HIPAA & HITECH Compliance

Overview

Motorola Solutions understands that in mission critical environments, data protection is inseparable from mission success, legal defensibility, and public trust. Our HIPAA Business Associate compliance program is designed to operate at the intersection of emergency response, regulated healthcare data, and government-grade security expectations.

We conduct privacy and security assessments, legal due-diligence reviews, and operational audits as part of our commitment to transparency, resilience, and public safety protection.

Applicability of Business Associate Obligations

Motorola Solutions communicates with its customers and conducts an analysis at the outset of each engagement to determine whether Business Associate obligations apply. Where our systems create, receive, maintain, or transmit Protected Health Information ("PHI") in support of public safety, emergency response, or healthcare-adjacent operations, we formally assume Business Associate responsibilities. This ensures precise regulatory alignment without overextension of legal exposure across mission systems.

Business Associate Agreement Governance

Prior to any access to PHI, Motorola Solutions executes a Business Associate Agreement (BAA) with each Covered Entity as applicable. These agreements establish enforceable controls governing permitted use, disclosure restrictions, safeguard obligations, breach notification timelines, and subcontractor controls. Once in force, operational systems, workforce conduct, and vendor relationships are governed by the BAA as a binding legal instrument.

Purpose Limitation & Controlled Access

PHI handled by Motorola Solutions is accessed solely for authorized operational purposes in support of emergency response, public safety operations, continuity of care, or system functionality. Layered access controls, operational segmentation, and least-privilege enforcement ensure personnel access only the information required to perform their duties. Unauthorized secondary use is formally prohibited by customer and supplier contracts, policies, procedures, technical design, and workforce enforcement.

Mission-Critical Administrative, Technical & Physical Safeguards

Motorola Solutions maintains a security architecture engineered for mission critical environments where uptime, resilience, and data integrity are paramount. Safeguards include encryption at rest and in transit, continuous system monitoring, intrusion detection, secure

authentication, detailed audit logging, secure facility controls, and environmental protections for infrastructure supporting emergency operations. Security design reflects the realities of 24/7 public safety operational continuity.

Risk Analysis & Operational Security Governance

Motorola Solutions maintains a continuous risk-management lifecycle designed to identify, assess, prioritize, and remediate threats across public safety information systems. Risk analyses are formally documented, reviewed by leadership, and aligned with operational mission demands. Written governance policies guide security operations, privacy protection, incident escalation, and system configuration in high-availability environments.

Workforce Training & Operational Accountability

All workforce members with potential access to PHI receive training on Motorola Solutions policies and procedures which were developed to address Motorola Solutions obligations towards PHI among other privacy and data security compliance obligations, such as other international and state health laws. Training addresses legal obligations, secure system usage, incident escalation chains, and public-trust responsibilities. Compliance is tracked and enforced under formal accountability and disciplinary standards consistent with public safety operating expectations.

Incident Detection, Public Safety Breach Response & Notification

Motorola Solutions operates a structured and tested incident-response program designed to function under real-world emergency conditions. Upon detection of any impermissible use, security incident, or breach involving PHI, Covered Entities and relevant authorities are notified without undue delay. Response procedures emphasize forensic preservation, operational containment, regulatory compliance, and cross-agency coordination.

Support for Individual Rights & Lawful Access

Where required by law or contract, Motorola Solutions supports Covered Entities in fulfilling individuals' rights of access, amendment, and accounting of disclosures. These workflows are designed to coexist with lawful-access obligations, public safety investigative requirements, and records-retention rules without compromising system security or evidentiary integrity.

Subcontractor & Public Safety Vendor Flow-Down Protections

Subcontractors are assessed using Motorola Solutions' supplier review process and if the subcontractor may access PHI on behalf of Motorola Solutions, the subcontractor is required to enter into comparable terms that will contractually bind the subcontractor to equivalent security, confidentiality, and incident-response obligations.

Return or Secure Destruction of PHI

Upon completion or termination of services, PHI is returned to the Covered Entity or securely destroyed in accordance with contractual terms.

Demonstrating Motorola Solutions Compliance

Motorola Solutions maintains comprehensive privacy and security programs which are internally and externally audited on an annual basis. Our privacy program is internally audited on an annual basis to the NIST Privacy Framework and externally audited to ISO/IEC 27701:2019 as well as all trust criteria, including privacy under the AICPA SOC2 framework. Our SOC2 report related to our Command Center offerings includes HIPAA criteria. Additional compliance information and copies of our ISO certificates or SOC3 reports summarizing our SOC2 reports may be found on the Motorola Solutions Trust Center compliance page.