Business Associate Agreement and Service Level Agreement

Oct 13, 2026 · @Edward Conklin

Version: [v.102026.1] · **Governing law:** Nebraska

Cover Terms

These Cover Terms, Exhibit B (Business Associate Agreement) and Exhibit C (Service Level Agreement) are entered into between the following parties:

- **[Central Data Storage, LLC]**, a [Nebraska limited liability company] with its principal office at [1901 N 21st Street Ste. 273, Lincoln, NE 68508] ("**CDS**"); and
- the customer identified on the Execution Page ("**Customer**").

1. Effective date. This agreement takes effect on the date Customer signs or electronically accepts it, as recorded on the Execution Page (the "**Effective Date**").

2. Relationship to the Terms of Service. Exhibits B and C form part of the CDS Terms of Service between CDS and Customer (the "**Agreement**"). If documents conflict, they control in this order:

1. Exhibit B, as to Protected Health Information;
2. Exhibit C, as to service levels;
3. the Terms of Service, as to everything else.

3. Electronic acceptance and signatures.

3.1 **Consent to electronic transactions.** The parties agree to conduct this transaction by electronic means. This agreement, any amendment, and any notice under it may be created, delivered, signed and stored electronically. The parties intend this to have full effect under the federal Electronic Signatures in Global and National Commerce Act (15 U.S.C. §7001 et seq.) and the Nebraska Uniform Electronic Transactions Act (Neb. Rev. Stat. §86-612 et seq.).

3.2 **Methods of acceptance.** Customer may accept this agreement by any of the following methods, and each has the same legal effect as a handwritten signature:

- clicking an "I Agree" or "I Accept" button presented with this agreement, after typing the signer's full name and title;
- applying an electronic signature through an electronic signature service designated by CDS; or
- signing the Execution Page by hand and delivering a scanned copy (PDF) by email.

3.3 **Authority.** The individual who accepts this agreement represents and warrants that:

- he or she is at least eighteen (18) years old;
- he or she has authority to bind Customer; and
- Customer is the entity named on the Execution Page.

CDS may rely on that representation.

3.4 **Record of acceptance.** When Customer accepts electronically, CDS will record the following:

- the signer's name, title and email address;
- Customer's legal name;
- the date and time of acceptance (UTC);
- the internet protocol (IP) address used; and
- the version identifier of this agreement.

The record will be associated with an unalterable copy of the accepted version. Within one (1) business day, CDS will email a PDF copy of the accepted agreement and the acceptance record to the signer. CDS will keep the record and accepted version for at least six (6) years after this agreement ends (45 CFR 164.316(b)(2)).

3.5 **Copies.** Customer may download or print this agreement before and after accepting it. On request, CDS will provide a paper copy at no charge.

3.6 **No challenge based on electronic form.** Neither party will contest the validity or enforceability of this agreement, or of any signature on it, because it was formed, signed or delivered electronically. A copy of the electronic record, including a printout or PDF, is admissible as evidence to the same extent as a signed paper original.

3.7 **Counterparts.** This agreement may be signed in counterparts, including electronic counterparts, which together form one instrument.

3.8 **Amendments.** An amendment to Exhibit B or Exhibit C binds Customer only if Customer affirmatively accepts it by one of the methods in Section 3.2. Continued use of the Services does not constitute acceptance of such an amendment, except as provided in Exhibit B §17 and Exhibit C §8.4.

3.9 **Security of the acceptance process.** CDS will present this agreement over an encrypted connection and will protect acceptance records against alteration. Neither party will use the acceptance process to collect Protected Health Information.

Exhibit B — Business Associate Agreement

This Business Associate Agreement ("**BAA**") is part of the Agreement between CDS and Customer. It applies whenever Customer is a covered entity or a business associate under HIPAA and CDS creates, receives, maintains or transmits Protected Health Information for Customer. When Customer is itself a business associate, CDS is Customer's subcontractor, and this BAA is the agreement required by 45 CFR 164.502(e)(1)(ii) and 164.504(e)(5).

1. Definitions

1.1 Capitalized terms used but not defined in this BAA have the meanings given in 45 CFR Parts 160 and 164 (the "**HIPAA Rules**"), including Breach, Designated Record Set, Disclosure, Health Care Operations, Individual, Required by Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information and Use.

1.2 "**PHI**" means Protected Health Information, including electronic Protected Health Information, that CDS creates, receives, maintains or transmits on behalf of Customer.

1.3 "**Services**" means the backup, storage, restore and support services CDS provides under the Agreement, for the CDS-Client software.

1.4 "**Unsuccessful Security Incident**" means an attempted Security Incident that does not result in unauthorized access to, or Use, Disclosure, modification or destruction of, PHI, or in interference with system operations. Examples include pings, port scans, blocked log-in attempts, denial-of-service attempts that do not cause an outage, and malware blocked before it runs.

1.5 "**Service Data**" means operational data CDS generates about the Services, such as job status, error codes, storage volumes and performance metrics, excluding any PHI.

2. Permitted Uses and Disclosures

2.1 **Services.** CDS may Use and Disclose PHI only as necessary to perform the Services, as this BAA permits or requires, or as Required by Law.

2.2 **Management and administration.** CDS may Use PHI for its proper management and administration and to carry out its legal responsibilities. CDS may Disclose PHI for those purposes only if:

- the Disclosure is Required by Law; or
- CDS first obtains reasonable written assurances from the recipient that it will:
    - hold the PHI confidentially;
    - Use or further Disclose the PHI only as Required by Law or for the purpose for which it was disclosed; and
    - notify CDS of any instance in which the confidentiality of the PHI has been breached.

2.3 **Minimum necessary.** CDS will limit its Uses and Disclosures of, and requests for, PHI to the minimum necessary to accomplish the intended purpose.

2.4 **Limit.** CDS will not Use or Disclose PHI in any manner that would violate Subpart E of 45 CFR Part 164 if done by Customer, except as permitted by Section 2.2.

3. Disclosure Rules

CDS will Disclose PHI only to the recipients, and on the conditions, in the table below. All other Disclosures are prohibited.

Recipient	When CDS may or must Disclose	Conditions
Customer	Always, to perform the Services and on request.	Through the CDS-Client or a verified Customer contact.
A third party Customer designates (including a successor practice, a new vendor or Customer's attorney)	On Customer's written direction.	Customer is responsible for determining that the Disclosure would be permitted under the HIPAA Rules if made by Customer. CDS will verify that the direction is authentic before acting.

Recipient	When CDS may or must Disclose	Conditions
An Individual	Only where required for Customer to meet 45 CFR 164.524 (see 45 CFR 164.502(a)(4)(ii)); otherwise only on Customer's written direction.	CDS forwards all other Individual requests to Customer under Section 6.2.
The Secretary of HHS	On request, to determine compliance with the HIPAA Rules.	Section 9.2 applies. Unless prohibited by law, CDS will notify Customer of the request.
CDS Subcontractors	As necessary to perform the Services.	Only under a written business associate agreement meeting Section 7.
Courts, government agencies and law enforcement	Only when the Disclosure is Required by Law as defined in 45 CFR 164.103. This includes court orders, court-ordered warrants, and subpoenas or summons issued by a court, grand jury, inspector general or administrative body authorized to require production.	Unless prohibited by law, CDS will notify Customer before disclosing so Customer can seek a protective order. CDS will disclose only what the legal process requires.
Any other requester (including an attorney-issued subpoena, an informal law enforcement request, or a request from an Individual's family or insurer)	Not permitted.	CDS will refer the request to Customer within five (5) business days and will not respond on Customer's behalf unless Customer directs it in writing.
CDS's attorneys, auditors and insurers	For CDS's management and administration only.	Section 2.2 applies.

Prohibited Uses and Disclosures. CDS will not:

- sell PHI or receive any payment in exchange for PHI (45 CFR 164.502(a)(5)(ii));
- Use or Disclose PHI for marketing or fundraising;
- de-identify PHI or create a limited data set from it;
- aggregate PHI with data of other customers, including for data aggregation services;
- Use PHI, or any data derived from PHI, to develop, train, fine-tune or evaluate any machine-learning or artificial-intelligence model; or
- Disclose PHI to any affiliate of CDS for that affiliate's own purposes.

Service Data. CDS owns Service Data and may use it to operate, secure and improve the Services. File names, folder paths and other metadata that identify, or could reasonably be used to identify, an Individual are PHI and are not Service Data.

4. Safeguards

4.1 CDS will use appropriate administrative, physical and technical safeguards to prevent Use or Disclosure of PHI other than as this BAA provides. CDS will comply with Subpart C of 45 CFR Part 164 with respect to electronic PHI.

4.2 CDS will encrypt PHI at rest and in transit using encryption consistent with the Secretary's guidance specifying the technologies and methodologies that render PHI unusable, unreadable or indecipherable to unauthorized persons. This includes [AES-256 at rest and TLS 1.2 or higher in transit, implemented in FIPS 140-validated cryptographic modules].

4.3 CDS will not store Customer's system log-in credentials. CDS will access Customer's systems remotely only at Customer's request, through a session Customer can see and end at any time, and will log each session.

4.4 CDS will:

- maintain a written information security program;
- conduct an accurate and thorough risk analysis at least annually (45 CFR 164.308(a)(1)(ii)(A)); and
- train its workforce on HIPAA and on this BAA.

Once each year, on request, CDS will provide Customer with [a summary of its most recent independent security assessment or a completed security questionnaire].

5. Reporting

5.1 **Breaches of Unsecured PHI.** CDS will notify Customer of any Breach of Unsecured PHI without unreasonable delay and no later than ten (10) business days after discovery, determined under 45 CFR 164.410(a)(2). The notice will include, to the extent then known:

1. the identity of each affected Individual or, if CDS cannot identify Individuals because the data is encrypted with a key only Customer holds, the affected devices, folders and files;
2. a description of what happened;
3. the date of the Breach and the date of discovery;
4. the types of PHI involved; and
5. what CDS has done to investigate, contain and mitigate the Breach.

CDS will supplement the notice as more information becomes available.

5.2 **Other incidents.** CDS will report to Customer the following within ten (10) business days after CDS becomes aware of it:

- any Security Incident other than an Unsuccessful Security Incident; and
- any Use or Disclosure of PHI not provided for by this BAA.

5.3 **Unsuccessful Security Incidents.** The parties acknowledge that Unsuccessful Security Incidents occur routinely. This Section is notice of them, and no further report is required.

5.4 **Ransomware and availability events.** An event caused by malicious activity that encrypts PHI or makes it unavailable is a Security Incident. CDS will report it under Section 5.2 whether or not CDS concludes that a Breach occurred.

5.5 **Law enforcement delay.** CDS may delay a notice as permitted by 45 CFR 164.412.

5.6 **Notices to others.** Customer determines whether a Breach requires notice. Customer provides notices to Individuals, the Secretary and the media, unless the parties agree in writing that CDS will do so. Except as Required by Law, CDS will not notify Individuals or regulators about Customer's PHI without Customer's consent. CDS will cooperate with Customer to meet any state-law deadline shorter than those in this Section.

5.7 **Mitigation.** CDS will mitigate, to the extent practicable, any harmful effect known to CDS of a Use or Disclosure of PHI by CDS or its Subcontractors in violation of this BAA.

6. Individual Rights

6.1 CDS does not maintain a Designated Record Set for Customer in the ordinary course of the Services. To the extent CDS holds PHI that Customer needs to respond to an Individual, CDS will, within ten (10) business days after Customer's written request:

1. restore or provide the PHI so that Customer can meet 45 CFR 164.524;
2. make the PHI available for amendment and incorporate any amendments, as required by 45 CFR 164.526; and
3. provide the information Customer needs to provide an accounting of Disclosures under 45 CFR 164.528.

CDS will document its Disclosures of PHI as needed for that accounting.

6.2 If an Individual asks CDS directly for access, amendment or an accounting, CDS will forward the request to Customer within five (5) business days. CDS will not respond to the Individual except as provided in Section 3.

7. Subcontractors

7.1 Under 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), CDS will ensure that each Subcontractor that creates, receives, maintains or transmits PHI on CDS's behalf agrees in writing to the same restrictions, conditions and requirements that apply to CDS under this BAA. This includes each Subcontractor that stores PHI, even if it cannot decrypt the data.

7.2 CDS will keep a current list of these Subcontractors at [URL] or provide it on request. CDS will give Customer at least thirty (30) days' notice by email before adding a Subcontractor that will store or access PHI. If Customer reasonably objects on data-protection grounds within that period and the parties cannot resolve the objection, Customer may terminate the affected Services and receive a pro-rata refund of prepaid fees.

7.3 CDS is responsible for its Subcontractors' compliance with this BAA. If CDS learns of a pattern of activity or practice of a Subcontractor that is a material breach of the Subcontractor's obligations, CDS will take reasonable steps to cure the breach or end the violation. If those steps are unsuccessful, CDS will terminate the arrangement if feasible (45 CFR 164.504(e)(1)(iii)).

8. Data Location

CDS and its Subcontractors will store PHI only in the United States. They will not permit access to PHI from outside the United States without Customer's prior written consent.

9. Fees and Payment. This Section applies to the Services covered by Exhibits B and C. It controls over any conflicting payment terms in the Terms of Service.

9.1 **Fees and billing.** Customer will pay the fees for the plan selected on the Execution Page, monthly or annually in advance, using the payment method on file. Fees begin on [the date of the first completed backup]. They renew automatically on the anniversary date of each billing period until the Agreement ends. CDS may change fees on at least thirty (30) days' email notice, and the change takes effect at Customer's next renewal. Fees exclude applicable taxes.

9.2 **Annual plans; no refunds.** Annual plans are priced at a discount from monthly pricing. Because of that discount, fees for annual plans are non-refundable, in whole or in part. This applies if Customer cancels early, stops using the Services, or has its account cancelled for nonpayment. Monthly fees are non-refundable for the month in which they are charged. The only exceptions are refunds required by applicable law or expressly provided in:

- Exhibit B §7.2 (objection to a new Subcontractor);
- Exhibit B §11.2 (termination for CDS's material breach of the BAA); or
- Exhibit C §7 (chronic service failure).

9.3 **Customer's responsibility.** It is Customer's responsibility to keep its payment method current and its account paid up to date to avoid any disruption in service. CDS will email Customer's billing contact when a payment fails or is past due.

9.4 **Nonpayment; suspension and cancellation.** Failure to pay may cause a disruption in service or cancellation of Customer's account. If a payment is not received when due, CDS may take either of the following actions forty-eight (48) hours after emailing notice of the failed payment to Customer's billing contact:

- suspend the Services; or
- cancel Customer's account and terminate the Agreement.

9.5 **Access to stored data.** Even if the Services are suspended or cancelled for nonpayment, CDS will not block Customer's access to retrieve PHI already stored with CDS.

- **During a suspension,** CDS will stop accepting new backups, but Customer may still restore its existing data.
- **After cancellation,** Exhibit B §12 (retrieval period, then destruction) applies.

CDS may require payment of past-due fees before extending the retrieval period or shipping data on an encrypted drive. CDS will not require payment as a condition of retrieval through the CDS-Client during the retrieval period.

9.6 **Reinstatement.** If Customer pays all past-due amounts while the Services are suspended, CDS will reinstate the Services within one (1) business day after receiving payment. After cancellation, CDS may reinstate the account at its discretion if Customer pays all past-due amounts before Customer's data is destroyed. Backups missed during a suspension or cancellation cannot be recovered.

10. Customer Obligations Performed by CDS; Books and Records

9.1 To the extent CDS carries out any of Customer's obligations under Subpart E of 45 CFR Part 164, CDS will comply with the requirements of Subpart E that apply to Customer in performing those obligations.

9.2 CDS will make its internal practices, books and records relating to the Use and Disclosure of PHI available to the Secretary for purposes of determining compliance with the HIPAA Rules.

9.3 CDS will retain the documentation required by the HIPAA Rules for six (6) years from the date of its creation or the date it was last in effect, whichever is later (45 CFR 164.316(b)(2)).

11. Customer Obligations

Customer will:

1. not ask CDS to Use or Disclose PHI in any manner that would not be permitted under the HIPAA Rules if done by Customer;
2. notify CDS, to the extent it affects CDS's Uses or Disclosures, of:
    - any limitation in Customer's notice of privacy practices;
    - any restriction Customer agrees to under 45 CFR 164.522; and
    - any change in or revocation of an Individual's authorization;
3. select the data to be backed up and set retention consistent with Customer's own record-retention obligations; and
4. safeguard any encryption key Customer holds.

If Customer loses a key that only Customer holds, CDS cannot recover the data and is not responsible for that loss.

12. Term and Termination

11.1 This BAA takes effect on the Effective Date and continues until CDS no longer holds any PHI.

11.2 If either party determines that the other has violated a material term of this BAA, it may terminate the Agreement if the violation is not cured within thirty (30) days after written notice. If cure is not possible, it may terminate immediately (45 CFR 164.504(e)(2)(iii)). If Customer terminates under this Section, CDS will refund prepaid fees for the unused portion of the term, notwithstanding any no-refund provision in the Agreement.

13. Return or Destruction of PHI

12.1 **Retrieval period.** For thirty (30) days after the Agreement ends for any reason, CDS will keep Customer's PHI and allow Customer to retrieve it [through the CDS-Client or on an encrypted drive at the fee in CDS's price list]. On Customer's written request made before that period ends, CDS will extend it once by thirty (30) days at then-current fees.

12.2 **Destruction.** After the retrieval period, CDS will destroy all PHI using methods consistent with NIST Special Publication 800-88. On request, CDS will certify the destruction in writing. CDS will retain no copies except as provided in Section 12.3.

12.3 **When destruction is infeasible.** Copies of PHI in CDS's replicas, snapshots or write-once storage that cannot be selectively deleted will be destroyed when they expire in the normal rotation. That will happen no later than [ninety (90)] days after the retrieval period ends. For those copies, and for any other PHI whose return or destruction is infeasible, CDS will:

- tell Customer in writing what is retained and why;
- continue to protect it under this BAA; and
- limit further Uses and Disclosures to the purposes that make return or destruction infeasible, for as long as CDS holds it.

14. Independent Contractor

CDS performs the Services as an independent contractor and not as Customer's agent. Customer does not control the manner or means by which CDS performs the Services.

15. Liability and Insurance

15.1 **Breach costs.** If a Breach results from the failure of CDS or its Subcontractor to comply with this BAA, CDS will reimburse Customer's reasonable, documented out-of-pocket costs of:

- legally required notices to Individuals, regulators and the media;
- a call center for ninety (90) days;
- twelve (12) months of credit monitoring for Individuals whose Social Security, driver's license or financial account numbers were involved; and
- fines or penalties imposed by a governmental authority, to the extent caused by that failure.

15.2 **Data protection cap.** CDS's total liability arising from this BAA will not exceed the greater of [$100,000] or [three (3)] times the fees paid by Customer in the twelve (12) months before the event giving rise to the claim. This cap includes liability under Section 14.1 and any indemnity in the Agreement relating to PHI.

This cap is separate from, and in addition to, the general limitation of liability in the Agreement. Costs listed in Section 14.1 are direct damages for purposes of the Agreement's exclusion of consequential damages. Neither cap applies to a party's fraud or willful misconduct.

15.3 **Insurance.** During the Agreement, CDS will maintain cyber liability and technology errors and omissions insurance with limits of at least [$1,000,000 per claim and in the aggregate]. CDS will provide a certificate of insurance on request.

16. Substance Use Disorder Records

If Customer notifies CDS in writing that it will store records subject to 42 CFR Part 2, then for those records CDS:

- acknowledges that, in receiving, storing, processing or otherwise dealing with any such records, it is fully bound by 42 CFR Part 2;
- will, if necessary, resist in judicial proceedings any effort to obtain access to the records except as permitted by 42 CFR Part 2; and
- will protect the records under this BAA and 42 CFR 2.16.

17. State Law and Non-PHI Health Data

CDS will process personal information and consumer health data that is not PHI only to provide the Services and on Customer's instructions. CDS will not sell or share it, and will not retain, use or disclose it for any other purpose. CDS will comply with state laws that apply to CDS as a service provider or processor, including the following:

- Cal. Civ. Code §1798.100 et seq.;
- RCW ch. 19.373; and
- Tex. Health & Safety Code ch. 181.

18. Change in Law

If the HIPAA Rules/HIPAA 2.0 or other applicable law change in a way that affects this BAA, the parties will amend this BAA as needed to comply. If they cannot agree on an amendment within sixty (60) days, either party may terminate the affected Services without penalty. A new legal obligation applies to CDS under this BAA from its compliance date.

189. Miscellaneous

19.1 **Precedence.** If this BAA conflicts with the Agreement or Exhibit C, this BAA controls as to PHI.

19.2 **Interpretation.** Any ambiguity will be resolved to permit compliance with the HIPAA Rules. A reference to a regulation means that regulation as amended.

19.3 **Amendment.** This BAA may be amended only in a writing signed or electronically accepted by both parties under Section 3 of the Cover Terms, or under Section 17. CDS may not change this BAA unilaterally.

19.4 **No third-party beneficiaries.** Nothing in this BAA confers rights on any person other than the parties.

19.5 **Survival.** Sections 5, 6.1, 9.2, 12, 13, 14 and 18 survive termination for as long as CDS holds PHI.

Exhibit C — Service Level Agreement

This Service Level Agreement ("**SLA**") is part of the Agreement between CDS and Customer. Capitalized terms not defined here have the meanings given in the Agreement or Exhibit B.

1. Scope

This SLA covers two service components:

- **Backup Ingest:** the ability of CDS Servers to accept and store backup data sent by a properly configured CDS-Client.
- **Restore Access:** the ability of Customer to start a folder-level restore through the CDS-Client, or to submit a file-level restore request to CDS support.

This SLA does not cover Customer's computers, networks or internet service.

2. Availability

2.1 **Target.** CDS will make Backup Ingest and Restore Access each available at least [99.5%] of each calendar month ("**Monthly Availability**").

2.2 **Measurement.** CDS checks each component automatically from at least [two (2)] network CDS's data centers.

2.3 To preform client support CDS must have Administrative rights through remote access to make appropriate changes to run the UnisonBDR software CDS's monitoring records are the records of measurement.

3. Exclusions

The following time is "**Excluded**" and does not count as Unavailable:

1. **Scheduled maintenance:** maintenance within [Sundays, 12:00 a.m. to 6:00 a.m. Central Time], announced by email at least [seventy-two (72)] hours in advance, up to [eight (8)] hours per month.
2. **Emergency maintenance:** maintenance needed to address an active security threat, announced as soon as practicable, up to [four (4)] hours per month. Time beyond that limit counts as Unavailable.
3. **Customer causes:** Customer's equipment, network or internet service; a CDS-Client version more than [two (2)] major releases behind the current version; Customer exceeding its purchased storage; loss of a Customer-held encryption key; or Customer's breach of the Agreement.
4. **Suspension:** a suspension permitted by the Agreement.
5. **Force majeure:** an event described in the force majeure clause of the Agreement. A failure of CDS's primary data center or hosting provider is not force majeure unless the event also prevents [CDS's secondary facility] from operating.
6. **Public internet:** a failure of the public internet outside the networks of CDS and its Subcontractors.

5. Backup Monitoring and Data Commitments

5.1 **Job monitoring.** CDS monitors each scheduled backup job.

- If a job fails, completes with errors or does not run as scheduled, CDS will send an automated alert to Customer's designated contact within [one (1) business day].

- If the problem continues for [two (2)] consecutive scheduled jobs, customer or CDS will call to open a case and work to resolve the issue.
- 5.2 **Integrity checks.** CDS verifies each backup set against test restore records when received and re-verifies stored data per customer cadence upon setup. If CDS detects corruption in stored data, it will notify Customer within [one (1) business day]. Where the source data is still available, CDS will request a new backup of it.

5.3 **Recovery point.** Customer sets the backup schedule and selects the data to back up. The recovery point for any file is the most recent backup of that file that completed successfully. CDS does not commit to a recovery point objective independent of Customer's schedule and equipment.

5.4 **Recovery time.** Restore completion time depends on data volume and Customer's internet bandwidth, and CDS does not guarantee it. CDS commits that:

- Restore Access is subject to the availability target in Section 2;
- CDS will begin work on a file-level restore request within the Severity 2 response time in Section 6; and
- for a full restore larger than [500 GB], CDS will, on request, ship Customer's data on an encrypted drive within [two (2) business days], at the fee in CDS's price list.

5.5 **Redundancy.** CDS stores each backup in at least [two (2)] copies [in two geographically separate facilities in the United States].

5.6 **Retention and versions.** CDS retains prior file versions for the period stated in Customer's plan.

5.7 **Restore testing.** On request, CDS will assist Customer with one test restore per [calendar quarter] at no charge and will confirm in writing that the test was completed. CDS will provide a record of each test restore on a desk top folder. Customer is responsible for validating restored data in its own applications.

6. Support

Support is available [Monday through Friday, 8:00 a.m. to 6:00 p.m. Central Time, excluding U.S. federal holidays] by phone at [support phone number] and by email at [support email address].

Severity	Definition	Response time	Resolution target
1 – Critical	Backup Ingest or Restore Access is Unavailable for Customer, or Customer has an active data-loss event (such as ransomware) and needs a restore.	8:00am-7:00pm Monday-Friday	Workaround in place or restore started during the response
2 – High	Backups failing repeatedly; a file-level restore request; restores significantly	8:00am-7:00pm Monday-Friday	[1 business day]

Severity	Definition	Response time	Resolution target
	degraded.		
3 – Normal	A single failed job; configuration questions; storage-limit issues.	8:00am-7:00pm Monday-Friday	[3 business days]
4 – Low	General questions and feature requests.	8:00am-7:00pm Monday-Friday	Reasonable efforts

"Response" means a qualified CDS technician has acknowledged the issue and begun work. An automated reply is not a response. Resolution times are targets, not commitments.

8. Relationship to the BAA and the Agreement

8.1 An outage, failed backup or degraded service is not by itself a Security Incident. Any event that may involve unauthorized access to PHI, or that makes PHI unavailable because of malicious activity, is handled under Section 5 of Exhibit B. That applies whether or not the event also affects Monthly Availability.

8.2 If CDS activates its disaster recovery or contingency plan in a way that affects Customer's data, CDS will notify Customer promptly, and in any event within [forty-eight (48)] hours.

8.3 This SLA describes service levels and is not a warranty that the Services will be uninterrupted or error-free. If this SLA conflicts with the Agreement, this SLA controls as to service levels, and Exhibit B controls as to PHI.

8.4 CDS may update this SLA on thirty (30) days' notice by email. No update may reduce any of the following during Customer's then-current term:

- the availability target;
- credit percentages; or
- support response times.

Execution Page

By signing below, or by accepting electronically under Section 3 of the Cover Terms, each party agrees to the Cover Terms, Exhibit B (Business Associate Agreement) and Exhibit C (Service Level Agreement). Version [CDS-BAA-SLA-2026.1].

[CENTRAL DATA STORAGE, LLC]	CUSTOMER
Signature: _____	Signature: _____
Name: _____	Customer legal name: _____
Title: _____	Signer name: _____

[CENTRAL DATA STORAGE, LLC]	CUSTOMER
Date: _____	Title: _____
Notice email: _____	Date: _____
	Address: _____
	Notice and incident contact email: _____
	Customer type (check one): ☐ Covered entity ☐ Business associate
	Stores 42 CFR Part 2 records: ☐ Yes ☐ No

Electronic acceptance record

CDS completes this record automatically when Customer accepts electronically. It forms part of this agreement.

Field	Value
Agreement version	[CDS-BAA-SLA-2026.1]
Customer legal name	
Signer name and title	
Signer email	
Acceptance method	☐ Click-through ☐ E-signature service ☐ Signed PDF
Date and time of acceptance (UTC)	
IP address	
Acceptance record ID	
Copy emailed to signer (date)	

Click-through acceptance text (to appear directly above the "I Agree" button):

> *I have read the Cover Terms, Business Associate Agreement and Service Level Agreement, version [CDS-BAA-SLA-2026.1]. I have authority to bind the customer named above, and I agree on its behalf. I agree that my electronic acceptance is a signature with the same effect as a handwritten signature. [Name] [Title] [I Agree]*