Illinois BIPA
Evidence Readiness Checklist

Illinois Biometric Information Privacy Act

Issued by	Clavira Standards Program
Document Type	Evidence Readiness Checklist
Version	1.0 · March 2026
Applies	Biometric Evidence Standard (BES-1)
Document ID	BES-IL-CL-1.0

This checklist applies the Clavira Biometric Evidence Standard (BES-1) to the evidentiary expectations of the Illinois Biometric Information Privacy Act (BIPA), 740 ILCS 14, as amended through SB 2979 (effective August 2, 2024). It is designed to help legal, compliance, and technical teams assess operational evidence readiness. Each section maps to statutory requirements and to the evidence architecture controls described in BES-1 and the companion Illinois BIPA Evidence Interpretation Guide (2026).

This checklist is provided for informational purposes only and does not constitute legal advice. Organizations should consult qualified legal counsel when assessing BIPA compliance obligations. This checklist does not determine whether any specific biometric program is lawful, does not replace legal counsel, and does not convert evidentiary recommendations into statutory requirements.

1. Scope & Applicability

The organization is a "private entity" under BIPA, excluding state and local governments, courts, and government contractors acting on behalf of government.

The organization collects, stores, or uses at least one covered biometric identifier under BIPA, including fingerprint, scan of hand or face geometry, retina or iris scan, or voiceprint.

Any claim of GLBA or HIPAA exemption has been assessed and validated with counsel. GLBA-based exemptions are fact-specific and may not extend to third-party vendors depending on entity, activity, and role in processing.

Biometric data flows have been mapped — identifying which systems collect, store, process, or transmit biometric identifiers and which vendors are involved at each stage.

2. Written Retention & Destruction Policy

BIPA Section 15(a) requires a publicly available written retention schedule and destruction guidelines. Under *Mora v. J&M Plating, Inc.,* 2022 IL App (2d) 210692*,* this policy must exist upon possession of biometric data later adoption may not cure earlier noncompliance.

A written biometric data retention and destruction policy exists and was in place before or at the time biometric collection began — not adopted retroactively.

The policy is publicly available, whether posted on the organization's website, included in an employee handbook, or embedded in a consumer-facing privacy notice.

The policy defines a retention schedule expressed as a concrete time window tied to a defined trigger and identifies the organization's destruction approach in a manner that is operationally reviewable and consistent with the policy.

Data is destroyed upon whichever occurs first: satisfaction of the initial purpose for collection, or within three years of the individual's last interaction with the entity. Legal holds or court orders extending the destruction timeline are documented as exceptions.

Evidence Readiness: Records exist showing the policy's adoption date, version history, and public availability — demonstrating the policy existed upon possession, not afterwards. The adoption date is verifiable independently of the policy document itself.

3. Notice & Written Consent

BIPA Section 15(b) imposes a strict sequence: notice → written release → collection. The sequence is not satisfied by policy existence alone — it must be demonstrable for each individual.

Before collecting biometric data, written notice is provided to each individual stating: that biometric data is being collected or stored, the specific purpose of collection and use, and the length of time the data will be stored and used.

A biometric-specific written release is obtained from each individual before collection occurs. The written release is presented in a manner that is clear, attributable, and separable from broader privacy or employment materials. It is informed, signed, and timestamped. Electronic signatures satisfy the written release requirement under SB 2979.

The notice and consent sequence is documented per individual — not as a general policy assertion. The version of the notice presented to each individual at the time of consent is preserved.

Records of consent, including timing relative to collection, are securely stored and retained in accordance with the retention policy. Where notice and written release are captured through different systems or workflows, the organization can still reconstruct the sequence reliably for each individual.

Evidence Readiness: For each individual, a time-ordered record exists showing notice was presented before consent was captured, and consent was captured before the first biometric collection event — consistent with the Contemporaneous Attestation Principle (BES-1, Principle 2). This sequencing is demonstrable by timestamp, not by policy assertion alone.

4. Prohibition on Sale & Profit

Biometric data is not sold, leased, traded, or otherwise profited from. No revenue is generated from selling biometric templates or datasets, or from licensing access to biometric data for analytics or other third-party use.

Vendor contracts explicitly prohibit vendors from selling, leasing, trading, or profiting from biometric data processed on the organization's behalf. The organization has evidence of vendor oversight sufficient to support those restrictions in adversarial review, rather than relying solely on contract language.

5. Disclosure & Redisclosure Restrictions

Biometric data is not disclosed unless one of the following conditions is satisfied: the individual has given consent to the specific disclosure; disclosure is necessary to complete a financial transaction requested by the individual; disclosure is required by state or federal law or municipal ordinance; or disclosure is required pursuant to a valid warrant or subpoena.

Requests from law-enforcement or governmental entities are evaluated against the specific disclosure bases permitted by BIPA Section 15(d). The organization does not assume that informal, discretionary, or purely administrative requests satisfy the statute without counsel review.

Vendor contracts include redisclosure limits and prohibit vendors from disclosing biometric data beyond the authorized processing relationship without separate legal or contractual authorization.

Evidence Readiness: An audit trail of all biometric disclosures — or documented confirmation that no disclosures occurred — is maintained and reconcilable against consent records.

6. Safeguards & Security

Biometric data is protected with at least the same level of care as other sensitive information in the organization's industry, consistent with BIPA Section 15(e)'s reasonable standard of care.

Technical safeguards appropriate to the organization's risk profile are in place, including storage and transmission protection, restricted system access, and strong authentication for privileged access where appropriate.

Administrative safeguards are in place, including incident-response procedures covering biometric-data events and regular training for personnel who handle biometric systems or related records.

Access, modification, and activity logs are maintained for biometric-data systems and can be exported for review.

Evidence Readiness: Access and modification logs for biometric systems are structured and retained in a form that can be exported and reconciled against attested event records (BES-1 SIEM Reconciliation).

7. Vendor & Third-Party Management

GLBA-based exemptions are fact-specific and may not shield third-party vendors from independent BIPA obligations. Evidence of vendor oversight — not just contractual terms — is expected in adversarial review.

All vendors that collect, store, or process biometric data on the organization's behalf are contractually bound to comply with BIPA's notice, consent, retention, and destruction requirements; not sell, lease, trade, or profit from biometric data; and limit redisclosure to uses permitted by contract.

Vendor contracts include data processing terms covering purpose limitation, confidentiality, and security; audit rights; breach notification obligations; and explicit deletion obligations covering both source records and derived work product.

Written confirmation of deletion has been obtained or is contractually required from vendors upon termination of biometric data processing, covering source records and, where applicable, relevant derived work product subject to contractual or legal deletion obligations.

Evidence Readiness: Vendor-side compliance events — consent, deletion, and disclosure — are reconciled against institutional records rather than assumed from contractual terms alone (BES-1 Principle 5, SIEM Reconciliation). Incident-notification records, audit reports, and deletion confirmations are retained as evidence artifacts.

8. Internal Processes & Documentation

A documented process exists for collecting and storing consent records per individual, enforcing the retention and destruction policy, and handling individual requests including access, deletion, and withdrawal of consent.

Biometric data flows and systems are fully mapped.

Regular internal audits or reviews are conducted to verify ongoing operational implementation — not just policy existence. Where gaps are identified, a documented corrective-action path exists covering triage, owner assignment, remediation, retest, and closure.

9. Training & Awareness

Employees and contractors who interact with biometric systems receive training on BIPA requirements including notice, consent, retention, and the prohibition on sale or profit; how to handle consent and respond to individual requests; and security and incident reporting procedures.

Training materials and completion records are maintained. Training updates are versioned when legal requirements, consent workflows, retention rules, or vendor-handling obligations materially change.

10. Risk & Litigation Preparedness

BIPA provides a private right of action with statutory damages of $1,000 per negligent violation and $5,000 per reckless or intentional violation, plus attorneys' fees, costs, and injunctive relief.

Under *Rosenbach* v. *Six Flags Entm't Corp*., 2019 IL 123186, failure to satisfy procedural prerequisites is a cognizable injury independent of downstream harm — no actual damage to the individual need be shown to establish standing.

A five-year statute of limitations applies to all BIPA claims under *Tims* v. *Black Horse Carrier*s, 2023 IL 127801. The organization has assessed whether historic collection, disclosure, retention, or deletion practices could create exposure that predates the current governance program.

Legal counsel has reviewed key documents — including the retention policy, consent forms, and vendor contracts — for BIPA alignment.

11. Evidence System Verification

This section maps operational evidence posture to the BES-1 integrity primitives. Policy existence and operational implementation are distinct. This section addresses the latter.

Event Attestation

Biometric governance events — notice, consent, enrollment, operational use, and deletion — are recorded as timestamped attestations at the moment they occur, not reconstructed after the fact.

Each attestation captures: subject identifier (non-biometric), event type, exact timestamp, consent scope reference, declared processing purpose, retention period expressed as a concrete window, and the policy and notice version in effect at the time of the event.

Notice version identifiers are preserved, enabling reconstruction of exactly what was presented to each individual at the time of consent.

Contemporaneous Attestation Principle

For each individual, evidence exists that notice preceded consent and consent preceded the first collection event — demonstrable by timestamp, not by policy assertion alone.

Post-hoc reconstruction of consent records, retention policies, or deletion evidence is identified and treated as lower assurance than point-of-capture attestation.

Anchor to Ledger (where implemented)

Cryptographic hashes of attested events are anchored to an append-only ledger to strengthen tamper-evidence.

Ledger trust assumptions — public versus private ledger, anchoring cadence, and key management — are documented. Authentication, key-management assumptions, and evidentiary-foundation requirements for potential legal proceedings are understood and planned for.

Proof Bundle

The organization can generate a complete, exportable evidence record for any individual covering: notice artifact, consent receipt linked to notice version, enrollment record, operational use events linked to declared purpose and consent scope, retention schedule version and clock in effect at collection, and deletion certificate including written vendor confirmation where applicable.

Proof Bundles are available in human-readable PDF and structured CSV/JSON. They do not contain biometric identifiers, templates, or raw scan data. Export access is restricted to authorized roles and all export actions are logged. Export scopes are limited to the records necessary for the review, response, or inquiry at issue.

SIEM Reconciliation

Biometric events recorded in operational logs can be cross-referenced against attested event records to identify discrepancies.

Alerts are configured for: biometric events without a prior consent attestation, retention schedule violations, deletion or destruction failures, and vendor disclosure events not reflected in governed records.

Vendor deletion confirmations — covering source records and derived work product — are tracked and reconcilable.

The evidence layer has been tested within the last quarter: a sample Proof Bundle has been exported and reviewed for completeness and accuracy. Where discrepancies are identified, a documented corrective-action path exists covering triage, owner assignment, remediation, retest, and closure.