GUIDE

Bronston Legal
TRUSTED TECHNOLOGY COUNSEL

MSP Compliance: A Strategic Guide

What You Must Do and What Could Happen If You Don't

Compliance expectations are tightening across healthcare, finance, and critical infrastructure, and regulators are applying more pressure on MSPs than ever before. MSPs face scrutiny for how they protect client data, document preventative measures, prove their use of best practices, and respond to incidents. Frameworks like HIPAA, FTC, CMMC, and STIR/SHAKEN carry real legal and financial consequences. MSPs that take compliance seriously are not only protecting themselves and their clients — they're also turning it into higher MRR and a genuine competitive advantage.

At Bronston Legal, we have spent more than 30 years guiding MSPs, IT providers, and telecom businesses through regulatory complexity. This guide outlines what matters most, and what is at stake if you ignore it.

Enforcement Is No Longer Optional

For years, many MSPs treated compliance as background noise. That era is over. The HIPAA Security Rule's most significant overhaul in two decades is pending, with OCR actively enforcing the current rule and signaling that policies without provable implementation define willful neglect. CMMC 2.0 Phase 2 — mandatory third-party assessments for defense contractors — takes effect this November 2026. The FTC's Health Breach Notification Rule enforcement is active. Twenty states now require written data processing agreements most MSP contracts lack.

Regulatory summary: *As of June 2026, an MSP serving clients across multiple industries in multiple states may simultaneously be subject to HIPAA, the FTC Safeguards Rule, the FTC Health Breach Notification Rule, CMMC (as an ESP), up to 20 state privacy laws, all 50 state breach notification laws, and FCC telecom regulations — each with independent enforcement mechanisms and penalty structures.*

States are also sharpening their tools. Louisiana requires AG notification after a breach affecting even one person. Clients increasingly pursue MSPs in breach litigation, and courts find undocumented decisions make MSPs more liable.

Key Regulations MSPs Must Address

Regulation	Who It Applies To	Status	Penalty Exposure
HIPAA Security Rule (45 CFR Part 164)	MSPs acting as Business Associates with access to PHI or ePHI	NPRM published Jan. 2025; final rule still pending as of mid-2026; OCR actively enforcing current rule. New requirements expected: mandatory encryption at rest/in transit, mandatory MFA, 72-hour incident reporting, annual pen testing.	Up to $1.9M per violation category per year (willful neglect: $73,011/day)
FTC Safeguards Rule (16 CFR Part 314 / GLBA)	MSPs serving non-bank financial institutions: auto dealers, mortgage brokers, tax preparers, financial advisors, insurance agencies, accounting firms	In full effect since June 2023. Requires written WISP with 9 elements, designated Qualified Individual, annual risk assessments, MFA, encryption, vendor oversight, and 30-day FTC breach notification.	Up to $51,744 per violation (inflation-adjusted); FTC consent decrees; individual and state enforcement
FTC Health Breach Notification Rule (16 CFR Part 318)	MSPs hosting or supporting health apps, wellness platforms, fitness devices, or any PHR-adjacent technology not covered by HIPAA	Substantially updated April 2024. Covers health apps and connected devices explicitly. "Breach" now includes unauthorized disclosures (e.g., sharing data with ad networks), not just hacking.	Up to $53,088 per violation; FTC civil enforcement. GoodRx: $1.5M. Easy Healthcare: $100K.
CMMC 2.0 (32 CFR Part 170 / DFARS 252.204-7021)	MSPs acting as External Service Providers (ESPs) for DoD contractors handling CUI or FCI	Phase 1 (self-assessments) effective Nov. 10, 2025. Phase 2 (mandatory C3PAO third-party assessments for Level 2 contracts) effective Nov. 10, 2026. Assessment backlog: ~97 authorized C3PAOs for 80,000+ organizations.	Loss of DoD contract eligibility; debarment; criminal prosecution (DOJ Civil Cyber-Fraud Initiative)
State Comprehensive Privacy Laws (CCPA/CPRA, VCDPA, CPA, etc.)	MSPs processing personal data of consumers in covered states — now 20 states active as of 2026	Indiana, Kentucky, and Rhode Island effective Jan. 1, 2026. Connecticut amendments July 1, 2026. Maryland's MODPA (strictest yet) effective Oct. 2026. All 20 laws require written DPAs with processors.	CA: up to $7,988/ intentional violation; NJ: up to $20,000/ subsequent violation; State AG enforcement; class actions

Key Regulations MSPs Must Address

Regulation	Who It Applies To	Status	Penalty Exposure
FCC STIR/SHAKEN & Robocall Mitigation (47 CFR Subpart HH)	MSPs providing UCaaS, VoIP, or telecom services; interconnected VoIP providers; intermediate and gateway providers	All small-provider extensions expired by 2023. RMD annual recertification due March 1, 2026. Third-party authentication mandate effective Sept. 2025. New Know-Your-Upstream-Provider (KYUP) rules proposed May 2026.	FCC fines up to $10,000/ violation for inaccurate RMD filings; $1,000/ violation for missed updates; traffic blocking; criminal liability
CALEA (47 U.S.C. § 1001 et seq.)	MSPs operating as telecom carriers or providing substantial replacement for telephone voice service	VoIP providers with direct number access must file CALEA System Security & Integrity plans with FCC before commencing service. Compliance attestations required for all numbering authorization renewals.	FCC penalties; suspension of numbering authorization; potential criminal liability
SOC 2 Type II (AICPA Trust Services Criteria)	MSPs whose enterprise clients require proof of security controls; increasingly a contractual prerequisite	Not a government mandate, but now a de facto market requirement. Enterprise buyers and cyber insurers require SOC 2 Type II reports. Overlaps substantially with FTC Safeguards Rule technical controls.	Loss of enterprise contracts; inability to renew cyber insurance at preferred rates
NIST SP 800-171 Rev. 2 (CUI Security Requirements)	MSPs handling Controlled Unclassified Information for federal agencies or contractors outside of DoD (also foundational to CMMC Level 2)	110 security controls across 14 domains. Self-assessment required under DFARS 252.204-7019. Score must be reported in SPRS system. Misrepresentation can trigger False Claims Act liability.	False Claims Act treble damages; debarment; DOJ Criminal Division enforcement
State Breach Notification Laws (all 50 states)	All MSPs — every state has a breach notification law; thresholds and timelines vary significantly	Louisiana requires AG notification for breaches affecting even a single Louisiana resident. Many states now have sub-30-day notification windows. Some states (e.g., NY SHIELD Act) impose independent security obligations.	State AG enforcement; civil penalties; private right of action in some states; reputational harm

Regulation-by-Regulation: What You Need to Know

1. HIPAA Security Rule (45 CFR Part 164)

The HIPAA Security Rule governs the protection of electronic protected health information (ePHI). MSPs that access, store, transmit, or maintain ePHI on behalf of covered entities (hospitals, clinics, health plans, clearinghouses) are Business Associates (BAs) and must comply with the Security Rule directly — not merely by contract. The most significant proposed update to the Rule in over two decades was published in January 2025, and while the final rule has not yet issued, OCR is enforcing current standards with increasing rigor.

- **What changed and what is pending:** The NPRM published January 6, 2025 (90 FR 800) proposes the most significant overhaul of the HIPAA Security Rule since 2003. As of mid-2026, OCR has not yet issued a final rule. A target of May 2026 passed without publication; no confirmed timeline exists. OCR is nonetheless enforcing current requirements aggressively, citing security risk analysis failures, inadequate access controls, and insufficient encryption as primary deficiencies.
- **What the proposed rule would require (prepare now):** (1) Mandatory encryption of ePHI at rest and in transit — the "addressable" designation eliminated; (2) MFA required for all systems accessing ePHI; (3) 72-hour incident reporting and 72-hour system restoration capability; (4) Annual penetration testing; (5) Network segmentation; (6) Comprehensive asset inventories with documented data flows; (7) Annual vendor compliance audits — a signed BAA alone will no longer be sufficient; written verification of a BA's implemented safeguards required annually; (8) Access revocation within one hour of employee termination.
- **MSP-specific exposure:** MSPs functioning as Business Associates (BAs) must sign Business Associate Agreements (BAAs) and comply with the Security Rule independently — not merely by contract. BAAs that are signed but not operationalized create enforcement exposure. OCR's standard: "Policies and procedures alone are not sufficient evidence of security measure implementation." Controls must be implemented, tested, and provable. Willful neglect violations: $73,011 per day, per violation category.
- **What MSPs should do now:** Conduct a formal risk analysis and document remediation actions. Implement MFA and encryption at rest across all systems handling ePHI. Build a 72-hour incident response and restoration capability. Update all BAAs and begin annual BA verification workflows. Engage HIPAA-qualified legal counsel to assess current posture before the final rule issues.

2. FTC Safeguards Rule (16 CFR Part 314 / GLBA)

The Gramm-Leach-Bliley Act's Safeguards Rule, as substantially updated in 2021 and in full effect since June 2023, requires non-bank financial institutions to implement comprehensive information security programs. This rule captures a far larger universe of MSP clients than most providers realize, and because the MSP has administrative access to those clients' systems, MSP security practices are squarely within scope.

- **Who is covered — broader than most MSPs realize:** The Safeguards Rule covers "financial institutions" as defined under GLBA, which includes any entity "significantly engaged" in financial activities. This encompasses auto dealers, mortgage brokers, tax preparers, accounting firms, insurance agencies, financial advisors, and many other SMB clients MSPs routinely serve. If your client handles nonpublic personal financial information (NPI), the Safeguards Rule almost certainly applies — and because your MSP has access to those systems, your practices are in scope.
- **The nine required WISP elements:** (1) Designate a Qualified Individual (QI) responsible for the information security program; (2) Conduct and document a written risk assessment; (3) Design and implement safeguards based on risk assessment findings; (4) Regularly monitor and test safeguards; (5) Train all relevant staff; (6) Oversee service providers by contract and monitoring; (7) Keep the program current as business changes; (8) Create a written incident response plan; (9) Report in writing to the board or governing body at least annually.
- **Technical controls required:** MFA on all systems storing customer information (the in-office exception was eliminated by the August 2024 IRS Pub 5708 update for tax preparers; the Safeguards Rule has always required MFA). AES-256 encryption at rest; TLS 1.2+ for data in transit. Automatic session timeouts. Role-based access with least privilege. Immediate access revocation on termination. Endpoint detection and response (EDR). Annual penetration testing or continuous monitoring as an alternative.
- **Breach notification:** The December 2023 amendment to the Safeguards Rule added a 30-day FTC breach notification requirement. Covered institutions must notify the FTC within 30 days of discovering a breach affecting 500 or more customers. Civil penalties: up to $51,744 per violation (inflation-adjusted annually). The FTC does not need to prove harm — the violation of the rule itself is the basis for enforcement.
- **MSP liability:** If your MSP provides IT services to a covered financial institution, your service agreement should address: (1) your obligations as a service provider under the Rule; (2) security requirements your MSP must meet; (3) your notification obligations if you discover a breach; and (4) your cooperation with the client's audit rights over your security practices. Failing to include these terms exposes both you and your client.

3. FTC Health Breach Notification Rule (16 CFR Part 318)

The Health Breach Notification Rule fills the gap between HIPAA and the explosion of consumer-facing health technology. If your MSP supports health apps, wellness platforms, fitness trackers, or any technology that collects personal health data outside the traditional healthcare system, this Rule may apply.

- **Who is covered:** The Health Breach Notification Rule (16 CFR Part 318) applies to vendors of personal health records (PHRs), PHR-related entities, and their third-party service providers — provided they are not already covered by HIPAA. The April 2024 amendments explicitly confirmed coverage of health apps, fitness trackers, wellness devices, and connected health technologies that fall outside HIPAA's scope. If your MSP hosts or supports any of these platforms, you may be a "third party service provider" under the Rule.
- **What constitutes a "breach":** The definition is broader than most expect. A breach is the unauthorized acquisition of unsecured PHR identifiable health information — and it explicitly includes unauthorized disclosures, not just hacking. Sharing user health data with advertising networks, analytics platforms, or any third party without valid user authorization triggers notification obligations, even if no external attack occurred. The FTC's action against GoodRx (sharing health data with Facebook and Google for advertising without user consent: $1.5M penalty) is the clearest illustration.
- **Notification requirements:** Covered entities must notify each affected individual without unreasonable delay and no later than 60 calendar days after discovery. For breaches affecting 500 or more individuals, concurrent notification to the FTC is required. For smaller breaches, an annual log may be submitted. Email notice must be supplemented by at least one additional electronic channel. If 10 or more affected individuals cannot be reached, substitute notice via a 90-day website posting or media notice is required.
- **Service provider path:** MSPs acting as third-party service providers do not notify individuals or the FTC directly. They must notify the PHR vendor or related entity they serve, identify which customers were affected, and obtain acknowledgment. The notification must be provided without unreasonable delay. Importantly, PHR vendors are required to inform their service providers that they are subject to the Rule — MSPs should not assume the client will do this and should independently assess applicability.

4. CMMC 2.0 (32 CFR Part 170 / DFARS 252.204-7021)

The Cybersecurity Maturity Model Certification program is the DoD's mechanism for ensuring that defense contractors and their supply chains protect Controlled Unclassified Information (CUI) and Federal Contract Information (FCI). MSPs serving defense contractors are almost certainly in scope — and many are unaware of what that means for them legally.

- **CMMC 2.0 enforcement timeline:** Phase 1 (Level 1 and Level 2 self-assessments required in new DoD solicitations) went live November 10, 2025. Phase 2 (mandatory C3PAO certification for Level 2 contracts) begins November 10, 2026. By October 31, 2026, CMMC requirements will appear in all new DoD contracts. Phase 3 (Level 3 DIBCAC certifications) arrives November 2027. Organizations not certified when a Phase 2 solicitation issues cannot compete for that award.
- **How MSPs are affected:** MSPs acting as External Service Providers (ESPs) that process, store, or transmit CUI, or that handle Security Protection Data (logs, SIEM outputs, audit artifacts), are in scope for their client's CMMC assessment. An MSP does not always need its own independent CMMC certification — it can be assessed within the client's assessment scope if its role is documented in the client's System Security Plan (SSP) and Customer Responsibility Matrix (CRM). However, if the MSP serves multiple DIB clients, obtaining its own Level 2 certification may be the only scalable path.
- **110 controls across 14 domains:** CMMC Level 2 is built on NIST SP 800-171 Rev. 2. Key technical requirements include: FIPS 140-2/140-3 validated cryptography for all CUI; SIEM deployment with verified audit log ingestion and continuous correlation; CUI enclave implementation with distinct access controls; verified mailbox auditing; network segmentation; multi-factor authentication; and comprehensive incident response capabilities. These are not documentable controls — they must be operational and verifiable.
- **Capacity crisis:** As of mid-2026, approximately 97 C3PAOs are authorized to conduct CMMC assessments against 80,000+ organizations requiring certification. Average wait times to begin a formal assessment are six months. Average remediation time before assessment readiness is 6–12 months. Organizations that do not begin now risk being locked out of the Phase 2 window entirely. A Plan of Action and Milestones (POA&M) provides a conditional path if the organization scores at least 88 of 110 controls (80%) — but POA&M items must be closed within 180 days.

5. State Comprehensive Privacy Laws

The state privacy landscape has moved from a handful of active laws to a 20-state patchwork as of 2026, with more coming. While no two laws are identical, they share a common core that every MSP must address, and the differences matter for compliance.

- **The current landscape:** As of June 2026, 20 states have active comprehensive privacy laws. The newest additions — Indiana, Kentucky, and Rhode Island — took effect January 1, 2026. Connecticut's amendments take effect July 1, 2026. Maryland's Maryland Online Data Privacy Act (MODPA), the strictest yet, takes effect October 2026 and prohibits the outright sale of sensitive data. More laws are coming in 2027.
- **What every state law requires from processors (i.e., your MSP):** All 20 active state laws require written data processing agreements (DPAs) between controllers (your clients) and processors (your MSP). These DPAs must specify: the purpose and duration of processing; the nature and categories of personal data processed; obligations on the processor to assist with consumer rights requests; security standards the processor must maintain; audit rights for the controller; and restrictions on subprocessing. Standard MSP service agreements almost never contain these provisions. This is one of the highest-frequency compliance gaps in the industry.
- **California (CPRA/CCPA):** The most mature and aggressively enforced framework. Civil penalties: $2,500 per unintentional violation; $7,988 per intentional violation — applied per individual consumer, per incident. The California Privacy Protection Agency's largest settlement to date is $2.75 million. New mandatory risk assessments for processing activities presenting significant privacy risk took effect January 1, 2026. Automated Decision-Making Technology (ADMT) opt-out rights for consumers take effect January 1, 2027. California's DELETE Act requires data brokers to process deletion requests through the centralized DROP system beginning August 1, 2026.
- **State breach notification laws:** All 50 states have breach notification laws. Louisiana requires notification of the state Attorney General for breaches affecting even a single Louisiana resident. Many states now require notification within 30–45 days of discovery. New York's SHIELD Act imposes independent data security obligations on any business holding New York resident data, regardless of whether the business operates in New York. MSPs that host client data bear responsibility for compliance with the laws of every state whose residents' data is on their systems.
- **Data Protection Impact Assessments (DPIAs):** Indiana (effective June 1, 2026), Rhode Island, Connecticut (effective August 1, 2026), Maryland, and other states require DPIAs before processing activities that present heightened risk of harm — including targeted advertising, profiling, and processing of sensitive data. As a processor, your MSP may be contractually required to support these assessments

6. FCC STIR/SHAKEN, CALEA, and Telecom Compliance

MSPs that provide VoIP, UCaaS, or any form of telephone service have stepped into a regulated industry without necessarily realizing it. The FCC treats interconnected VoIP providers as telecom carriers for purposes of STIR/SHAKEN, CALEA, the Robocall Mitigation Database, and related obligations. Non-compliance is not a technical issue — it is a legal one with criminal exposure.

- **Who must comply:** All voice service providers in the U.S. call chain are subject to STIR/SHAKEN obligations — originating providers, non-gateway intermediate providers, and gateway providers. Every meaningful small-provider extension has expired. The 100,000-line threshold exemption expired in 2023. The FCC's April 2026 Fact Sheet explicitly proposes to repeal remaining undue-hardship extensions. MSPs offering UCaaS, VoIP, or any form of telephone service should assume full compliance obligations apply.
- **Robocall Mitigation Database (RMD):** Every voice provider must maintain an active RMD filing with a current Robocall Mitigation Plan and recertify annually by March 1. The 2026 recertification window opened February 1, 2026. In August 2025, the FCC removed over 1,400 voice service providers from the RMD in two enforcement actions — any traffic from those providers is blocked from U.S. networks until cured. New base forfeitures: $10,000 for inaccurate or false RMD filings; $1,000 for failure to update within 10 business days of material changes.
- **Own-certificate rule (effective September 2025):** As of September 18, 2025, providers with a STIR/SHAKEN implementation obligation must sign calls using their own certificate obtained from an approved Certificate Authority — not the certificate of a third-party signing partner. Even if signing is outsourced, the provider must (1) make all attestation level decisions and (2) ensure calls are signed with the provider's own certificate obtained via its own SPC token from the Policy Administrator.
- **Know Your Upstream Provider (KYUP):** On May 20, 2026, the FCC adopted a Further Notice of Proposed Rulemaking proposing significant new KYUP obligations. Proposed requirements include: due diligence before entering into or renewing upstream provider agreements; confirming upstream providers have compliant RMD filings and SPC tokens; checking providers against the to-be-created Foreign Adversary Control System; and evaluating traceback history. Comments are due 30 days after Federal Register publication.
- **CALEA intersection:** VoIP providers with direct number access (numbering authorizations) must file CALEA System Security & Integrity plans with the FCC before commencing service. All numbering authorization renewals now require attestation of CALEA compliance. MSPs that provide voice services may not realize they have acquired telecom provider status — with full CALEA obligations attached. Failure to file CALEA plans before service commencement is itself a violation.
- **FCC Form 499 and USF:** Providers subject to STIR/SHAKEN obligations that have not previously filed FCC Form 499-A must do so — including retroactive filings for prior years of service. Form 499 determines Universal Service Fund contribution obligations and registers the provider with the FCC. Unfiled years generate separate penalty exposure.

Where MSPs Get Into Trouble

1. **No written security program:** The FTC Safeguards Rule and the current HIPAA Security Rule both require documented, implemented written information security programs. Many MSPs have a template they purchased years ago and never operationalized. Clients in regulated industries now ask to see these programs before signing. Regulators want to see that identified risks drove documented control decisions — not that a policy document exists in a drawer.

2. **Inadequate documentation of client decisions:** When a client declines a recommended security control, that declination must be confirmed in writing, with an explanation of the risk being accepted. Without this documentation, the MSP cannot defend itself when a breach occurs involving the very control the client refused. Client ignorance is not a defense for the MSP.

3. **Contracts that inadvertently accept unlimited liability:** Standard MSP agreements may cap liability but fail to specify what security controls the MSP will implement — creating an implied warranty of comprehensive security. Limitation-of-liability clauses may not hold where courts find gross negligence. Compliance-aware contract drafting clearly delineates the MSP's security scope and does not inadvertently warrant what is not being delivered.

4. **No designated compliance owner:** The FTC Safeguards Rule requires a Qualified Individual responsible for the information security program. The proposed HIPAA Security Rule would formalize a similar requirement. Larger clients increasingly require a named compliance point of contact. If no one in your organization owns compliance, nothing will be consistently implemented or documented.

5. **Missing or deficient data processing agreements:** All 20 active state privacy laws require written DPAs between controllers and processors. Most standard MSP agreements contain no DPA. This is not a minor gap — it is a direct violation of the applicable state law that can be enforced independently of any breach occurring.

6. **Telecom services without regulatory standing:** MSPs offering VoIP or UCaaS without RMD filing, STIR/SHAKEN implementation, and CALEA compliance plans are operating as unregistered telecom providers. The FCC removed over 1,400 providers from the RMD in 2025 — blocking their traffic overnight. This is not a theoretical risk.

7. **Unsigned, unfiled, or outdated BAAs:** Business Associate Agreements that are not signed, not implemented, or not updated to reflect current HIPAA requirements are as dangerous as having no BAA at all. OCR finds BAA deficiencies in nearly every investigation. Annual BAA review and vendor compliance verification are now effectively required even under the current rule.

8. **Misrepresented CMMC compliance:** MSPs that tell defense contractor clients their security practices meet CMMC requirements without independent verification face DOJ False Claims Act exposure. A federal indictment issued in December 2025 charged an individual — not a company — for misrepresenting cybersecurity compliance to obtain federal contract work. Individual criminal liability is a real outcome.

Contracts, Documentation, and Legal Infrastructure

Beyond the technical requirements of each regulatory framework, the legal infrastructure supporting your compliance posture — your contracts, documentation practices, and organizational structure — determines whether you can defend yourself when things go wrong.

- **The BAA problem:** Many MSPs have signed Business Associate Agreements with healthcare clients but have never implemented the security controls those agreements require. Courts and OCR treat unsigned or unimplemented BAAs as violations of both the contract and the HIPAA Security Rule. Worse, BAAs that limit the MSP's liability in ways inconsistent with HIPAA are themselves non-compliant. BAAs should be reviewed annually and updated to reflect the proposed Security Rule changes before they take effect.
- **Limitation-of-liability clauses and their limits:** Standard MSP agreements typically include caps on liability, often limited to fees paid in the prior 12 months. These caps have been challenged and sometimes pierced in data breach litigation, particularly where the MSP's negligence is characterized as gross negligence or willful misconduct — both of which are typically carved out of liability caps. Well-drafted agreements specify exactly what security controls the MSP will implement, document agreed-upon service levels for security functions, and clearly allocate responsibility for compliance obligations that neither party should be allowed to disclaim entirely.
- **Client declination letters:** When a client refuses a recommended security control or configuration, that refusal should be memorialized in writing immediately — with a clear explanation of the security risk being declined. Without this documentation, MSPs who later face breach liability cannot demonstrate they exercised reasonable professional care. Industry best practice is to treat these letters as mandatory, not optional.
- **DPAs are now a baseline requirement:** If your MSP handles personal data on behalf of clients in any of the 20 states with active comprehensive privacy laws, your client agreements must include compliant data processing agreements. These are not the same as BAAs, confidentiality provisions, or general privacy clauses. They require specific terms mandated by state law, and failure to have them in place exposes both your MSP and your client to enforcement action and civil liability.

The Cost of Getting It Wrong

Compliance failures carry real price tags. The current HIPAA Security Rule's willful neglect tier reaches $73,011 per day, per violation category. The FTC can impose civil penalties of up to $51,744 per violation for Safeguards Rule violations — assessed per individual affected customer, per incident. CMMC non-compliance means loss of DoD contract eligibility and potential debarment. FCC fines for STIR/SHAKEN and RMD violations accrue daily. State privacy penalties are per-consumer, and California's largest CPRA settlement to date is $2.75 million.

Reputational damage hits harder and faster. Word of a breach spreads through industry networks before regulators call. Clients share what their MSP did wrong at peer gatherings and conferences. A single significant breach — and the disclosure that the MSP lacked basic documentation or contractual protections — can end relationships with multiple clients simultaneously.

The personal liability dimension is no longer theoretical. The SEC has taken enforcement action against individual executives for misrepresenting cybersecurity posture. Federal prosecutors charged an individual for CMMC compliance fraud in 2025. State attorneys general are naming individuals in privacy law enforcement actions. Compliance is no longer only a corporate risk.

The Competitive Upside of Getting It Right

Compliance is not only about avoiding penalties. It is a competitive differentiator most MSPs are leaving on the table. SMB clients often struggle to distinguish one MSP from another, so price becomes the default. A documented compliance practice breaks that cycle.

- **Win regulated-industry clients.** Healthcare, finance, DoD, and government clients require vendors with demonstrable compliance. A well-documented security posture and a library of compliant agreements opens doors that are closed to less-prepared MSPs.
- **Command better contract terms.** Understanding your obligations lets you negotiate agreements that allocate risk fairly rather than inadvertently accepting unlimited liability for an undefined security scope.
- **Package compliance as a service line.** Compliance obligations — Safeguards Rule WISPs, HIPAA risk analyses, CMMC readiness support, DPA drafting — are billable, recurring services. Turning regulatory burden into revenue with higher-value, stickier clients is the MSP business model for this regulatory environment.
- **Strengthen cyber insurance.** MSPs with documented programs and clean records get better rates and fewer exclusions at renewal, when insurers are tightening underwriting more than ever. The 10 controls that most underwriters now require — MFA, EDR, tested backup, email security, patch management, security awareness training, written IR plan, vendor inventory, network segmentation, privileged access management — map directly to the FTC Safeguards Rule technical requirements.

Why You Need Industry-Specific Legal Counsel

General business attorneys and large law firms miss the 2026-specific nuances that matter most — from the HIPAA Security Rule's pending changes and the expanded FTC obligations to CMMC's ESP scoping rules and the DPA requirements now active in 20 states. They may draft a contract that looks complete on the surface but leaves you exposed.

At Bronston Legal, we know your business, not just the law. We understand MSP operating models, channel partner agreements, and telecom regulatory frameworks. We spot the risks that generalist lawyers miss and we move faster because there's no learning curve.

Our compliance services include:

- HIPAA Security Rule compliance analysis and Business Associate Agreement drafting and review
- FTC Safeguards Rule assessments and Written Information Security Program (WISP) drafting
- FTC Health Breach Notification Rule compliance and breach response preparation
- CMMC 2.0 readiness assessment, scoping, and vendor agreement review
- State privacy law data processing agreement (DPA) drafting — all 20 active states
- FCC and telecom regulatory compliance: STIR/SHAKEN, RMD filings, CALEA guidance
- MSA, SLA, and client agreement drafting and review with current liability allocation
- Client declination letters and compliance documentation frameworks
- Cyber insurance readiness assessments
- Ongoing compliance counsel for MSPs operating across multiple regulatory frameworks

Ready to get compliant and stay that way?

Bronston Legal is the trusted counsel of choice for MSPs, service providers, channel partners, and their customers nationwide.

Reach out today to learn how we can help protect and grow your business.

info@techlawyers.com
techlawyers.com
888-469-0579