Snap
Solutions for Occupational Medicine

Snap System Security & Compliance Policies

1 Purpose

This policy establishes the framework to protect the organization's information assets, ensuring confidentiality, integrity, and availability. It defines the security measures, compliance requirements, and operational procedures necessary to safeguard sensitive data. All information within this documented may also be referenced a www.snapsolutions.com

2. Scope

This policy applies to all employees, contractors, and third-party vendors accessing or handling the organization's information systems and data.

3. Legal Compliance

3.1 **Compliance with FMCSA Regulations on Driver Examination Data**

- Driver medical exam data is securely stored and transmitted per FMCSA rules. (FMCSA Submission Application in Process - Pending Approval)
- Data is encrypted using AES-256 (Advanced Encryption Standard with 256-bit keys), ensuring robust protection against unauthorized access. AES-256 is a symmetric encryption algorithm widely recognized for its high security, making brute-force decryption infeasible.
- Only authorized personnel with credentials verified through Multi-Factor Authentication (MFA) and Role-Based Access Control (RBAC) are permitted to access sensitive data.

3.2 **Compliance with HIPAA for Protecting Health Information**

- Protected Health Information (PHI) is encrypted both in transit and at rest. TLS (Transport Layer Security) 1.2/1.3 secures data transmission, preventing interception, while AES-256 encryption ensures data storage remains impenetrable.
- RBAC limits access to PHI exclusively to personnel with appropriate healthcare roles, reducing the attack surface and mitigating insider threats.
- A comprehensive logging system records data access events, ensuring traceability and accountability.

3.3 **Compliance with Federal Trade Commission (FTC) Rules on PII Protection**

- Personally Identifiable Information (PII), including names, addresses, and social security numbers, is encrypted using AES-256 to render the data unreadable without proper decryption keys.
- Multi-Factor Authentication (MFA) combines user credentials with secondary factors (e.g., one-time codes, biometric verification) to prevent unauthorized account access.

- Secure hashing algorithms (e.g., SHA-256) are used to protect sensitive user credentials, ensuring even compromised databases cannot reveal passwords.

4. Data Security

4.1 Encryption of Data at Rest and in Transit

- Data at rest is secured using AES-256 encryption, ensuring data stored on physical servers or cloud databases remains protected.

- Data in transit is safeguarded with TLS 1.2/1.3 protocols, using strong cipher suites (e.g., AES-GCM, ECDHE) to prevent eavesdropping, man-in-the-middle attacks, and data tampering.

- Encryption keys are managed securely using a Key Management System (KMS), ensuring regular rotation and restricted access.

4.2 Implementation of Role-Based Access Control (RBAC)

- RBAC enforces least-privilege access, where users can only access the data necessary for their job functions.

- Each use roles has defined permissions, ensuring sensitive data operations (e.g., deletion, export) are restricted.

- Periodic access reviews ensure permissions remain appropriate and inactive accounts are deactivated promptly.

4.3 Implementation of Audit Logging for Data Access and Modifications

- Detailed audit logs record user access, data retrievals, modifications, and deletions. Logs include user ID, timestamp, IP address, and action details, enabling rapid incident investigation.

- Audit logs are secured from tampering through Write Once Read Many (WORM) storage and cryptographic signing.

4.4 Regular Security Audits and Vulnerability Assessments

- External cybersecurity firms will conduct annual penetration tests, simulating real-world attacks to identify vulnerabilities.

- Automated vulnerability scanners will assess infrastructure, web applications, and code repositories for security flaws

- Security results will drive patching and remediation efforts.

5. Privacy Protection

5.1 **Defined Data Retention Policies for Driver Records**

- Data lifecycle policies will define record retention durations, archival strategies, and secure deletion processes.

- Metadata tagging ensures records are easily identified for retention or disposal.

5.2 **Secure Disposal Methods for Outdated or Expired Data**

- Secure disposal methods include cryptographic erasure (e.g., NIST 800-88 compliance) and physical media destruction.

5.3 **Incident Response Plan for Data Breaches**

- The incident response plan details breach detection, containment, forensic analysis, mitigation, and regulatory reporting.

- A cybersecurity insurance policy will ensure financial resilience in case of data breaches.

6. System Security

6.1 **Regular Software and Security Patch Updates**

- Patch management tools (e.g., WSUS, SCCM, Ansible) automate system updates.

- Critical patches are deployed within 3 days of release.

6.2 **Secure Storage of Driver Examination Results with Controlled Access**

- Amazon S3 buckets are configured with fine-grained Identity and Access Management (IAM) policies.

- Data is encrypted at rest with AWS KMS-managed AES-256 keys.

6.3 **Data Backup and Disaster Recovery Plans**

- Backups include full daily snapshots and hourly incrementals.

- Backup integrity is verified through periodic restore tests.

6.4 **Firewall and Intrusion Detection System (IDS)**

- Next-generation firewalls (NGFWs) inspect traffic for malware and anomalies.

- IDS systems detect signature-based attacks (e.g., SQL injections, buffer overflows) and zero-day anomalies.

7. FMCSA Compliance

7.1 Automated Upload of Examination Results to FMCSA NRCME

- An API integration securely uploads encrypted examination results to FMCSA's National Registry (FMCSA Submission Application in Process - Pending Approval)

7.2 Retaining Driver Medical Records for at Least 3 Years

- Data retention policies ensure records are preserved securely for 3+ years, preventing accidental deletion while enabling secure retrieval.

7.3 Ensuring Third-Party Vendors Comply with FMCSA Regulations

- Vendors must present evidence of compliance and complete security questionnaires.

7.4 Upload / Interface DOT Exams / Results Timeline

- All Results will be interfaced / uploaded to FMCSA by days end test / exam was performed.

7.5 Customer Service line Availability for Certified Medical Examiners

- Available hours for customer service issues are 9am to 5pm PST, Mon-Fri. 323-543-0040

8. System Maintenance

8.1 Regular System Upgrades as per FMCSA Policies

- All systems undergo quarterly updates, with rollback plans for failed upgrades.

8.2 Monitoring System Performance and Resolving Vulnerabilities

- SIEM platforms will analyze logs in real time, flagging abnormal behaviors.

8.3 Ensuring Compliance with New FMCSA Regulatory Updates

- Regulatory monitoring tools track FMCSA policy changes to ensure compliance.

9. Policy Review and Update

This policy will be reviewed annually, or as significant changes occur in regulations or business operations.