the Service does not

transfer Customer's record custody obligations.

Return, destruction, backup treatment, and permitted retention of PHI are governed by the BAA. Other Customer Data will be deleted within 90 days after the export period unless law, a preservation obligation, or a written agreement requires retention. Backups will expire under the disclosed retention schedule and remain protected with restricted access. If PHI destruction or return is infeasible, Company will explain the reason and continue required protections and use restrictions. No deletion will override a legal hold or required record availability.

16. Changes, disputes, and general terms

Material changes to this Agreement require advance notice and affirmative acceptance and will not apply to earlier disputes or retroactively reduce data protections. Company may update operational features without materially reducing purchased functionality during a committed term. If a legal or security requirement demands an urgent operational change, Company will give notice as soon as practicable and preserve required protections.

Wisconsin law governs, excluding its conflict of laws rules, except where mandatory law requires otherwise. Subject to mandatory venue protections, disputes may be brought in state or federal courts with jurisdiction in Dane County. Before litigation, the parties will try in good faith to resolve a dispute for 30 days after written notice. This does not delay required reporting, emergency relief, or filing necessary to preserve a legal deadline. This Agreement imposes no mandatory arbitration, jury waiver, class action waiver, or shortened statutory claim period.

Neither party is the other's agent or partner. Customer may not assign the subscription without reasonable prior written approval, except in a lawful business succession with adequate safeguards. Company may assign it in a business transfer only if the successor assumes its obligations and applicable data protection requirements are met. An event beyond reasonable control may excuse affected performance only to the extent permitted by law, with prompt notice and reasonable mitigation; it does not excuse required safeguards, reporting, or protection of retained data.

If a provision is unenforceable, the remaining provisions continue to the extent legally permitted. Failure to enforce once is not a waiver. These terms and their identified incorporated documents form the complete agreement on the Service. Electronic signatures and counterparts may be used. Notices must go to the stated contacts, which each party must keep current. Confidentiality, lawful data handling, accrued payments, applicable liability limits, indemnities, dispute terms, and owner protections survive as appropriate to their purpose.

17. Electronic signature and checkout acceptance

Customer confirms that it reviewed this Agreement, particularly Sections 11 through 14, and the subscription summary displayed before signing. By typing the representative's full name, affirmatively checking the acceptance and electronic signature boxes, and selecting Sign Agreement and Continue to Checkout, the representative adopts that action as their electronic signature and intends to bind Customer. The representative signs solely in an organizational capacity, without a personal guarantee. An electronic signature does not itself authorize a payment or recurring charge. Any required BAA must be separately accepted and executed before PHI processing is authorized.

Electronic records and copies

Customer agrees to use electronic records for this Agreement, its acceptance record, and the related business subscription order. Before signing, Customer may view, download or print the full Agreement and subscription summary. Company will provide a retainable copy of the accepted version and signature receipt to the representative's business email and make them available through Customer's account. This consent does not extend to promotional messages, unrelated contracts, or records for which separate legally required consent is needed.

To access and retain these records, use an internet connected device, a current browser, an email account, and the ability to download or print HTML or PDF records. If Customer cannot access or retain them, do not sign electronically; contact support@afhcareportal.com for an alternative. Customer may request a paper copy at no charge or withdraw consent for future electronic contract records by contacting that address. Withdrawal does not undo an earlier signature or cancel the subscription; Company will coordinate an alternative delivery method for future required records. Customer must keep its notice email current. Material changes to access requirements will be disclosed with any additional consent required by law.