
QUEEN CITY MEDICAL TRANSPORT

Data Privacy and Security Policy

Version 1.0 | Effective Date: October 16, 2026 | Document Owner: Privacy & Security Officer

■ **CONFIDENTIAL — INTERNAL USE ONLY**

Queen City Medical Transport

DATA PRIVACY AND SECURITY POLICY

Version: 1.0

Effective Date: October 16, 2026

Reviewed By: Privacy & Security Officer

Approved By: Senior Leadership

This document contains confidential and proprietary information belonging
to Queen City Medical Transport.

Unauthorized distribution is strictly prohibited.

TABLE OF CONTENTS

- 1. Purpose and Scope
- 2. Definitions
- 3. Legal and Regulatory Framework

4. Protected Health Information (PHI) – Privacy Protections

4.1 Use and Disclosure of PHI

4.2 Minimum Necessary Standard

4.3 Verbal Communications

4.4 Paper Records

4.5 Patient Rights

5. Electronic Data Security (ePHI Safeguards)

5.1 Administrative Safeguards

5.2 Physical Safeguards

5.3 Technical Safeguards

5.4 Password and Access Management

5.5 Network Security

5.6 Mobile Device Policy

6. Personally Identifiable Information (PII) – Data Protection

7. Business Associate Obligations

8. Intellectual Property and Proprietary Data Protection

9. Data Retention and Disposal

10. Incident Response and Breach Notification

10.1 What Constitutes a Security Incident

10.2 Reporting Obligations

10.3 Incident Response Steps

10.4 Breach Notification Timeline

10.5 Documentation

11. Employee Training and Awareness

12. Enforcement and Disciplinary Action
13. Policy Review and Updates
14. Contact Information and Privacy Officer
15. Acknowledgment

1. Purpose and Scope

This Policy establishes the standards that **Queen City Medical Transport** (hereinafter "the Company") follows to protect the privacy, confidentiality, integrity, and security of patient and client information in accordance with applicable federal and state law. The Company is committed to maintaining the trust of those it serves by handling all data responsibly and lawfully.

Applicability

This Policy applies to:

- All full-time and part-time employees
- Contractors, subcontractors, and temporary workers
- Volunteers and interns
- Vendors, suppliers, and business associates
- Any other individual or entity that accesses, handles, transmits, or stores Company data in any capacity

Scope of Data Covered

This Policy covers all formats and media in which data may exist, including:

- **Electronic data** – databases, emails, cloud storage, mobile devices, laptops, desktops, servers

- **Paper records** – printed files, forms, trip logs, patient manifests, correspondence
- **Verbal communications** – spoken conversations in person or by telephone
- **Any other media** – photographs, faxes, audio recordings, or any format that contains protected information

Compliance with this Policy is mandatory. Failure to comply may result in disciplinary action, up to and including termination of employment or contract, and may expose individuals to civil or criminal liability.

2. Definitions

The following terms are used throughout this Policy. All personnel subject to this Policy are expected to understand and apply these definitions in their daily work.

Term	Definition
Protected Health Information (PHI)	Individually identifiable health information that is transmitted or maintained in any form or medium — including electronic (ePHI), paper, or verbal. PHI includes information relating to an individual's past, present, or future physical or mental health condition; provision of health care; or payment for health care.
Electronic PHI (ePHI)	PHI that is created, stored, transmitted, or received in electronic form. ePHI is subject to both the HIPAA Privacy Rule and the HIPAA Security Rule.
Personally Identifiable Information (PII)	Any information that can be used, alone or in combination with other data, to identify a specific individual. Examples include full name, home address, Social Security Number

Term	Definition
	(SSN), date of birth, driver's license number, financial account information, and biometric data.
HIPAA	The Health Insurance Portability and Accountability Act of 1996. A federal law establishing national standards for the protection of sensitive patient health information from being disclosed without the patient's consent or knowledge.
HITECH	The Health Information Technology for Economic and Clinical Health Act of 2009. An act that strengthened HIPAA enforcement, expanded business associate obligations, and established breach notification requirements.
Business Associate	A person or entity that performs functions or activities on behalf of, or provides services to, Queen City Medical Transport that involve the use or disclosure of PHI. Examples include billing companies, IT vendors, and legal counsel.
Covered Entity	A health plan, health care clearinghouse, or health care provider that transmits health information in electronic form in connection with a standard transaction as defined under HIPAA.
Data Breach	The unauthorized acquisition, access, use, or disclosure of PHI or PII that compromises the security or privacy of the information and poses a significant risk of financial, reputational, or other harm to the individual whose information was affected.
Minimum Necessary Standard	The HIPAA principle that use of and access to PHI and PII must be limited to the minimum amount necessary to accomplish the intended, legitimate purpose. Access beyond what is operationally required is prohibited.
Business Associate Agreement (BAA)	A written contract between Queen City Medical Transport and a business associate that establishes the

Term	Definition
	permitted and required uses and disclosures of PHI and the safeguards the business associate must implement.
Privacy Officer / Security Officer	The designated individual at Queen City Medical Transport responsible for developing, implementing, and enforcing this Policy and all related privacy and security practices.

3. Legal and Regulatory Framework

Queen City Medical Transport operates within a comprehensive legal and regulatory environment governing the privacy and security of health information and personal data. The Company is committed to full compliance with all applicable laws. The following laws and regulations form the foundation of this Policy:

Law / Regulation	Key Requirements Applicable to the Company
HIPAA Privacy Rule (45 CFR Part 164, Subpart E)	Establishes national standards for the protection of PHI. Governs permissible uses and disclosures, patient rights, and notice of privacy practices.
HIPAA Security Rule (45 CFR Part 164, Subpart C)	Requires covered entities and business associates to implement administrative, physical, and technical safeguards to protect ePHI from unauthorized access, alteration, or destruction.
HITECH Act (Pub. L. 111-5, Title XIII)	Strengthens HIPAA enforcement; expands business associate liability; establishes breach notification requirements for individuals, HHS, and the media; increases civil and criminal penalties.
Ohio Privacy and Data	Ohio's data breach notification statute

Law / Regulation	Key Requirements Applicable to the Company
Protection Laws	(Ohio Rev. Code § 1347.12) requires notification to affected Ohio residents in the event of a breach. The Ohio Data Protection Act provides a safe harbor for organizations implementing recognized cybersecurity frameworks.
CMS / Medicare & Medicaid Regulations	Centers for Medicare & Medicaid Services (CMS) regulations applicable to non-emergency medical transportation (NEMT) providers, including requirements related to beneficiary data and billing integrity.
Federal Transportation Regulations	Applicable federal requirements governing transportation providers that handle protected patient populations, including recordkeeping and data integrity obligations.

■ Penalties for Non-Compliance

Violations of HIPAA and HITECH may result in significant civil monetary penalties ranging from **\$137 to \$2,067,813 per violation category per year**, depending on culpability. Willful violations that are not corrected may result in criminal prosecution, fines, and imprisonment. State law violations may carry additional penalties. Queen City Medical Transport expects all personnel to take these obligations seriously.

4. Protected Health Information (PHI) - Privacy Protections

PHI is among the most sensitive categories of information the Company handles. All personnel who access, use, or disclose PHI — in any format — must adhere to the following standards without exception.

4.1 Use and Disclosure of PHI

PHI may only be used or disclosed under the following circumstances:

- **Treatment, Payment, or Healthcare Operations:** PHI may be used internally and shared with authorized providers or payers as necessary to arrange or document medical transportation services.
- **As Required by Law:** Disclosure is permitted where mandated by federal or state law (e.g., public health reporting, law enforcement requests with proper legal authority).
- **With Valid Patient Authorization:** A signed, HIPAA-compliant written authorization from the patient is required for all other disclosures not covered above.

Any use or disclosure of PHI that does not fall within the above categories is **strictly prohibited** without written patient consent. Incidental disclosures may occur in the normal course of operations but must be minimized through the safeguards described in this Policy.

4.2 Minimum Necessary Standard

All employees and contractors must adhere to the Minimum Necessary Standard when accessing or sharing PHI:

- Access to PHI is limited to what is necessary to perform assigned job duties.
- Personnel may not access PHI belonging to patients who are not assigned to their active work responsibilities.
- Curiosity, personal interest, or convenience is not a valid justification for accessing PHI.
- Access permissions will be reviewed periodically and adjusted to reflect current job roles.

- Requests for access beyond assigned permissions must be submitted to and approved by the Privacy Officer.

4.3 Verbal Communications

Spoken communication is a common source of inadvertent PHI disclosure. Staff must observe the following precautions:

- Do not discuss PHI in public areas, including waiting rooms, lobbies, hallways, or outside company facilities.
- Lower voices when discussing patient information in shared workspaces.
- Confirm the identity of the recipient before verbally sharing PHI over the telephone.
- Do not leave voicemail messages containing PHI on unverified numbers.
- Use private rooms or spaces when detailed clinical or personal information must be discussed.

4.4 Paper Records

Physical records containing PHI are subject to the following controls:

- All paper PHI records must be stored in **locked filing cabinets or secure rooms** when not in active use.
- Records must never be left unattended in unsecured or publicly accessible areas.
- Printed materials containing PHI must be retrieved promptly from shared printers or fax machines.
- When paper records are no longer needed and have met their required retention period, they must be **cross-cut shredded** — disposal in regular trash or recycling is prohibited.

- Trip logs, patient manifests, and intake forms must be treated as PHI at all times, including during transport in vehicles.

4.5 Patient Rights

Patients have the following rights under HIPAA with respect to their PHI. Queen City Medical Transport is committed to honoring these rights fully and promptly:

- **Right to Access:** Patients may request access to and copies of their PHI held by the Company.
- **Right to Amend:** Patients may request corrections or amendments to inaccurate or incomplete PHI.
- **Right to an Accounting of Disclosures:** Patients may request a list of disclosures of their PHI made in the prior six years.
- **Right to Request Restrictions:** Patients may request restrictions on certain uses or disclosures of their PHI, which the Company will evaluate and accommodate where feasible.
- **Right to Confidential Communications:** Patients may request that communications occur through alternative means or at alternative locations.

The Company will respond to all patient rights requests **within 30 days** of receipt, as required by HIPAA. All requests should be directed to the Privacy Officer. Requests and responses must be documented and retained.

5. Electronic Data Security (ePHI Safeguards)

The HIPAA Security Rule requires Queen City Medical Transport to implement administrative, physical, and technical safeguards to protect

ePHI. The requirements in this section apply to all electronic systems used to create, receive, maintain, or transmit ePHI.

5.1 Administrative Safeguards

Administrative safeguards are the policies, procedures, and management processes that govern the conduct of the workforce with respect to ePHI protection:

- **Security Officer Designation:** A designated Privacy and Security Officer is responsible for developing, implementing, maintaining, and enforcing all security policies and procedures.
- **Risk Analysis and Management:** The Company will conduct a thorough, documented risk analysis at least annually to identify potential vulnerabilities to ePHI. Risk management measures will be implemented to reduce identified risks to a reasonable and appropriate level.
- **Workforce Training:** All employees with access to ePHI must complete HIPAA security training at hire and annually thereafter (see Section 11).
- **Access Management:** Workforce access to ePHI will be granted based on job role and the minimum necessary standard. Access must be formally approved and documented.
- **Sanction Policy:** Workforce members who violate security policies are subject to disciplinary action as outlined in Section 12.
- **Contingency Planning:** The Company maintains a documented contingency plan covering data backup procedures, disaster recovery, and emergency access to ePHI to ensure business continuity.

5.2 Physical Safeguards

Physical safeguards restrict physical access to electronic information systems and the facilities in which they are housed:

- **Facility Access Controls:** Physical access to server rooms, workstations, and filing areas containing ePHI is restricted to authorized personnel only. Access logs will be maintained.
- **Workstation Controls:** Workstations must be positioned to minimize unauthorized viewing of ePHI. Screens must be locked when unattended (maximum 5-minute idle timeout).
- **Device and Media Controls:** All physical media (hard drives, USB drives, CDs, printed reports) containing ePHI must be inventoried and securely handled. Devices being decommissioned must be sanitized in accordance with NIST 800-88 standards.
- **Vehicle Security:** Electronic devices must **never** be left unattended in company or personal vehicles used for work purposes, even if the vehicle is locked.
- **Portable Device Encryption:** All portable devices (laptops, tablets, external drives) that store or access ePHI must be **encrypted using AES-256 or equivalent** and password-protected.

5.3 Technical Safeguards

Technical safeguards are the technology controls used to protect ePHI and control access to it:

- **Unique User Identification:** Every workforce member must be assigned a unique user ID. Shared or generic login credentials are prohibited.
- **Automatic Logoff:** Systems containing ePHI must be configured to automatically log off after no more than 5 minutes of inactivity.

- **Encryption in Transit and at Rest:** All ePHI must be encrypted during transmission using TLS 1.2 or higher. ePHI stored on servers, databases, or portable devices must be encrypted at rest.
- **Audit Controls:** Systems must generate and retain audit logs that record who accessed ePHI, when, and what actions were taken. Logs must be reviewed periodically by the Security Officer.
- **Integrity Controls:** Measures must be in place to ensure that ePHI is not improperly altered or destroyed. File integrity monitoring should be employed where technically feasible.
- **Access Controls:** Role-based access controls (RBAC) must be implemented to ensure workforce members access only the ePHI necessary for their job functions.

5.4 Password and Access Management

Effective access management is a critical line of defense against unauthorized ePHI access:

- Passwords must be a **minimum of 12 characters** and include a combination of uppercase letters, lowercase letters, numbers, and special characters.
- Passwords must be changed at least every **90 days**. Reuse of the last 10 passwords is prohibited.
- Shared credentials, group passwords, and written-down passwords are strictly prohibited.
- **Multi-Factor Authentication (MFA)** is required for all remote access to Company systems and for any system containing ePHI accessible outside the Company's physical premises.
- Terminated employees' and contractors' credentials must be disabled **immediately** upon separation.

- Privileged accounts (administrators, system accounts) must be subject to enhanced monitoring and reviewed quarterly.

5.5 Network Security

The Company's network is a critical asset. The following controls must be maintained:

- Unsecured public or shared Wi-Fi networks (e.g., coffee shops, hotels) may **never** be used to transmit ePHI or access Company systems.
- All remote access to Company systems must occur over a **Company-approved Virtual Private Network (VPN)** using strong encryption.
- Firewalls must be maintained on all network perimeters and updated regularly. Firewall configurations must be reviewed at least annually.
- Antivirus and anti-malware software must be installed, active, and configured to receive automatic updates on all Company devices.
- Network traffic must be monitored for anomalous activity. Intrusion detection or prevention systems should be employed where feasible.
- Software and operating system patches must be applied in a timely manner. Critical security patches must be applied within **30 days** of release.

5.6 Mobile Device Policy

Mobile devices present unique security risks. The following requirements apply to all mobile devices used in connection with Company data or systems:

- All mobile devices (smartphones, tablets) used to access ePHI or Company systems must be enrolled in the Company's **Mobile Device Management (MDM)** system prior to use.
- Devices must be password-protected and configured to lock after no more than 5 minutes of inactivity.

- All devices must have device-level encryption enabled.
 - The Company reserves the right to remotely wipe a Company-managed device in the event of loss, theft, suspected compromise, or employee separation.
 - Lost or stolen devices must be reported to the Security Officer **immediately upon discovery** — no exceptions.
 - Installation of unauthorized applications on Company-managed devices is prohibited.
 - Personal devices used for Company business (BYOD) must meet the same MDM enrollment, encryption, and password requirements as Company-owned devices.
-

6. Personally Identifiable Information (PII) - Data Protection

In addition to PHI, Queen City Medical Transport collects, stores, and processes PII belonging to employees, clients, vendors, and drivers. This section establishes the Company's obligations for protecting PII.

What Constitutes PII

PII includes, but is not limited to, the following categories of information:

- Full legal name
- Home address or personal mailing address
- Date of birth
- Social Security Number (SSN) or Tax Identification Number (TIN)
- Driver's license or state ID number

- Financial account numbers, credit card numbers, or banking information
- Personal telephone numbers or personal email addresses
- Biometric data (fingerprints, facial recognition data)
- Passport or immigration document numbers
- Any combination of data that, when combined, could identify an individual

PII Data Minimization

- PII collected must be **adequate, relevant, and limited** to what is necessary for the specific, identified purpose for which it is collected.
- PII must not be collected, retained, or used for purposes beyond those for which it was originally obtained without additional authorization.

PII Security Requirements

- PII must be stored securely using the same safeguards described for PHI in Section 5, including encryption, access controls, and physical security.
- Access to PII must be limited to personnel with a legitimate need and must adhere to the Minimum Necessary Standard.
- PII must not be transmitted via unsecured channels (e.g., unencrypted email, text message) without explicit authorization and appropriate safeguards.

Employee and Vendor PII

- **Employee PII** collected for human resources, payroll, or benefits purposes is subject to the same security controls as any other PII under this Policy.

- **Driver PII** — including driving records, license information, and background check results — must be stored securely and accessed only by authorized HR or management personnel.
 - **Vendor and Business Partner PII** — including contact information, banking details, and tax identification numbers — is covered by this Policy and must be protected from unauthorized access or disclosure.
-

7. Business Associate Obligations

Queen City Medical Transport regularly works with third-party vendors, technology providers, billing companies, and other partners who may have access to PHI or PII. These relationships carry significant compliance obligations for both parties.

Business Associate Agreement (BAA) Requirement

- A signed, HIPAA-compliant **Business Associate Agreement (BAA)** must be executed with every vendor, contractor, or partner that will access, use, create, receive, maintain, or transmit PHI on behalf of the Company.
- No PHI may be shared with any third party until a fully executed BAA is in place.
- The Privacy Officer maintains a registry of all current BAAs, including effective dates, renewal dates, and covered services.

Business Associate Safeguard Requirements

- Business associates are required to implement administrative, physical, and technical safeguards that are equal to or exceed the standards set forth in this Policy and in the HIPAA Security Rule.

- Business associates may not subcontract work involving PHI to a subcontractor without first obtaining a written subcontractor BAA and notifying Queen City Medical Transport.

Audit Rights

- Queen City Medical Transport reserves the right to audit any business associate for compliance with the terms of their BAA and applicable law.
- Business associates must cooperate fully with any audit request and provide documentation within a reasonable timeframe as specified by the Company.

Breach Notification by Business Associates

- Business associates must notify Queen City Medical Transport of any known or suspected breach of PHI or PII **within 24 hours** of discovery.
- Notification must include, to the extent known: the nature of the incident, the PHI or PII involved, the individuals affected, and remediation steps taken or planned.

■ Consequences of Non-Compliance

Failure by a business associate to comply with the terms of their BAA, this Policy, or applicable law may result in **immediate termination of the business relationship**, referral to the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR), and pursuit of legal remedies including recovery of damages and attorney's fees.

8. Intellectual Property and Proprietary Data Protection

Queen City Medical Transport's competitive position, operational efficiency, and client relationships depend on the protection of its proprietary business information. All workforce members are obligated to safeguard Company intellectual property and confidential business data.

What Constitutes Proprietary Information

The following categories of information are considered proprietary and confidential to Queen City Medical Transport:

- Routing software, algorithms, and dispatch technologies
- Scheduling systems and operational platforms
- Patient manifests, trip data, and service records (distinct from patient-specific PHI obligations)
- Operational procedures, protocols, and training materials
- Pricing structures, rate schedules, and contract terms
- Client and payer contracts and relationships
- Financial data, cost structures, and business strategies
- Personnel information and internal communications
- Any other non-public business information developed or used by the Company

Employee Obligations

- Employees and contractors may not copy, reproduce, share, sell, publish, or otherwise disclose proprietary information without explicit **written authorization** from senior leadership.
- Proprietary information may only be used for legitimate Company business purposes.

- Upon separation from employment or termination of a contract — for any reason — all proprietary materials, in all formats, must be **returned to the Company or permanently deleted** within 3 business days.
- Employees acknowledge that proprietary information remains the exclusive property of Queen City Medical Transport at all times, including after separation.

Non-Disclosure Agreements

Non-Disclosure Agreements (NDAs) may be required as a condition of employment, contract engagement, or access to sensitive systems for:

- Employees with access to financial, strategic, or client information
- Independent contractors and technology vendors
- Any other individual granted access to proprietary systems or confidential business data

Consequences of Unauthorized Disclosure

Unauthorized use or disclosure of proprietary information may result in:

- Immediate disciplinary action, up to and including termination
- Civil legal proceedings, including injunctive relief and monetary damages
- Criminal prosecution where applicable under state or federal law
- Referral to law enforcement agencies

9. Data Retention and Disposal

Queen City Medical Transport maintains records for the duration required by law and disposes of them securely upon expiration of their required

retention period. Premature destruction or improper disposal of records is a policy violation.

Retention Schedule

Record Type	Minimum Retention Period	Notes
Medical transport records, trip logs, and patient data	7 years from date of service	Longer retention may be required by state Medicaid, payer contracts, or applicable law. The greater period controls.
HIPAA-related policies, procedures, and documentation	6 years from creation or last effective date	Required by the HIPAA Privacy Rule.
Security incident and breach records	6 years	Must include documentation of the incident, assessment, response, and outcome.
Employee personnel records	3 years post-separation	Longer retention may apply for EEOC, FMLA, or workers' compensation records.
Business Associate Agreements (BAAs)	6 years from execution or last effective date	Required by HIPAA.
Employee training records	6 years	Must document dates, content, and acknowledgment of completion.
Financial and billing records	7 years	Subject to IRS and CMS requirements.

A comprehensive Records Retention Schedule is maintained by the Privacy Officer and reviewed annually.

Secure Disposal Requirements

- **Electronic Records:** Must be securely deleted using NIST SP 800-88 compliant methods, including cryptographic erasure, degaussing, or

physical destruction of storage media. Standard delete functions are not sufficient.

- **Paper Records:** Must be cross-cut shredded using a DIN 66399 P-4 standard shredder or higher, or incinerated by an approved document destruction service. No PHI or PII may be disposed of in regular waste or recycling containers.
- **Hard Drives and Portable Media:** Must be physically destroyed or degaussed before disposal, recycling, or donation. A certificate of destruction from a qualified vendor is recommended.
- Records of all disposal activities must be maintained by the Privacy Officer.

10. Incident Response and Breach Notification

A prompt, organized, and well-documented response to security incidents is critical to minimizing harm and meeting legal obligations. All workforce members play a role in the Company's incident response capability.

10.1 What Constitutes a Security Incident

A security incident includes any of the following events involving PHI, PII, or Company systems:

- Unauthorized access to, use of, or disclosure of PHI or PII
- Malware infection, ransomware, or virus attack on Company systems
- Loss or theft of a device containing PHI, PII, or Company data
- Phishing attack resulting in credential compromise or data access
- Accidental disclosure of PHI or PII to an unauthorized party

- Improper disposal of PHI or PII (paper or electronic)
- Unauthorized modification or deletion of records
- Any other event that threatens the confidentiality, integrity, or availability of PHI, PII, or critical Company systems

10.2 Reporting Obligations

- All employees, contractors, and business associates must **immediately report** any known or suspected security incident to the designated Privacy and Security Officer.
- Employees must not attempt to investigate or remediate an incident on their own prior to reporting.
- **Failure to report a known or suspected incident is itself a policy violation** and subject to disciplinary action, regardless of whether a breach actually occurred.
- Reports may be made verbally (with written follow-up) or in writing using the Company's Incident Report Form.

10.3 Incident Response Steps

Upon receiving a report of a suspected incident, the Privacy and Security Officer will initiate the following response process:

1. **Contain the Incident:** Isolate affected systems, revoke compromised credentials, or physically secure affected devices to prevent further unauthorized access or data loss.
2. **Assess Nature and Scope:** Determine what data was affected, who may have accessed it, how many individuals are impacted, and whether the incident constitutes a reportable breach under HIPAA/HITECH.

3. **Notify Appropriate Parties:** Based on the assessment, notify affected individuals, regulatory bodies, law enforcement (if applicable), and business associates in accordance with the timelines in Section 10.4.
4. **Document Everything:** Maintain a complete written record of the incident, all response actions taken, parties notified, and outcomes.
5. **Remediate:** Implement corrective measures to address the root cause and prevent recurrence. Update policies, procedures, and safeguards as appropriate.

10.4 Breach Notification Timeline (HIPAA / HITECH)

Where an incident is determined to constitute a reportable breach, the following notification deadlines apply:

Notification Recipient	Deadline	Applicable Trigger
Affected Individuals	Within 60 days of breach discovery	All reportable breaches of PHI
U.S. Dept. of Health & Human Services (HHS / OCR)	Within 60 days for breaches of 500+ records; Annually for smaller breaches (by March 1 of the following year)	All reportable breaches of PHI
Media Outlets (prominent state/regional media)	Within 60 days of breach discovery	Breaches affecting 500 or more residents of a single state or jurisdiction
Business Associates	Within 24 hours of internal discovery	Where the breach involves a business associate's systems or data
Ohio Residents (State Law)	In the most expedient time possible; no later than 45 days under Ohio Rev. Code § 1347.12	Breaches of PII affecting Ohio residents

Notification content must comply with HIPAA's minimum required elements, including the nature of the breach, types of information involved, steps individuals should take to protect themselves, and contact information for the Privacy Officer.

10.5 Documentation

- All security incidents — regardless of whether they rise to the level of a reportable breach — must be documented.
 - Documentation must include: date and time of discovery, nature of the incident, affected data and individuals, response actions taken, notification records, and remediation steps.
 - All incident and breach records must be retained for a minimum of **6 years** from the date of creation or the last effective date of the related document, whichever is later.
-

11. Employee Training and Awareness

An informed and security-conscious workforce is the Company's most important safeguard. Queen City Medical Transport is committed to providing ongoing training and awareness programs to ensure all personnel understand their obligations under this Policy and applicable law.

Training Requirements

- **Initial Training:** All new employees and contractors must complete HIPAA Privacy and Security training **at the time of hire**, prior to being granted access to PHI, ePHI, or Company systems.
- **Annual Refresher Training:** All workforce members must complete refresher training at least once per calendar year. Training must be completed within the assigned deadline.

- **Role-Specific Training:** Employees with elevated access to PHI, ePHI, or sensitive systems (e.g., dispatch operators, billing staff, IT personnel) must complete additional targeted training appropriate to their responsibilities.
- **Training on Policy Updates:** Employees may be required to complete supplemental training following material updates to this Policy or applicable law.

Training Content

Training programs will cover, at minimum:

- Overview of HIPAA, HITECH, and applicable state privacy laws
- Employee responsibilities under this Policy
- How to identify, handle, and protect PHI and PII
- Recognizing phishing, social engineering, and other security threats
- Password security and safe device usage
- Incident reporting procedures and breach notification obligations

Phishing Simulation and Awareness

- The Company will conduct periodic phishing simulation exercises to assess employee awareness and identify areas for improvement.
- Results will be used to tailor future training and awareness programs.
- Employees who repeatedly fall victim to phishing simulations may be required to complete additional mandatory training.

Training Records

- Training completion records — including dates, content covered, and employee acknowledgment — must be maintained for each workforce member.

- Records must be available for review by the Privacy Officer and produced upon request in connection with any regulatory audit or investigation.
 - Employees who fail to complete required training by the assigned deadline may have their system access **suspended** until training is successfully completed.
-

12. Enforcement and Disciplinary Action

Queen City Medical Transport takes violations of this Policy seriously. Consistent enforcement is essential to maintaining a culture of privacy and security, protecting patients and clients, and fulfilling the Company's legal obligations.

Scope of Disciplinary Action

- Violations of this Policy may result in disciplinary action consistent with Queen City Medical Transport's Employee Handbook, up to and including **immediate termination of employment or contract**.
- The severity of disciplinary action will consider the nature of the violation, whether it was intentional or negligent, the harm caused or potential for harm, and whether the employee has prior violations.
- Intentional violations, or violations that result in significant harm to patients, clients, or the Company, may be referred to **law enforcement or regulatory agencies**, including HHS Office for Civil Rights (OCR).

Examples of Policy Violations

The following behaviors constitute violations of this Policy, among others:

- Accessing PHI or PII without a legitimate business need

- Sharing login credentials with another person
- Disposing of PHI in unsecured trash or recycling
- Failing to report a known or suspected security incident
- Using personal or unsecured email to transmit PHI or ePHI
- Leaving a workstation unattended and unlocked
- Disclosing proprietary Company information to unauthorized parties
- Failing to complete mandatory training by the required deadline

Non-Retaliation

- Employees are **protected from retaliation** for reporting — in good faith — a suspected violation of this Policy, a potential breach, or any concern related to privacy and security compliance.
- Retaliation against a reporting employee is itself a serious policy violation and will be subject to disciplinary action.
- Reports may be made directly to the Privacy Officer or through any other reporting mechanism established by the Company.

Investigation Responsibility

- The Privacy and Security Officer is responsible for receiving reports of alleged violations, conducting or coordinating investigations, and documenting findings and outcomes.
 - All investigations will be conducted confidentially to the extent practicable.
 - The Privacy Officer may involve legal counsel, HR, or external forensic resources as appropriate.
-

13. Policy Review and Updates

This Policy is a living document that must evolve in response to regulatory changes, operational developments, and the findings of security incidents and audits.

Review Schedule

- This Policy will be reviewed and updated at least **once per calendar year**.
- An unscheduled review will be conducted in the event of:
 - Significant changes to HIPAA, HITECH, state privacy laws, or other applicable regulations
 - A material security incident or data breach
 - Significant changes to Company operations, technology, or workforce structure
 - Findings from a risk analysis or compliance audit

Approval and Communication

- All revisions to this Policy must be approved by **Senior Leadership** prior to taking effect.
- The Privacy Officer will maintain a version history documenting each revision, its effective date, and a summary of changes.
- Employees will be notified of all material changes to this Policy and may be required to review and re-acknowledge the updated Policy prior to continued system access.

Version History

Version	Effective Date	Description of Changes	Approved By
1.0	October 16, 2026	Initial Policy Release	Senior Leadership

Version	Effective Date	Description of Changes	Approved By
<i>[Future versions]</i>			

14. Contact Information and Privacy Officer

Queen City Medical Transport has designated a Privacy and Security Officer who is responsible for implementing and maintaining this Policy, responding to questions and concerns, and coordinating the Company's compliance activities.

All privacy concerns, access requests, breach reports, policy questions, or compliance concerns should be directed to the Privacy and Security Officer using the contact information below.

Privacy & Security Officer - Contact Information	
Name	<i>[Privacy Officer Name]</i>
Title	<i>Privacy and Security Officer, Queen City Medical Transport</i>
Phone	<i>[Phone Number]</i>
Email	<i>[Email Address]</i>
Mailing Address	Queen City Medical Transport <i>[Street Address]</i> Mount Healthy, Ohio 45231
Office Hours	<i>[Office Hours]</i>

For complaints related to HIPAA privacy rights that are not resolved internally, patients and employees may also contact:

- **HHS Office for Civil Rights (OCR):** www.hhs.gov/ocr | 1-800-368-1019

- **Ohio Attorney General's Office:** www.ohioattorneygeneral.gov

■ **Important**

Queen City Medical Transport will **never** retaliate against any individual for filing a complaint with the Privacy Officer or with HHS OCR regarding a potential privacy or security violation.

15. Acknowledgment

By signing below, I confirm that I have received, read, and understood the **Queen City Medical Transport Data Privacy and Security Policy (Version 1.0, Effective October 16, 2026)**. I agree to comply with all requirements set forth in this Policy and understand that failure to comply may result in disciplinary action, up to and including termination of employment or contract, and may expose me to personal legal liability.

I understand that this Policy may be updated from time to time and that I am responsible for remaining familiar with the current version of the Policy as communicated by the Company.

Printed Full Name

Signature

Title / Position

Date (MM/DD/YYYY)

Department / Work Location

Employee ID / Contractor ID (if applicable)

This signed acknowledgment form must be returned to the Privacy and Security Officer or Human Resources upon completion. A copy will be

retained in the employee's personnel file for the duration of the retention period specified in Section 9 of this Policy.