VACCINATION CARD SYSTEM (SYCVAC)
&
RED-IMMUNIZATION CARD(RIC) or RED-CARD
Limited Liability Company (LLC)

SYCVAC (Vaccination Card System) & IT-LOBS LLC
California, United States of America **(USA)**

SYCVAC Platform: Global Digital Immunization Privacy & Governance Policy

Document Type: Enterprise Privacy Policy & Data Governance Framework

Version: 3.0

Effective Date: January 7 2023

Last Updated: March 19th 2026

Classification: Public External Facing **Companion Document:** SYCVAC Security & Compliance White Paper (architecture, encryption, IAM/RBAC, HIPAA safeguards, ISO/NIST alignment, disaster recovery, and interoperability, see Section 26)

1. Introduction

SYCVAC ("we," "us," "our," or the "Company") operates the SYCVAC Platform (the "Service" or "Platform"), a digital immunization governance infrastructure comprising four interoperating services: a Digital Immunization Record, a Digital Immunization Passport, a Digital Immunization Credential, and Public Health Surveillance capabilities supported by AI-driven predictive analytics.

This Policy is written to serve as a reference document for a broad set of stakeholders, including Ministries of Health, National Immunization Programs, hospitals and healthcare networks,

international health organizations, public health agencies, and technology integration partners. It describes what information the Platform collects, how it is used and shared, the legal and technical safeguards applied, and the respective responsibilities of the Company, healthcare providers, government bodies, and end users.

This Policy does not replace jurisdiction-specific Data Processing Agreements (DPAs), Business Associate Agreements (BAAs), or bilateral Memoranda of Understanding (MOUs) executed with government or institutional partners; where such agreements exist, their terms govern the specific relationship in addition to this Policy.

SYCVAC's comprehensive approach to privacy protection, data security, and operational resilience. By implementing advanced cybersecurity principles, privacy-by-design practices, and enterprise-grade security controls, SYCVAC provides a trusted digital foundation for national and international immunization programs, ensuring that vaccination information remains secure, accessible, and protected throughout an individual's lifetime.

2. Scope of Service

This Policy applies to all data processed through:

- The SYCVAC mobile and web applications used by individuals ("Users").
- Provider-facing interfaces used by clinicians and vaccination sites ("Provider Portal").
- Government and institutional dashboards used by health authorities ("Authority Console").
- Application Programming Interfaces (APIs) are used for interoperability with national immunization registries, electronic health record (EHR) systems, and international health credential frameworks.
- Backend infrastructure, including data storage, credentialing services, analytics pipelines, and audit systems.

This Policy applies globally but is implemented with jurisdiction-specific configurations (e.g., data residency, retention periods, and consent mechanics) to comply with local law. Where local law imposes a stricter requirement than this Policy, local law prevails for that jurisdiction.

3. **Definitions**

Term	**Definition**
Digital Immunization Record (DIR)	The longitudinal, authoritative record of an individual's vaccination and immunization history is maintained on the Platform.
Digital Immunization Passport (DIP)	A portable representation of immunization status used for travel, border entry, or access-control purposes.
Digital Immunization Credential (DIC)	A cryptographically signed, machine-verifiable artifact (e.g., verifiable credential, signed QR code) enabling a third party to verify status without accessing the full DIR.
Verifier	Any party (e.g., border official, employer, venue operator) that scans or checks a DIC.
Issuing Authority	The healthcare provider, facility, or government body authorized to record an immunization event and trigger credential issuance.
De-identified Data	Data from which direct and indirect identifiers have been removed such that it cannot reasonably be re-linked to an individual.
Pseudonymized Data	Data in which identifying fields are replaced with artificial identifiers, re-linkable only via separately secured keys.

Term	Definition
Personal Health Information (PHI)	Identifiable health information as defined under applicable law (e.g., HIPAA, GDPR "special category data").
Data Controller	The entity determining the purposes and means of processing (typically the relevant Ministry of Health or the Company, depending on jurisdiction and contractual arrangement).
Data Processor	The entity processing data on behalf of a Controller (typically the Company or a subprocessor).

4. Governance Roles and Responsibilities

Role	Primary Responsibilities
SYCVAC (Platform Operator)	Operates and secures the Platform; acts as Data Processor for government-controlled deployments and as Data Controller for direct-to-consumer features, as specified in the deployment agreement.
Ministries of Health / National Immunization Programs	Typically act as Data Controller for national deployments; define retention, reporting, and consent policy within local law; authorize Issuing Authorities.
Healthcare Providers	Act as Issuing Authorities, responsible for the accuracy of immunization data entered into the Platform (see Section 19).

Role	Primary Responsibilities
Data Protection Officer (DPO) / Privacy Office	Oversees Company-wide privacy compliance, handles user rights requests, liaises with regulators (see Section 28).
Platform Governance Board	Where established under a national deployment, provides oversight of AI/analytics use, surveillance data governance, and policy exceptions (see Sections 9–10).
Independent Security Auditor	Performs periodic third-party audits referenced in the companion Security & Compliance White Paper.

5. Information Collected

5.1 Identity and Account Information

Name, date of birth, national ID or passport number (where required for cross-border verification), contact details, authentication credentials, and biometric identifiers used strictly for identity binding where legally permitted and consented to.

5.2 Immunization and Health Data

Vaccine type, manufacturer, lot number, dose sequence, administration date and location, administering provider, adverse event reports, medical exemptions, and prior-infection or immunity documentation.

5.3 Credential and Verification Metadata

Cryptographic key material, issuance and revocation timestamps, and verification event logs (time, verifier identity, and validity outcome).

5.4 Device, Network, and Usage Data

Device identifiers, IP address, application version, session logs, and diagnostic/crash data.

5.5 Location Data

Coarse or precise location is collected only where a feature (e.g., outbreak proximity alerts) requires it and only with explicit, separately revocable consent.

5.6 Surveillance and Analytics Inputs

De-identified or pseudonymized immunization coverage data, demographic aggregates, and epidemiological indicators used for outbreak modeling (see Sections 9–10).

6. Digital Immunization Record Privacy

The DIR is the authoritative, longitudinal health record maintained per individual. Specific protections:

- Access to a full DIR is restricted to the individual (or guardian), authorized Issuing Authorities involved in their care, and authorized government reviewers acting under a lawful basis.
- Amendments to the DIR require verification against the Issuing Authority's source record; users may request correction but cannot unilaterally edit clinical entries (see Section 18).
- The DIR is logically and, where required by law, physically segregated by jurisdiction to support data residency requirements.
- Historical versions of the DIR are retained in an immutable audit trail (see Section 16) to preserve clinical integrity and detect tampering.

7. Digital Immunization Passport Privacy

The DIP packages a subset of DIR data for travel, border-entry, or facility-access use cases.

- The DIP discloses only the data elements required for the specific use case (e.g., vaccine name and date, not full clinical history), following a minimum-necessary design principle.

- Users control which DIP "profile" (e.g., a travel-specific export) is generated for a given purpose, where the deployment configuration allows.
- DIP data shared with border or immigration authorities is subject to the receiving jurisdiction's own data protection law upon receipt; SYCVAC's obligations under this Policy govern only the transmission and the data retained on-Platform.

8. Digital Immunization Credential Privacy

The DIC is a cryptographically signed artifact enabling offline or low-connectivity verification.

- DICs are signed using asymmetric cryptography; private signing keys never leave the issuing infrastructure (as detailed in the companion Security & Compliance White Paper).
- A Verifier scanning a DIC receives a validity result (e.g., valid/invalid, expiry date) and, where configured, a minimal display payload (e.g., name and vaccine status) — not the full DIR.
- Revoked or expired credentials fail verification immediately upon the next connectivity-based revocation check; offline verification windows are bounded by policy-configurable expiry.
- Verifiers are contractually and technically prevented from bulk-harvesting DIC data; verification logs are retained by SYCVAC for audit purposes as described in Section 16.

9. Public Health Surveillance Data Governance

- Surveillance analytics rely on de-identified or aggregated data by default. Identifiable data is used only where a specific legal mandate (e.g., notifiable disease reporting) requires it, and only to the extent that the mandate specifies.
- A documented **de-identification standard** (e.g., expert determination or safe-harbor methodology consistent with applicable law) governs what qualifies as de-identified for surveillance purposes; this standard is available to Governance Board members and auditors on request.

- Aggregated outputs (coverage maps, outbreak indicators, dashboards) are reviewed for re-identification risk (e.g., small-cell suppression in low-population areas) before publication.
- Data used for surveillance is logically partitioned from operational credentialing data to reduce the risk of purpose-creep.
- Where a national deployment operates under a Data Sharing Agreement with a Ministry of Health, that Agreement governs the specific surveillance data flows and retention for that jurisdiction, supplementing this Policy.

10. AI and Predictive Analytics Governance

The Platform may use AI/machine-learning models (e.g., outbreak-risk prediction, coverage-gap forecasting, anomaly detection in adverse-event reporting).

- **Training data:** Models are trained on de-identified or synthetic data wherever feasible. Use of identifiable data for model training requires a documented legal basis and Governance Board approval where applicable.
- **Human oversight:** Predictive outputs used to inform public health decisions (e.g., outbreak alerts) are reviewed by qualified epidemiological staff before action; the Platform does not autonomously trigger enforcement actions (e.g., travel restrictions) without human authorization.
- **Explainability:** Where AI outputs materially affect an individual (e.g., flagging a credential for manual review), the individual may request a general explanation of the factors involved, subject to trade-secret and security limitations.
- **Bias and validation:** Models are periodically evaluated for demographic bias in coverage and outbreak predictions; validation methodology is documented for regulator and Governance Board review.
- **No automated individual denial:** The Platform does not use AI to autonomously deny an individual's credential validity solely on predictive/statistical grounds unrelated to their actual immunization record.

11. Data Processing Legal Basis

Processing is conducted under one or more of the following bases, as applicable per jurisdiction:

- **Consent** (e.g., optional location-based features, biometric binding).
- **Contract** (providing the Service to a registered User).
- **Legal obligation** (public-health reporting mandates).
- **Public interest / public health** (surveillance, outbreak response), consistent with frameworks such as GDPR Art. 9(2)(i), HIPAA public health exceptions, or equivalent national statutes.
- **Legitimate interests** (fraud prevention, platform security, service improvement), balanced against individual rights via documented Legitimate Interest Assessments where required.

12. Information Sharing

Recipient	Purpose	Data Shared	Basis
Ministries of Health / National Immunization Programs	Program administration, mandated reporting	Identifiable or aggregate, per national law	Legal obligation / public interest
Credential Verifiers	Status verification	Minimum-necessary validity signal	Contract/consent
Healthcare Providers	Recording/updating immunizations	Relevant DIR entries	Contract/user authorization
International Health Organizations	Cross-border surveillance cooperation	De-identified/aggregated	Public interest, per applicable treaty or agreement
Technology Subprocessors (cloud hosting, messaging, analytics)	Platform operation	As needed, under DPA	Contract
Regulators / Courts	Legal compliance	As legally required	Legal obligation

Recipient	Purpose	Data Shared	Basis
Successor Entities	Merger, acquisition, restructuring	Subject to equivalent protections	Contract / legitimate interest

We do not sell personal data, and we do not use immunization or health data for advertising purposes.

13. International Data Transfers

- Where feasible, data is stored within the region of the deploying Ministry of Health or institutional partner to satisfy data residency requirements.
- Cross-border transfers (e.g., DIP verification at an international border, cross-national surveillance cooperation) are governed by appropriate safeguards: Standard Contractual Clauses, adequacy determinations, binding corporate rules, or equivalent mechanisms recognized under applicable law.
- A jurisdiction-by-jurisdiction data residency and transfer map is maintained and made available to institutional partners and auditors on request.

14. Security Architecture

This Policy addresses security at a governance level. Full technical detail — cloud infrastructure design, encryption standards, network segmentation, and key management — is documented separately in the **SYCVAC Security & Compliance White Paper**, provided to institutional partners, auditors, and regulators under appropriate confidentiality terms. At a policy level:

- Data is encrypted in transit and at rest using industry-standard cryptographic algorithms.
- Environments are segmented by function (credentialing, surveillance, provider access) to limit blast radius in the event of compromise.
- Infrastructure and application security are subject to periodic independent penetration testing and vulnerability assessment.

15. Identity and Access Management

- Access to Platform systems is governed by Role-Based Access Control (RBAC), granting the minimum permissions necessary for a given role (User, Provider, Authority Reviewer, Administrator, Auditor).
- Multi-factor authentication (MFA) is required for all Provider Portal, Authority Console, and administrative access.
- Access provisioning and deprovisioning follow documented joiner-mover-leaver processes; access reviews are conducted periodically.
- Privileged access to production health data is logged and subject to just-in-time elevation and approval workflows where technically supported.
- Detailed IAM/RBAC architecture is described in the companion Security & Compliance White Paper.

16. Audit Logging

- All access to identifiable immunization data, all credential issuance and verification events, and all administrative actions are logged in an immutable audit trail.
- Audit logs capture actor identity, timestamp, action, and (where applicable) justification/purpose code.
- Logs are retained per Section 17 and are made available to authorized regulators, Governance Boards, and institutional partners for compliance review.
- Anomalous access patterns (e.g., bulk record access, off-hours privileged access) trigger automated alerting to the security operations function (see Section 23).

17. Data Retention

Data Category	**Retention Period**
Digital Immunization Record	Duration required by applicable public-health record-keeping law, or account lifetime, whichever is longer
Credential verification logs	12–24 months (configurable per jurisdiction), then deleted or aggregated

Data Category	Retention Period
Audit logs	Minimum period required by applicable regulatory/security standard (e.g., typically 1–7 years depending on jurisdiction)
Surveillance data (de-identified)	Retained indefinitely for public health research, subject to Governance Board review
Surveillance data (identifiable, legally mandated)	Retained only as long as the specific legal mandate requires
Account/profile data after deletion request	Deleted or anonymized within [X] days, subject to legal retention exceptions

18. User Rights

Subject to applicable law, individuals may have the right to:

- Access their DIR, DIP export history, and DIC verification logs.
- Request correction of inaccurate data, subject to verification against the Issuing Authority's source record.
- Request deletion of account data, except where retention is legally mandated.
- Restrict or object to specific processing (e.g., withdraw from optional surveillance features).
- Receive their data in a portable, commonly used format.
- Withdraw consent for optional features at any time, without affecting the lawfulness of prior processing.
- Lodge a complaint with a competent supervisory authority or the Company's Privacy Office (Section 28).

19. Healthcare Provider Responsibilities

Healthcare Providers acting as Issuing Authorities are responsible for:

- Accurately entering immunization events into the Platform at the time of administration.
- Verify patient identity before issuing a DIR entry or triggering credential issuance.

- Report adverse events through designated channels in accordance with national pharmacovigilance requirements.
- Maintaining their own access credentials securely and promptly reporting suspected compromise.
- Comply with applicable professional, licensing, and data protection obligations independent of this Policy.

20. Government / Public Health Authority Responsibilities

Ministries of Health, National Immunization Programs, and public health agencies using the Platform are responsible for:

- Defining and authorizing the scope of surveillance data use within their jurisdiction, consistent with local law.
- Authorizing and deprovisioning Issuing Authorities and Authority Console users.
- Ensuring any identifiable data requested under a legal mandate is limited to what the specific mandate requires.
- Establishing and, where applicable, chairing the Platform Governance Board for their deployment.
- Coordinating with the Company on incident response and breach notification obligations specific to their jurisdiction (Section 23).

21. Children's Privacy

Where the Platform records a minor's immunizations, the minor's DIR is created and managed by a parent or legal guardian. Minors do not independently register or manage DICs without guardian oversight, consistent with applicable child-privacy law. Access transitions to the individual upon reaching the age of majority in their jurisdiction, or as otherwise provided by local law.

22. Third-Party Integrations

- The Platform interoperates with national immunization registries, EHR systems, and international digital health credential frameworks via secured APIs.
- Integration partners are subject to data-sharing agreements specifying permitted use, security requirements, and audit rights.
- The Company maintains a registry of active third-party integrations and subprocessors, available to institutional partners and regulators on request.
- Interoperability standards and API architecture are detailed in the companion Security & Compliance White Paper.

23. Incident Response

- The Company maintains a documented incident response plan covering detection, containment, eradication, recovery, and notification.
- Suspected or confirmed breaches involving identifiable health data trigger notification to affected Ministries of Health, institutional partners, and, where legally required, affected individuals and regulators, within the timeframes mandated by applicable law (e.g., 72 hours under GDPR, or as specified under HIPAA/local breach notification statutes).
- A post-incident review is conducted for material incidents, with findings shared with the relevant Governance Board.

24. Disaster Recovery and Business Continuity

- The Platform maintains documented Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for core services (credentialing, verification, DIR access).
- Data is backed up according to a defined schedule, with backups encrypted and geographically or logically separated from primary production environments.
- Failover and continuity procedures are tested periodically; results are summarized for institutional partners on request.

- A full technical disaster recovery architecture is described in the companion Security & Compliance White Paper.

25. Accessibility

The Platform is designed to meet recognized digital accessibility standards (e.g., WCAG 2.1 AA or successor) to support equitable access for users with disabilities, including compatibility with screen readers and support for offline/low-connectivity credential verification in low-infrastructure settings.

26. Compliance Framework

The Platform's privacy and security program is designed with reference to recognized frameworks, including (as applicable per deployment):

- **HIPAA** (U.S. health data safeguards, where applicable).
- **GDPR** (EU/EEA data protection, including special-category health data provisions).
- **ISO/IEC 27001** (information security management).
- **NIST Cybersecurity Framework / NIST 800-53** (security controls alignment).
- **WHO Digital Documentation of COVID-19 Certificates (DDCC)** and related interoperability standards, where relevant to cross-border credential recognition.
- Applicable national health-data and digital-identity statutes in each deployment jurisdiction.

Detailed control mappings, audit certifications, and architecture alignment are provided in the companion **SYCVAC Security & Compliance White Paper**, available to Ministries of Health, institutional partners, and auditors under appropriate confidentiality arrangements.

27. Changes to This Policy

We may update this Policy to reflect changes in our practices, the Platform's capabilities, or applicable law. Material changes will be communicated to Users and institutional partners through the Service, direct notice to Governance Boards, or other reasonable means, with the "Last Updated" date revised accordingly. Where a national deployment operates under a separate

Data Sharing Agreement, material changes affecting that Agreement will be coordinated with the relevant Ministry of Health.

28. Contact Information

SYCVAC Privacy Office Email: privacy@sycvac.com

For Institutional and Government Partners Governance and Compliance Inquiries: contact@sycvac.com

Security Incident Reporting: infosupport@sycvac.com