

CADReport — Terms of Service

CADReport LLC · Effective date: 2026-07-28

"You"/"your" means the customer (the fire department or its authorized entity).

"We"/"us"/"CADReport" means CADReport LLC.

1. Agreement to Terms

1.1 These Terms of Service (the "**Terms**") are a contract between you and CADReport. By creating an account, accessing, or using the CADReport service (the "**Services**"), you agree to these Terms. If you do not agree, do not use the Services.

1.2 **Authority to accept.** The person accepting these Terms represents that they are authorized to bind the department or organization to this contract. If you are accepting on behalf of a department, "you" means that department.

1.3 If your department is or becomes a HIPAA covered entity, or enables any feature that stores patient health information, the **Business Associate Agreement ("BAA")** also applies and is incorporated into these Terms (see §21). For anything involving patient health information, the BAA controls.

2. Definitions

2.1 "**Services**" — the CADReport records-management system and related features described in §3.

2.2 "**Customer Data**" — the data you and your users put into or generate in the Services (incident records, personnel information, apparatus checks, and similar).

2.3 "**Authorized User**" — a person you permit to use the Services under your account (department members and staff).

2.4 "**PHI (Protected Health Information)**" — patient health information as defined by HIPAA. **PHI is governed by the BAA, not these Terms.** These Terms defer to the BAA on anything involving PHI and do not restate its rules.

2.5 Capitalized terms that HIPAA defines (such as PHI, Breach, Security Incident) carry their HIPAA meanings, for consistency with the BAA.

3. Description of the Services

3.1 CADReport is a **records-management system (RMS)** for fire departments. It ingests dispatch (CAD) data into run sheets and helps you produce incident reports — including reports for the federal NERIS reporting program — along with related tools: an audit trail, training and personnel records, apparatus/truck checks, pre-incident planning, a map, and integrations.

3.2 **CADReport is not a patient-care reporting system (not an ePCR).** It is not designed to hold full patient-care records. It stores the standard incident fields a fire RMS receives (such as address, incident type, times, and reporting party). Do not load full patient-care narratives or detailed clinical information into it.

3.3 We may add, change, or remove features over time. We will not make a change that materially reduces the core Services during a paid term without notice (see §16 and §23).

4. License & Access Grant

4.1 **What you may do.** We grant you a limited, non-exclusive, non-transferable, non-sublicensable right to access and use the Services for your department's own operations during your subscription.

4.2 **Per-tenant / per-user scope.** The right extends to your department (your "tenant") and your Authorized Users only.

4.3 **What you may not do.** You may not (a) resell, rent, or provide the Services to a third party as a service bureau; (b) reverse engineer, decompile, or try to extract the source code, except where law forbids that restriction; (c) use the Services to build or benchmark a competing product; (d) use the Services to train machine-learning or AI models without our written consent; or (e) access the Services beyond the features or limits you've subscribed to.

5. Accounts, Eligibility & Tenancy

5.1 **Registration.** You provide accurate account information and keep it current.

5.2 **Account security.** You are responsible for keeping your account credentials secure and for all activity under your account. Notify us promptly if you believe an account has been compromised.

5.3 **Authorized Users.** You are responsible for your Authorized Users' use of the Services and for their compliance with these Terms.

5.4 **Per-tenant isolation.** Each department's data lives in its own separate database. One department cannot see another's data.

6. HIPAA Status & Covered-Entity Attestation

6.1 **Your determination, not ours.** Whether your department is a HIPAA "covered entity" is a determination only your department can make, based on its own operations and, if needed, its own legal counsel. **CADReport does not determine, assess, or indicate your department's covered-entity status, and nothing in the Services does so.**

6.2 **Official resources.** We link the federal government's official **CMS Covered Entity Decision Tool** and related HHS guidance so your department can make its determination using the government's own resources.

6.3 **Your attestation.** During onboarding your department attests whether it is a covered entity. If you attest that you are — or you elect the BAA voluntarily — a signed BAA is required before any PHI is stored in the Services. If you attest that you are not, the BAA does not apply; your data remains protected under these Terms regardless.

6.4 **Recorded.** Your attestation is recorded with a timestamp and the identity of the person who made it, and kept as part of your account record. You are responsible for updating it if your operations change (for example, if your department begins billing electronically, directly or through a billing service).

6.5 **Not legal advice.** The linked resources are the government's; we provide access to them, not advice about them.

7. Acceptable Use & Customer Responsibilities

7.1 **Use the Services lawfully** and only for your department's legitimate operations.

7.2 **Do not** (a) upload unlawful, infringing, or malicious content; (b) attempt to breach or probe security, or access data that isn't yours; (c) interfere with or overload the Services; or (d) misuse the Services in a way that exposes protected information unnecessarily.

7.3 **Your own compliance.** You are responsible for using the Services in a compliant way — including configuring the PHI-protection controls we provide (see §10–§12) and limiting the patient information you submit to the minimum necessary. We provide the controls and safe defaults; you own the decision to relax them and own the physical environment where the Services are displayed or heard.

7.4 **Compliance requirements are yours to determine and configure.** The Services include tools to track and report on compliance requirements (such as apparatus/equipment checks, training, and inspections). You are responsible for determining whether each requirement is binding on your department by your **Authority Having Jurisdiction ("AHJ")** or is an **internal best practice**, and for configuring each requirement accordingly. CADReport provides the tracking and reporting tools; it does **not** determine which standards or requirements apply to or bind your department. The reports the Services generate indicate, for each requirement, the designation you configured, so each report reflects your department's decision.

7.5 **Devices and access are yours to control.** You are responsible for the devices used to access the Services — including **personal devices** (phones, tablets, home computers) that your members use through a web browser or any CADReport application. This includes keeping those devices reasonably secure, controlling who you give the **department access code** to, and ensuring the Services are viewed only by authorized people and not the public. The protections we provide (such as the PHI filter in §10) are enforced on our servers before information reaches any device; the specific safeguards are determined by CADReport and may evolve, while the device itself, and who holds the access code, remain yours to manage.

8. Customer Data, Data Protection & Data License

8.1 **You own your data.** All Customer Data remains yours. Ending the Services does not transfer ownership to us.

8.2 **Limited license to run your service — single-tenant scope.** You grant us a limited license to host, store, process, and transmit your Customer Data **solely to provide the Services to you**. We do **not** use your data for our own analytics, product development, advertising, or any cross-customer purpose. We do **not** de-identify, mine, sell, or repurpose your data.

8.3 **Personnel information.** Your staff's personal information — name, address, rank, emergency contact, and similar — is Customer Data protected under this section and processed only to run your department's service. It is **not** PHI, is **not** governed by the BAA, and is **not** de-identified or repurposed.

8.4 Confidentiality and protection. We protect Customer Data with administrative, physical, and technical safeguards, including encryption in transit and at rest. Even for departments that are **not** HIPAA covered entities, your data is protected under these Terms and any applicable state confidentiality law — "not a covered entity" never means "not protected."

8.5 Privacy Policy. Our separate **Privacy Policy** describes how we handle personal information, and includes an acknowledgment of applicable state privacy rights (such as California's).

8.6 PHI is governed by the BAA. This section defers to the BAA for anything involving PHI and does not restate PHI terms.

8.7 Operations. We operate, maintain, and protect the infrastructure of the Services. We may access Customer Data and may move a customer's instance, data, or backups between CADReport resources — always within the United States — as needed to provide, maintain, support, or protect the Services, including in response to outages, inadequate resource conditions, load balancing, hosting issues, security events, and planned maintenance. Where conditions require immediate action, we may act without prior notice.

9. Intellectual Property & Proprietary Rights

9.1 We own all right, title, and interest in the Services — the software, platform, design, and any improvements, including improvements suggested by or derived from customer feedback. These Terms grant you a right to use the Services (§4), not any ownership of them.

9.2 You keep all rights in your own Customer Data (§8). Nothing here transfers your data ownership to us.

9.3 Feedback. If you send us suggestions, we may use them to improve the Services without obligation to you.

10. Incident List

10.1 What it is. The incident list is the landing page at department login. It shows current and historical incidents in configurable categories and refreshes when a new incident arrives.

10.2 Protected information — the PHI filter. The incident list can surface an incident's address. For every incident category, the address is withheld from shared or unattended displays once the incident is no longer operationally active; the incident type and subtype remain shown, and individually signed-in access to the full record is recorded. During an incident and for a brief operational period afterward, the address stays openly viewable for operational needs. This protection is on by default for every category; you may turn it off for any category in the CAD category settings, at your own discretion and responsibility. The specific safeguards are determined and maintained by CADReport and may change as the product evolves.

10.3 Your responsibility. You are responsible for the physical placement of any screen showing the incident list, so it is visible only to responders and not the public, and for any decision to turn off the PHI filter.

11. AV Alerts / Enable Sound

11.1 **What it is.** "AV Alerts" (admin) and "Enable Sound" (browser) reproduce an audio and/or visual output when a dispatch transmission changes an incident's status.

11.2 **Not an alerting system.** This feature is **not** a primary, backup, or reliable source of incident alerting. It may fail to activate, activate late, or activate in error. You must rely solely on your own certified alerting equipment. The feature is provided **as is**, without warranty of any kind.

11.3 **Protected information.** Audio or visual output can include PHI (incident type and address). Announcement of the **address** is off unless you configure it on **and** a named user acknowledges enabling station-wide announcement of the address; that acknowledgment is recorded.

11.4 **Your responsibility.** You are responsible for the physical placement of any speaker or display used for this feature, so output reaches only responders and not the public, and for what the feature is configured to announce.

12. Map

12.1 **What it is.** The map shows incidents and operational layers (water sources, hazards, boundaries, pre-plans, stations, and incident layers) for your area. It is an operational tool available whether or not a user is logged in.

12.2 **Protected information.** The EMS / medical incidents layer can surface PHI (medical incident location). This layer is **off by default**. Any user may turn it on; by enabling the medical category you accept responsibility for the PHI it then displays.

12.3 **Response mode.** When an incident is live, the map's response mode shows operational detail for that incident — including prior incidents at the address, nearest hospitals, and landing zones — for the responding personnel. This is a permitted operational use and remains fully available.

12.4 **Your responsibility.** You are responsible for the physical placement of any screen showing the map, so PHI reaches only responders and not the public, and for any decision to enable the medical incidents layer.

13. Confidentiality

13.1 **Confidential Information** means non-public information one party shares with the other that is marked or would reasonably be understood as confidential — including the non-public parts of the Services and your non-public business information.

13.2 Each party will use the other's Confidential Information only to perform under these Terms, protect it with reasonable care, and not disclose it except to people who need it and are bound to keep it confidential.

13.3 **Exclusions.** Confidential Information does not include information that is public through no fault of the receiver, already known without a duty of confidence, independently developed, or rightfully received from someone else.

13.4 This section runs alongside — and does not override — the BAA's PHI obligations. For PHI, the BAA controls.

14. Fees & Payment

14.1 Fees, billing frequency, and any usage limits are stated in your **Contract or order form**, not in these Terms. During a free trial, no fees apply.

14.2 **Taxes.** Fees are exclusive of taxes; you are responsible for any applicable taxes other than taxes on our income.

14.3 **Non-payment.** If fees are past due, we may suspend the Services after reasonable notice. Suspension for non-payment does not delete your data during the retention period in §15.

15. Term & Termination

15.1 **Term.** These Terms apply for as long as you use the Services or have an active subscription.

15.2 **Cancellation.** Cancellation is requested by an authorized representative of your department contacting us; there is no self-service cancellation control. On a confirmed cancellation request, the Services are suspended for seven (7) days, after which your Customer Data is offloaded to a coordinated location for your download, with any security keys for that data provided directly to your authorized representative. Cancellation stops future billing.

15.3 **Termination for cause.** Either party may terminate if the other materially breaches these Terms and fails to cure within **thirty (30) days** of written notice (or immediately where cure is not feasible).

15.4 **Effect of termination.** On termination, your access ends and your Customer Data is made available as described in §15.2. Thirty (30) days after the data is made available for download, we delete our copies (routine encrypted backups age out per our backup schedule) — except where applicable law requires a different retention or preservation period, in which case the legally required period controls. For PHI, the BAA's return-or-destroy obligation applies **in addition** to this section.

16. Warranties & Disclaimers

16.1 **Our limited promise.** We will provide the Services with reasonable skill and care.

16.2 **"As is" for everything else.** Except for §16.1, the Services are provided **"as is"** and **"as available."** We disclaim all other warranties, express or implied, including implied warranties of merchantability, fitness for a particular purpose, and non-infringement, to the fullest extent the law allows.

16.3 **No warranty of your compliance.** Using the Services does not guarantee your department's own HIPAA or other legal compliance — that remains your responsibility (§7.3, and the BAA).

16.4 **The AV/alerting feature** is specifically not warranted (§11.2); do not rely on it for alerting.

17. Limitation of Liability

17.1 **No indirect damages.** Neither party is liable to the other for any indirect, incidental, special, consequential, exemplary, or punitive damages, or for lost profits, lost revenue, or lost

data, arising out of or relating to these Terms or the Services, even if advised of the possibility of such damages.

17.2 General cap. Except as stated in §17.3, each party's total cumulative liability arising out of or relating to these Terms and the Services will not exceed the total fees paid by the customer to CADReport in the twelve (12) months before the event giving rise to the liability.

17.3 Exclusions from the cap. The cap in §17.2 does not apply to: (a) a party's gross negligence or willful misconduct; (b) a party's breach of its confidentiality obligations; (c) a party's indemnification obligations under §18; or (d) liability that applicable law does not permit to be limited. Liability arising from a breach of protected health information is governed by the BAA §6.3, which controls for such matters.

17.4 One recovery. The limits in this section and in the BAA are cumulative ceilings, not additive; the same loss is not recovered twice under both documents.

18. Indemnification

18.1 Mutual, fault-based. Each party (the "indemnifying party") will defend, indemnify, and hold harmless the other party from third-party claims and government fines and penalties to the extent they arise from the indemnifying party's own (a) breach of these Terms, (b) gross negligence or willful misconduct, or (c) violation of applicable law. Neither party indemnifies the other for the portion of any loss caused by the other party's own act or omission.

18.2 PHI matters. Claims arising from protected health information are governed by BAA §6.2, which controls; this section covers non-PHI claims and does not restate or expand PHI obligations.

18.3 Process. The indemnified party will promptly notify the indemnifying party of the claim, allow the indemnifying party to control the defense (with counsel reasonably acceptable to the indemnified party), and cooperate. No settlement that imposes any obligation on the indemnified party is made without its consent.

19. Insurance

19.1 CADReport will maintain, at its own expense, cyber-liability / privacy-liability insurance with limits of at least **\$1,000,000 per claim and in the aggregate** for the term of the Services. On written request, CADReport will provide a certificate of insurance evidencing this coverage.

20. Relationship of Agreements

20.1 These Terms are the master agreement between you and CADReport. The **BAA is incorporated into these Terms** by reference for any department to which it applies.

20.2 Order of precedence. For anything involving PHI, the **BAA controls**. For all other matters, **these Terms control**. A separate signed order form or Contract controls over these Terms only for the specific commercial terms it states.

21. Governing Law & Dispute Resolution

21.1 These Terms are governed by the laws of the **Commonwealth of Pennsylvania**, without regard to conflict-of-laws rules.

21.2 **Informal resolution first.** The parties will try in good faith to resolve any dispute informally before starting formal proceedings.

21.3 **Venue.** The state and federal courts located in **Chester County, Pennsylvania** have exclusive jurisdiction over any dispute not resolved informally, and each party consents to that venue.

22. Changes to These Terms

22.1 We may update these Terms. For **material** changes we will give notice and, where the change materially affects your rights or obligations, obtain your acceptance before it applies to you. Minor changes take effect on notice.

22.2 This works together with the BAA's "amend to comply with law" clause and the versioning-and-re-consent mechanism.

22.3 **Changes required by law.** If a change to the Services or to these Terms is required by applicable law, regulation, or a governmental authority, we may make that change effective on notice, without waiting for acceptance; where the change is material, the notice will identify the legal basis. If a change required by law materially reduces the core Services for the remainder of a paid term, you may terminate and receive a pro-rata refund of prepaid, unused fees.

23. General / Miscellaneous

23.1 **Assignment.** You may not assign these Terms without our written consent. We may assign them in connection with a merger, acquisition, or sale of assets.

23.2 **Severability.** If any provision is unenforceable, it is modified to the minimum extent necessary to make it enforceable, and the rest stays in effect.

23.3 **No waiver.** Not enforcing a provision once doesn't waive the right to enforce it later.

23.4 **Notices.** Formal notices (breach, termination, assignment) must be in writing to the contact each party designates; routine in-app or email notices are fine for everything else.

23.5 **Force majeure.** Neither party is liable for a failure or delay caused by events beyond its reasonable control (acts of God, war, terrorism, pandemic, government action, network or utility failures).

23.6 **Entire agreement.** These Terms, the BAA (where it applies), the Privacy Policy, and any order form or Contract are the entire agreement and supersede prior discussions on their subject.

23.7 **Counterparts / e-signature.** These Terms and the BAA may be accepted electronically, which is binding.