



COMPLIANCE STATEMENT

Privacy, Security and HIPAA Support Commitment

Privacy, Security and HIPAA Support Commitment

Prepared for: [Healthcare Provider / Clinic Name]

Prepared by: Medex Pro RCM Solutions

Effective Date: [Effective Date]

Version: 1.0

Document Type	Compliance Statement
Company	Medex Pro RCM Solutions
Services	Medical Billing, RCM, Credentialing, Coding Support, Claims and AR Follow-up
Contact	[Your Name] [Your Title]
Email	info@medexprousa.com
Phone	(512) 298-2956
Website	medexprousa.com

Medex Pro RCM Solutions Compliance Statement

1. Statement of Commitment

Medex Pro RCM Solutions is committed to maintaining privacy, security, confidentiality, and responsible handling of healthcare information received while performing medical billing, revenue cycle management, coding support, credentialing, claims follow-up, payment posting, reporting, and related administrative services.

When Medex Pro RCM Solutions creates, receives, maintains, or transmits Protected Health Information on behalf of a healthcare provider, Medex Pro RCM Solutions will use reasonable administrative, physical, and technical safeguards designed to support compliance with the Health Insurance Portability and Accountability Act, the HITECH Act, and applicable privacy and security requirements.

2. Scope of Compliance

This Compliance Statement applies to Medex Pro RCM Solutions workforce members, contractors, systems, workflows, and service activities that involve patient, billing, insurance, provider, or other confidential healthcare information.

- Medical billing and claim submission activities.
- Revenue cycle management and accounts receivable follow-up.
- Provider credentialing and enrollment support.
- Eligibility verification, denial management, and payer communication.
- Handling of patient demographics, insurance details, EOBs, ERAs, claim records, and related PHI.
- Use of provider-approved billing software, clearinghouses, payer portals, and secure document-sharing channels.

3. HIPAA and Business Associate Responsibilities

Medex Pro RCM Solutions understands that it may act as a Business Associate when providing services that involve PHI for a Covered Entity. Before PHI is shared, the parties should execute a Business Associate Agreement that defines permitted uses and disclosures, safeguards, breach reporting, subcontractor requirements, and return or destruction of PHI at termination.

- Use and disclose PHI only for authorized service purposes or as otherwise permitted by the applicable agreement and law.
- Limit PHI access to the minimum necessary information required for assigned work.
- Maintain confidentiality of PHI and other provider information.
- Assist the Covered Entity with compliance-related requests where required by the Business Associate Agreement.
- Require appropriate written obligations from subcontractors or vendors that may create, receive, maintain, or transmit PHI on behalf of Medex Pro RCM Solutions.

4. Privacy and Security Safeguards

Safeguard Area	Compliance Practice
Administrative Safeguards	Policies, workforce expectations, access approval, role assignment, incident response process, and periodic review of privacy and security practices.
Technical Safeguards	Unique user access where available, password protection, role-based permissions, secure transmission methods, audit trails where supported, and use of approved systems.
Physical Safeguards	Protection of devices, restricted access to work areas where PHI is handled, secure document storage, and secure disposal of printed or downloaded information.
Workforce Safeguards	Confidentiality expectations, privacy awareness, security training, supervision, and access removal for inactive workforce members.
Vendor Safeguards	Use of service providers and subcontractors only where appropriate confidentiality and security obligations are in place.

5. Access Control and Minimum Necessary Use

Medex Pro RCM Solutions will seek to ensure that access to PHI is limited to authorized workforce members who need the information to perform assigned billing, credentialing, claims, reporting, or administrative tasks.

- Access should be role-based and limited to assigned responsibilities.
- Shared accounts should be avoided where individual user accounts are available.
- User access should be removed or disabled when no longer required.
- Workforce members should not download, copy, print, or retain PHI unless necessary for approved work.
- PHI should not be used for personal purposes, unauthorized marketing, or unrelated business activity.

6. Data Handling and Confidentiality

Provider and patient information should be used only for authorized service delivery and should be stored, transmitted, and disposed of through approved methods.

- PHI should be transmitted through secure systems, approved portals, encrypted channels, or provider-approved methods.
- Sensitive documents should not be sent through unsecured channels unless specifically authorized by the provider and permitted by applicable policy.
- Printed PHI should be minimized and securely destroyed when no longer needed.
- Billing records, claim details, payer notes, EOBs, ERAs, and credentialing documents should be treated as confidential information.
- Data retention and return or destruction of PHI should follow the executed agreement and provider instructions.

7. Incident Response and Breach Reporting

Medex Pro RCM Solutions will maintain a process for identifying, escalating, investigating, and responding to suspected privacy or security incidents involving PHI or confidential provider information.

- Suspected unauthorized access, use, disclosure, loss, theft, or compromise of PHI should be escalated promptly.
- Medex Pro RCM Solutions will cooperate with the healthcare provider in reviewing incidents and gathering available facts.
- Where a breach or reportable incident is identified, notice will be provided according to the applicable Business Associate Agreement and legal requirements.
- Corrective actions may include access changes, workforce retraining, additional safeguards, vendor review, or workflow updates.

8. Workforce Training and Confidentiality

- Workforce members should receive privacy and security awareness appropriate to their duties.
- Workforce members should understand confidentiality obligations and acceptable use of systems.
- Unauthorized sharing, copying, storage, or disclosure of PHI is prohibited.
- Access credentials should not be shared and should be protected from unauthorized use.

9. Provider Responsibilities

Effective compliance depends on cooperation between Medex Pro RCM Solutions and the healthcare provider. The provider remains responsible for clinical documentation, patient authorization decisions, payer enrollment approvals, medical necessity decisions, and final compliance oversight for its own practice operations.

- Provide accurate and complete patient, insurance, encounter, and documentation information.
- Provide secure system access and promptly remove access when services end.
- Notify Medex Pro RCM Solutions of special privacy restrictions, patient requests, payer requirements, or legal limitations that affect billing work.
- Execute a Business Associate Agreement before sharing PHI.
- Review reports, claim issues, coding questions, and payer correspondence in a timely manner.

10. Compliance Controls Summary

Control	Statement
Confidentiality	PHI and provider information are treated as confidential and used only for authorized services.
Access Management	Access is limited to authorized users based on business need.
Secure Communication	PHI is shared through secure or provider-approved methods.
Subcontractor Oversight	Subcontractors handling PHI are expected to follow written privacy and security obligations.
Incident Reporting	Suspected incidents are escalated, investigated, and reported according to the applicable agreement.
Return or Destruction	PHI is returned, destroyed, or protected after service termination as required by the agreement.
Continuous Improvement	Workflows and safeguards may be updated based on provider requirements, regulatory changes, system changes, or operational risk.

11. Contact for Compliance Matters

Company	Medex Pro RCM Solutions
Compliance Contact	[Compliance Officer / Authorized Representative]
Email	info@medexprousa.com
Phone	(512) 298-2956

Address	[Company Address]
---------	-------------------

Acknowledgment

The undersigned acknowledges receipt of this Compliance Statement and understands that final obligations shall be governed by the executed services agreement, Business Associate Agreement, and applicable law.

Healthcare Provider / Covered Entity	Medex Pro RCM Solutions
Name: _____	Name: _____
Title: _____	Title: _____
Signature: _____	Signature: _____
Date: _____	Date: _____

Disclaimer: This statement describes operational expectations and is not legal advice or a guarantee of regulatory compliance.