SOC 2 Type 2 and HIPAA/HITECH Compliance Infrastructure

HOTB Software Solutions

HOTB Software Solutions delivers secure, cloud-based, **purpose-built systems for federal program administration**. With more than $10 billion in appropriated funds managed across 20+ public-sector agencies and over 1.1 million applications processed, HOTB has engineered its security and compliance posture to meet the rigorous expectations of federal stakeholders. Our systems are hosted entirely within U.S.-based Amazon Web Services (AWS) data centers and are governed by two parallel, third-party Type 2 attestations — a SOC 2 Type 2 report, and a HIPAA/HITECH Type 2 report. Both examinations were performed under AICPA attestation standards for the 12-month period ending November 15, 2025, and both were issued by the independent service auditor on December 1, 2025.

SOC 2 Type 2 Attestation

HOTB's SOC 2 Type 2 examination was performed under the AICPA attestation standards (AT-C 105 and AT-C 205) and the 2017 Trust Services Criteria for Security (TSP section 100). The auditor issued a clean opinion concluding that HOTB's controls were both suitably designed and operated effectively throughout the November 16, 2024 to November 15, 2025 examination period. All Common/Security criteria were applicable to the system, and no significant incidents were reported.

HIPAA / HITECH Type 2 Attestation

HOTB's HIPAA/HITECH Type 2 examination was performed under the AICPA attestation standards (AT-C 105, AT-C 205, and AT-C 315) over the same November 16, 2024 to November 15, 2025 examination period. The auditor issued a clean opinion confirming that HOTB's systems were suitably designed, fairly presented, and that controls operated effectively throughout the period to meet applicable HIPAA and HITECH requirements. No significant incidents were reported during the examination period.

The examination tested controls across all five HIPAA Security Rule families: Administrative Safeguards, Physical Safeguards, Technical Safeguards, Organizational Requirements, and Breach Notification. AWS serves as the subservice organization for physical and infrastructure security under a formal Business Associate Agreement (BAA). Technical safeguards examined include AWS KMS encryption of electronic Protected Health Information (ePHI) at rest, TLS-encrypted transmission, AWS CloudTrail audit logging, AWS GuardDuty intrusion detection, AWS WAFv2 traffic filtering, and Amazon Inspector vulnerability scanning. For federal programs handling PHI, ePHI, or sensitive health-related applicant data, HOTB brings demonstrated, third-party-attested HIPAA operational maturity to the engagement.

Key Security and Compliance Controls

The following controls form the operational backbone of HOTB's compliance program and are reviewed continuously as part of HOTB's internal audit cycle and external SOC 2 Type 2 examination:

- **Access Control.** Role-based access enforced under least-privilege principles; authentication via account credentials, multi-factor authentication (MFA), and AWS IAM. Access reviewed quarterly with immediate revocation upon personnel changes.
- **Encryption.** AES-256 encryption at rest for all sensitive data; TLS 1.2+ encryption in transit using strong cipher suites, with deprecated protocols disabled.
- **Monitoring and Logging.** Centralized logging via AWS CloudWatch and CloudTrail; AWS GuardDuty and AWS WAF provide real-time threat detection. Audit logs are immutable, tamper-evident, and reviewed quarterly.
- **Change Management.** Formal change-control process with segregation of duties; isolated development, QA, and production environments; QA regression testing required prior to any production deployment.
- **Backup and Disaster Recovery.** Layered backup schedule (daily 30-day, weekly 90-day, monthly long-term retention) replicated across geographically separated AWS regions in Northern California, Northern Virginia, and Ohio. Recovery Time Objective of 30 minutes; Recovery Point Objective of 24 hours. Restoration procedures are validated through quarterly disaster recovery drills.
- **Incident Response.** Documented IT and security incident response procedures; real-time alerting for severe events; automatic security ticket generation and defined escalation paths.
- **Risk Management.** Continuous risk assessment classified as low, medium, or high; high-risk items routed directly into HOTB's internal audit program. Risk program reviewed and updated annually under board oversight.
- **Personnel Controls.** Background checks for new hires, signed confidentiality agreements, and annual mandatory training on information security and privacy policies.

Why It Matters for Federal Partners

By combining a SOC 2 Type 2 attestation and a parallel HIPAA/HITECH Type 2 attestation, HOTB delivers a compliance posture that is both auditable and operationally proven. Two clean third-party opinions, issued in the same week by the same independent service auditor, for the same 12-month operating period, give federal partners independent validation that the platform's controls were not only designed correctly but operated effectively throughout an entire year of live production. The result is a Software Solution that federal agencies can deploy with confidence — secure by design, compliant by construction, and ready for audit on day one.