STRATEGIQUE PARTNERS

Behavioral Health M&A Intelligence Series

COMPLIANCE & TRANSACTION READINESS RESOURCE · BEHAVIORAL HEALTH EHR

Behavioral Health EHR

Compliance Checklist

HIPAA, 42 CFR Part 2, Cybersecurity, and M&A Readiness for Behavioral Health Organizations

42 CFR	10+	100+	2026
Part 2 Compliance	**Safeguard Categories**	**Checklist Controls**	**Edition**
SUD record confidentiality	*Administrative, technical, physical*	*Diligence-ready documentation*	*Updated for current M&A market*

Published: June 2026 · Last Updated: June 2026 · Data Current Through: Q1 2026

Prepared by Strategique Partners Research · Reviewed by the Strategique Partners M&A Advisory Team

WHAT THIS RESOURCE COVERS

Behavioral health organizations manage some of the most sensitive healthcare information in existence, psychotherapy notes, psychiatric evaluations, crisis intervention records, trauma histories, and medication-assisted treatment documentation chief among them. This guide consolidates the 2026 compliance landscape into a single working resource: a practical, checklist-driven framework covering HIPAA administrative, technical, and physical safeguards; 42 CFR Part 2 requirements for substance use disorder records; cybersecurity and incident-response preparedness; and the specific ways compliance posture now shapes valuation and buyer interest in behavioral health M&A.

TABLE OF CONTENTS

1. Why EHR Compliance Matters in Behavioral Health

2. Why EHR Compliance Matters in Behavioral Health M&A

3. Behavioral Health M&A Readiness Considerations

4. Administrative Safeguards

5. 42 CFR Part 2 Compliance Checklist for SUD Providers

6. Technical Safeguards

7. Incident Response & Breach Preparedness

8. How EHR Compliance Affects Valuation and Buyer Interest

9. Strengthening Compliance Readiness

10. Potential Consequences of Non-Compliance

11. Compliance Readiness & M&A Preparation

12. How Strategique Partners Serves Behavioral Health Organizations

SECTION 1 Why EHR Compliance Matters in Behavioral Health

Behavioral health organizations manage some of the most sensitive healthcare information in existence. Unlike many medical specialties, mental health and substance use disorder (SUD) treatment providers routinely maintain psychotherapy notes, psychiatric evaluations, crisis intervention records, trauma histories, addiction treatment documentation, medication-assisted treatment (MAT/MOUD) records, and other highly sensitive patient information.

As regulatory expectations continue to evolve, compliance extends beyond HIPAA privacy rules. Behavioral health organizations must also address cybersecurity preparedness, interoperability standards, vendor management, disaster recovery planning, and, where applicable, compliance with 42 CFR Part 2 requirements governing substance use disorder records.

A Single Compliance Failure Can Result In:

- Regulatory fines and penalties
- Civil litigation
- Loss of patient trust
- Increased cyber insurance costs
- Accreditation concerns
- Reputational damage
- Business interruption
- Potential licensure complications

Compliance Is Now a Business Process, Not Just a Legal Obligation

EHR compliance is no longer solely a legal or regulatory issue. It has become an important operational and transaction-readiness consideration for behavioral health organizations pursuing growth, investment, partnership opportunities, or future sale transactions.

SECTION 2 Why EHR Compliance Matters in Behavioral Health M&A

During mergers & acquisitions and financial due diligence reviews, buyers increasingly evaluate technology infrastructure, cybersecurity controls, data governance policies, and compliance practices before determining valuation and transaction structure.

Weak cybersecurity controls, incomplete documentation, missing audit logs, poor vendor oversight, inadequate backup procedures, or deficiencies in 42 CFR Part 2 compliance may create transaction risk. These issues can lead to prolonged diligence timelines, increased legal review, escrow holdbacks, indemnification requirements, or purchase price adjustments.

Organizations that maintain strong behavioral health EHR governance, documented security controls, encryption standards, consent management procedures, and mature compliance programs are often viewed as lower-risk acquisition targets. Effective EHR compliance supports operational readiness, facilitates post-acquisition integration, and helps organizations demonstrate transaction preparedness during buyer diligence.

SECTION 3 Behavioral Health M&A Readiness Considerations

Behavioral health buyers and investors routinely evaluate EHR systems during diligence. Common areas of review include:

- HIPAA compliance standards
- Cybersecurity controls and incident history
- Business Associate Agreements (BAAs)
- Access control procedures
- Audit log retention practices
- Data backup and disaster recovery capabilities
- CMS behavioral health billing standards
- Interoperability readiness
- Revenue cycle management
- Vendor management practices
- 42 CFR Part 2 compliance procedures
- CMS behavioral health documentation
- Data migration readiness

> *Organizations with documented controls and mature compliance programs often experience smoother diligence processes, stronger buyer confidence, and fewer post-closing compliance concerns. Some behavioral health businesses may choose to outsource behavioral health licensing and compliance to meet the required standards.*

SECTION 4 Administrative Safeguards

The foundation of any behavioral health compliance program. These controls establish governance, accountability, and the documentation trail that buyers and regulators alike will expect to see.

Risk Management

- ☐ Conduct a comprehensive HIPAA Security Risk Assessment annually
- ☐ Maintain documented risk mitigation plans
- ☐ Review security controls after significant system changes
- ☐ Maintain written HIPAA policies and procedures
- ☐ Assign a designated Security Officer and Privacy Officer
- ☐ Document remediation activities resulting from risk assessments
- ☐ Maintain evidence of compliance reviews and corrective actions

Organizations preparing for investment or acquisition should maintain documentation demonstrating ongoing compliance monitoring and risk mitigation efforts. Buyers frequently request this information during diligence reviews.

Workforce Training

- ☐ Conduct annual HIPAA training for all staff
- ☐ Provide phishing and cybersecurity awareness training
- ☐ Train employees on secure EHR access procedures
- ☐ Document all compliance training activities
- ☐ Establish disciplinary procedures for HIPAA violations
- ☐ Train workforce members on data-sharing protocols
- ☐ Conduct periodic security awareness refreshers

Compliance training records are commonly reviewed during diligence to assess organizational maturity and operational readiness.

Vendor Management

- ☐ Maintain current Business Associate Agreements (BAAs)
- ☐ Evaluate vendor cybersecurity practices annually
- ☐ Review cloud hosting and backup providers for HIPAA compliance
- ☐ Verify that all third-party vendors handling ePHI maintain appropriate safeguards
- ☐ Review vendor incident response obligations
- ☐ Document vendor security assessments
- ☐ Establish procedures for periodic vendor compliance reviews

Third-party vendor relationships frequently become a focus area during operational and technology diligence because vendor failures can create significant compliance, cybersecurity, and post-closing integration risks.

SECTION 5 42 CFR Part 2 Compliance Checklist for SUD Providers

Organizations providing substance use disorder treatment should evaluate whether their EHR systems support compliance with federal confidentiality requirements governing SUD records.

Consent Management

- ☐ Does the EHR support Part 2 consent tracking?
- ☐ Are patient consent records retained and auditable?
- ☐ Are consent workflows documented and consistently followed?
- ☐ Are Treatment, Payment, and Healthcare Operations (TPO) consent procedures updated where applicable?
- ☐ Can consent status be verified before disclosure occurs?

Redisclosure Controls

- ☐ Are redisclosure restrictions documented?
- ☐ Are disclosure procedures reviewed regularly?
- ☐ Are disclosure logs maintained?
- ☐ Are staff trained on redisclosure limitations?
- ☐ Are information-sharing requests evaluated against Part 2 requirements?

SUD Record Segmentation

- ☐ Are SUD records segmented when necessary?
- ☐ Are access permissions configured appropriately?
- ☐ Are sensitive records protected through role-based access controls?
- ☐ Are record-sharing procedures documented and reviewed periodically?

Vendor Oversight

- ☐ Are BAAs updated for vendors handling SUD records?
- ☐ Are vendor disclosure practices reviewed for Part 2 compliance?
- ☐ Are data-processing arrangements documented?
- ☐ Are vendor responsibilities clearly defined?

Buyer Diligence Readiness

- ☐ Are data-room exports reviewed before sharing with potential buyers?
- ☐ Are disclosure limitations documented?
- ☐ Are Part 2-related compliance procedures available for diligence review?
- ☐ Are Notice of Privacy Practices updated where required?
- ☐ Are disclosure workflows documented and auditable?

Part 2 Gaps Are a Direct Transaction-Risk Factor

Failure to properly manage SUD records can create compliance concerns that may increase transaction risk and complicate diligence efforts during acquisitions or investment transactions.

SECTION 6 Technical Safeguards

Technical controls are where most diligence time is spent, they are verifiable, auditable, and directly tied to breach risk. This section consolidates every technical safeguard category that buyers and regulators evaluate in 2026.

Access Controls

- ☐ Implement Multi-Factor Authentication (MFA)
- ☐ Assign unique user credentials to every employee
- ☐ Establish role-based access controls
- ☐ Disable inactive user accounts promptly
- ☐ Enforce password complexity requirements
- ☐ Configure automatic session timeouts
- ☐ Review user access privileges periodically
- ☐ Document access-control procedures

Strong access controls help buyers verify that patient information is appropriately protected and reduce perceived cybersecurity risk during diligence reviews.

Encryption

- ☐ Encrypt EHR databases
- ☐ Encrypt data at rest
- ☐ Encrypt data in transit
- ☐ Encrypt backup files
- ☐ Encrypt laptops, tablets, and mobile devices
- ☐ Verify encryption standards meet current industry best practices
- ☐ Maintain documentation of encryption controls

Encryption remains one of the most important safeguards for protecting behavioral health records. Robust encryption controls may reduce transaction risk by limiting exposure associated with historical breaches, data migration activities, and post-closing integration efforts.

Monitoring & Audit Logs

- ☐ Enable EHR audit logging
- ☐ Track all access to patient records
- ☐ Review audit logs monthly
- ☐ Monitor failed login attempts
- ☐ Monitor record exports and downloads
- ☐ Maintain audit records according to retention requirements
- ☐ Document audit review procedures
- ☐ Retain records of suspicious activity investigations
- ☐ Review privileged-user access regularly
- ☐ Establish escalation procedures for identified issues

Audit logs serve as a critical compliance and diligence resource. Buyers frequently review audit logging practices to assess cybersecurity maturity, compliance readiness, incident history, and the organization's ability to support post-acquisition investigations and regulatory reviews.

Cloud Storage & Data Hosting

Cloud Compliance

- ☐ Verify cloud providers execute Business Associate Agreements
- ☐ Confirm cloud environments are HIPAA-compliant
- ☐ Restrict cloud access through role-based permissions
- ☐ Enable detailed access logging
- ☐ Conduct regular vendor security reviews
- ☐ Document cloud security controls
- ☐ Review vendor security certifications where applicable
- ☐ Establish procedures for periodic cloud-security assessments

Vendor relationships, hosting arrangements, and cloud architecture are commonly reviewed during operational and technology diligence. Buyers often evaluate whether cloud infrastructure supports scalability, security, and future integration requirements.

Data Backups & Disaster Recovery

- ☐ Perform daily encrypted backups
- ☐ Store backups in geographically separate locations
- ☐ Test restoration procedures at least annually
- ☐ Maintain documented disaster recovery procedures
- ☐ Define Recovery Time Objectives (RTOs)
- ☐ Define Recovery Point Objectives (RPOs)
- ☐ Document backup validation procedures
- ☐ Review backup effectiveness periodically
- ☐ Maintain records of recovery testing exercises
- ☐ Establish business continuity procedures

Reliable backup and disaster recovery programs help reduce operational risk and demonstrate business continuity preparedness during diligence reviews.

Physical Security Controls

- ☐ Restrict access to server rooms
- ☐ Implement workstation security policies
- ☐ Secure laptops and mobile devices
- ☐ Use screen-locking procedures
- ☐ Maintain visitor logs where applicable
- ☐ Establish secure media destruction procedures
- ☐ Document hardware disposal processes
- ☐ Conduct periodic physical-security reviews
- ☐ Maintain inventory records for critical hardware

Physical safeguards remain an important component of broader cybersecurity and compliance programs and may be reviewed during operational diligence.

CMS Interoperability & Information Sharing

Interoperability Readiness

- ☐ Ensure EHR supports FHIR-based data exchange
- ☐ Enable secure patient access to records
- ☐ Support electronic provider-to-provider data sharing
- ☐ Establish secure API management procedures
- ☐ Review information-blocking requirements annually
- ☐ Document interoperability workflows
- ☐ Evaluate integration readiness with external systems
- ☐ Maintain records of interoperability testing

CMS continues expanding interoperability expectations through patient access initiatives, provider data-sharing requirements, electronic prior authorization programs, and information-blocking enforcement efforts. Organizations pursuing growth or acquisition opportunities should evaluate whether their EHR systems can support future integrations and data migration requirements.

Secure Record Sharing

- ☐ Use encrypted email solutions
- ☐ Use secure patient portals
- ☐ Implement secure file-transfer systems
- ☐ Restrict use of personal email accounts
- ☐ Prohibit unauthorized messaging applications
- ☐ Verify recipient identity before disclosure
- ☐ Document record-sharing procedures
- ☐ Review disclosure workflows regularly
- ☐ Monitor external data-sharing activity

Improper record-sharing procedures can create HIPAA and 42 CFR Part 2 compliance concerns that may affect diligence outcomes, transaction timelines, and post-closing integration planning.

Telehealth Security

- ☐ Use HIPAA-compliant telehealth platforms
- ☐ Encrypt telehealth sessions
- ☐ Document telehealth consent procedures
- ☐ Securely store telehealth documentation
- ☐ Verify patient identity during remote visits
- ☐ Ensure telehealth vendors maintain BAAs
- ☐ Conduct periodic telehealth security reviews
- ☐ Monitor telehealth vendor compliance practices

SECTION 7 Incident Response & Breach Preparedness

- ☐ Maintain a written Incident Response Plan
- ☐ Define breach notification procedures
- ☐ Conduct annual incident-response exercises
- ☐ Maintain ransomware response procedures
- ☐ Establish vendor breach-notification requirements
- ☐ Document all security incidents
- ☐ Maintain cyber incident documentation for buyer review
- ☐ Retain breach investigation records
- ☐ Document remediation activities
- ☐ Test disaster recovery procedures annually
- ☐ Maintain cyber insurance documentation
- ☐ Review incident-response procedures periodically

Recent regulatory developments have increased expectations surrounding incident-response planning, contingency preparation, cybersecurity governance, and breach preparedness.

Buyers increasingly evaluate cybersecurity preparedness, historical breach activity, and incident-response maturity as part of compliance, operational, and technology diligence reviews.

SECTION 8 How EHR Compliance Affects Valuation and Buyer Interest

Behavioral health buyers increasingly evaluate EHR compliance as an operational-readiness indicator. While compliance alone does not determine enterprise value, deficiencies can increase perceived risk and influence transaction structure, diligence requirements, and integration planning.

Potential Consequences of Compliance Weaknesses

- Extended diligence timelines
- Additional legal and compliance review
- Escrow holdbacks
- Purchase-price adjustments
- Post-closing indemnification requirements
- Delayed integration efforts
- Increased cybersecurity review costs
- Additional remediation requirements before closing

What Buyers Reward

Organizations with mature cybersecurity controls, documented HIPAA programs, strong vendor oversight, clean audit histories, effective backup procedures, and established Part 2 compliance practices are often viewed more favorably during transaction reviews. Buyers increasingly prioritize operational quality, compliance readiness, and risk management capabilities alongside financial performance when evaluating behavioral health acquisition opportunities.

SECTION 9 Strengthening Compliance Readiness

1. Conduct Comprehensive Security Risk Assessments

The most common compliance weakness identified during investigations remains the failure to perform thorough risk assessments. Organizations should evaluate:

- Cybersecurity risks
- Insider threats
- Cloud-storage vulnerabilities
- Vendor-related risks
- Telehealth security concerns
- Data-sharing workflows
- Incident-response readiness
- Part 2 compliance procedures

Risk assessments should be documented, reviewed regularly, and linked to formal remediation plans.

2. Invest in Secure EHR Infrastructure

Behavioral health organizations should prioritize:

- Secure behavioral health EHR systems
- Encrypted cloud storage
- MFA implementation
- Endpoint protection
- Continuous monitoring tools
- Secure telehealth infrastructure
- Modern interoperability capabilities
- Disaster recovery preparedness

Strong technology infrastructure supports compliance, operational efficiency, and transaction readiness.

3. Establish Strong Vendor Oversight

Every organization handling patient data should be evaluated regularly, including:

- Billing cycles
- Revenue-cycle vendors
- IT providers
- Cloud vendors
- Telehealth vendors
- Data-backup providers
- Managed service providers
- Data-integration vendors

Vendor-related deficiencies can create compliance exposure and transaction risk if not properly managed.

4. Implement a Minimum Necessary Access Model

Staff should only access the information necessary to perform their responsibilities. Organizations should periodically review access rights, user permissions, and role assignments to ensure compliance with HIPAA and broader security expectations.

5. Build a Culture of Compliance and Operational Readiness

Regulatory compliance should not be treated as an annual exercise. Behavioral health organizations should integrate privacy, security, cybersecurity, and data-governance practices into daily operations through continuous training, monitoring, leadership oversight, and accountability.

Organizations preparing for future investment or acquisition opportunities should view compliance as a core business process rather than solely a regulatory obligation.

SECTION 10 Potential Consequences of Non-Compliance

Regulatory Exposure

Non-compliance may result in:

- HIPAA investigations
- OCR enforcement actions
- CMS audits
- State regulatory reviews
- Accreditation
- Corrective Action Plans
- Civil monetary penalties

Operational Consequences

Organizations may also experience:

- Ransomware-related downtime
- Service interruptions
- Inability to access patient records
- Increased insurance premiums
- Contract losses
- Disrupted referral relationships
- Increased remediation costs

Reputation and Patient Trust Risks

For behavioral health organizations, trust is essential. Breaches involving psychiatric records, psychotherapy documentation, or substance use disorder treatment information can significantly impact patient confidence, referral relationships, payer relationships, and long-term organizational reputation.

SECTION 11 Compliance Readiness & M&A Preparation

Preparing for a future acquisition, investment transaction, accreditation review, regulatory audit, or growth initiative requires more than basic HIPAA compliance.

Behavioral health organizations should be prepared to demonstrate:

- Cybersecurity maturity
- HIPAA compliance readiness
- 42 CFR Part 2 compliance procedures
- Vendor oversight controls
- Disaster recovery preparedness
- Data-sharing governance
- EHR operational readiness
- Technology diligence preparedness
- Integration readiness
- Revenue-cycle infrastructure support

Compliance Readiness Is a Value Driver, Not a Checkbox

Strategique Partners assists behavioral health organizations with compliance readiness reviews, operational assessments, EHR and billing optimization initiatives, transaction preparedness planning, and behavioral health M&A advisory services.

Next Steps

- Schedule a Compliance Readiness Review
- Discuss Pre-Sale Diligence Preparation
- Evaluate EHR and Billing Cleanup Opportunities
- Schedule a Behavioral Health Consulting Consultation

Final Takeaway

For behavioral health organizations in 2026, EHR compliance extends far beyond simply storing patient records. Organizations must demonstrate secure storage, encrypted transmission, controlled access, vendor oversight, audit-log management, disaster recovery preparedness, interoperability readiness, cybersecurity maturity, and compliance with applicable HIPAA and 42 CFR Part 2 requirements.

More importantly, compliance should be viewed as an operational readiness and transaction readiness initiative. Strong EHR governance not only protects patient information but can also improve buyer confidence, support diligence efforts, reduce transaction risk, and strengthen long-term organizational value.

STRATEGIQUE PARTNERS

Specialized M&A Advisory for Behavioral Health Business Owners Across the United States

Strategique Partners is a specialized M&A advisory firm serving behavioral health business owners, operators, private equity sponsors, and healthcare investors across the United States. For behavioral health organizations specifically, we offer a full spectrum of compliance, operational, and transaction advisory services, from the moment you begin strengthening EHR governance through post-close integration.

Compliance & Transaction Services

→ **Compliance Readiness Reviews —** Independent assessment of HIPAA, 42 CFR Part 2, and cybersecurity controls against current buyer and regulatory expectations.

→ **Pre-Sale Diligence Preparation —** Data-room readiness, documentation gap analysis, and remediation planning ahead of a sale or capital raise.

→ **EHR & Billing Optimization —** Technology and revenue-cycle assessments that reduce diligence friction and strengthen operational readiness.

→ **M&A Advisory Services —** Full sell-side and buy-side representation for behavioral health organizations, informed by current compliance and valuation intelligence.

Take the Next Step

Whether you are strengthening compliance ahead of an audit, preparing for a future transaction, or evaluating your organization's readiness for growth, Strategique Partners is here to guide you.

- Schedule a Compliance Readiness Review: strategiquepartners.com/mergers-acquisitions/
- Discuss Pre-Sale Diligence Preparation: strategiquepartners.com/mergers-acquisitions/
- Evaluate EHR and Billing Cleanup Opportunities: strategiquepartners.com/billing/
- Schedule a Behavioral Health Consulting Consultation: strategiquepartners.com/appointment/

Phone: **(561) 206-2105** · Website: **strategiquepartners.com**

Prepared by Strategique Partners Research
Behavioral Health M&A Intelligence Series · 2026 Edition