Illinois BIPA
Evidence Interpretation Guide

Statutory Requirements, Consent Protocols & Evidentiary Standards

Issued by	Clavira Standards Program
Document Type	Interpretation Guide
Version	1.0 · 2026
Applies	Biometric Evidence Standard (BES-1)
Document ID	BES-IL-IG-1.0

This guide interprets how the Illinois Biometric Information Privacy Act (BIPA), 740 ILCS 14, as amended through SB 2979 (effective August 2, 2024), applies evidence expectations to biometric governance programs. It applies the Clavira Biometric Evidence Standard (BES-1) to the evidentiary obligations arising under Illinois law. It is intended to support legal, compliance, and technical teams responsible for biometric system governance and compliance documentation.

This guide reflects the law as of early 2026. All citations refer to Illinois statutory text, court decisions, or trusted legal commentary. This guide is provided for informational purposes only and does not constitute legal advice. This guide does not determine whether any specific biometric program is lawful, does not replace legal counsel, and does not convert evidentiary recommendations into statutory requirements. Organizations should consult qualified legal counsel when assessing BIPA compliance obligations.

Section 1: BIPA Scope & Coverage

BIPA applies to private entities that collect, use, store, or disclose biometric identifiers or biometric information. "Private entity" is defined broadly and excludes only state and local governments, courts, judges, and government contractors working on behalf of government.

Covered biometric identifiers include: retina or iris scan, fingerprint, voiceprint, and scan of hand or face geometry.

Excluded: writing samples, photographs, demographic data, and health care information protected under HIPAA.

Extraterritorial application. Courts assessing BIPA's application to out-of-state entities look to whether the relevant conduct and injury occurred primarily and substantially in Illinois.

Key exemptions. Financial institutions subject to GLBA benefit from a statutory exemption, but courts have interpreted its scope based on whether the entity and activity fall within GLBA's Title V coverage. This exemption is fact-specific and may not extend to third-party vendors depending on entity, activity, and role in processing. HIPAA-covered health information and government contractors working on government projects are also exempt.

Compliance is assessed not only by the existence of written policies or notices, but by whether statutory requirements were actually satisfied at the time biometric data was collected, used, retained, or disclosed. Illinois decisions and the structure of BIPA's operative provisions make timing and execution materially important to the compliance analysis. In practice, organizations may be required to demonstrate when notice was provided, when written release was obtained, what purpose was disclosed, and whether retention and destruction obligations were executed as required.

Section 2: Written Retention & Destruction Policy

Statutory requirement. BIPA Section 15(a) requires a written policy, made publicly available, that establishes a retention schedule for biometric data and guidelines for permanent destruction. Destruction must occur when the initial purpose is satisfied, or within three years of the individual's last interaction — whichever comes first.

Timing is central to the violation analysis. In *Mora v. J&M Plating, Inc.,* 2022 IL App (2d) 210692, the appellate court interpreted Section 15(a)'s duty as triggered by possession and held that a retention and destruction schedule must exist before or at the time biometric collection begins. Later adoption may not cure earlier noncompliance. Mental state may still affect remedies — statutory damages tiers under Section 20 distinguish negligent from reckless or intentional violations — but timing of policy adoption is a threshold compliance element independent of intent.

Required policy design elements. As an operational matter, a defensible policy typically identifies the trigger for retention, the applicable retention window, the method of permanent destruction, and any documented exception process for legal holds or court orders. These elements strengthen demonstrability, but they should be understood as implementation guidance rather than additional statutory text.

Evidentiary significance. The policy's adoption date is itself an evidence artifact. A policy that cannot establish when it came into effect — relative to when biometric collection began — creates evidentiary weakness and may be challenged as insufficient to demonstrate compliance with the sequencing requirement. Under the Contemporaneous Attestation Principle (BES-1, Principle 2), policy version history, effective date records, and publication timestamps are first-class evidence artifacts.

Section 3: Notice & Written Consent

Statutory requirement. BIPA Section 15(b) requires a strict sequence before collection: written notice stating biometric data is being collected, the purpose, and the duration — followed by a written release (informed written consent).

A defensible BIPA posture generally requires a biometric-specific written release that is not obscured within broader privacy materials or general employment documentation. SB 2979 (2024 amendment) clarifies that electronic signatures satisfy the written release requirement.

The sequence is strict: notice → consent → collection. Documentation of timing is essential. This is not a policy commitment — it is a statutory sequencing obligation. Retroactive consent documentation is generally lower assurance and may be challenged as insufficient to demonstrate statutory sequencing; defensible posture requires a timestamped consent record that predates the first collection event.

Translations are recommended where the population includes non-English speakers.

Evidentiary significance. For each individual, a time-ordered record should exist 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. A notice artifact that cannot establish its presentation timestamp relative to the consent event and the first collection event creates an evidentiary gap that logs and dashboards alone are unlikely to close.

Section 4: Prohibition on Sale & Profit

Statutory requirement. Section 15(c) prohibits entities from selling, leasing, trading, or otherwise profiting from biometric data.

Examples of prohibited conduct include selling biometric templates or datasets, and licensing access to biometric data for analytics or other third-party use.

Paying a vendor for biometric processing may be permissible, but the organization should ensure by contract and oversight that the vendor does not use biometric data for any purpose beyond the authorized processing relationship. In adversarial review, that restriction is more defensible when it is supported by oversight evidence rather than assumed from contract language alone.

Section 5: Disclosure Restrictions

Statutory requirement. Section 15(d) prohibits disclosure unless one of the following conditions is met: the individual consents to the disclosure; disclosure is needed 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.

Operational implication. Requests from law-enforcement or governmental entities should be evaluated against the specific disclosure bases permitted by Section 15(d). Organizations should avoid assuming that informal, discretionary, or purely administrative requests satisfy the statute without counsel review.

Vendor redisclosure. Redisclosure by vendors should be contractually restricted and operationally monitored. Where an organization relies on a vendor to process biometric data, redisclosure boundaries are more defensible when they are documented in both contract terms and oversight records.

Evidentiary significance. The basis relied upon for each disclosure event should be documented. An audit trail of all biometric disclosures — or documented confirmation that no disclosures occurred — should be maintained and reconcilable against consent records.

Section 6: Safeguards & Security

Statutory requirement. Section 15(e) requires a private entity in possession of biometric identifiers or biometric information to store, transmit, and protect that data using the reasonable standard of care within its industry and in a manner that is the same as or more protective than the manner in which it stores, transmits, and protects other confidential and sensitive information.

Recommended control posture. A defensible security posture typically includes controls such as encryption at rest and in transit where appropriate, restricted administrative access, strong authentication for privileged access, structured access logging, and incident-response procedures capable of addressing unauthorized access, disclosure, or retention failures. These are recommended control measures that can help demonstrate a reasonable standard of care; they are not additional statutory elements of BIPA itself.

Evidentiary significance. Access and modification logs for biometric systems should be structured and retained in a form that can be exported and reconciled against attested event records, consistent with BES-1 SIEM Reconciliation. Security controls are easier to demonstrate when their implementation, scope, and review history are documented at the time of deployment rather than reconstructed at the time of review.

Section 7: Private Right of Action & Damages

Statutory right. Any "aggrieved" person may bring a claim without proving actual harm beyond a violation of statutory rights. In *Rosenbach* v. *Six Flags Entm't Corp*., 2019 IL 123186, the Illinois Supreme Court held that failure to satisfy procedural prerequisites is a cognizable injury independent of downstream harm — no showing of concrete damage to the individual is required to establish standing.

Statutory damages. Section 20 provides:

- $1,000 per negligent violation
- $5,000 per reckless or intentional violation
- Plus attorneys' fees, costs, and injunctive relief

SB 2979 (2024 amendment) limits recovery in certain circumstances: one recovery per person for multiple collections by the same method without consent under Section 15(b), and one recovery per person for repeated disclosures to the same recipient without consent under Section 15(d). Whether the SB 2979 damages limitation applies retroactively remains a live issue and should be evaluated with counsel. A conservative posture is to avoid assuming the limitation resolves exposure for pre-amendment conduct absent case-specific legal analysis.

Statute of limitations. A five-year statute of limitations applies to all BIPA violations under *Tims* v. *Black Horse Carriers*, 2023 IL 127801. Exposure can reach back five years from the date of filing — meaning organizations face potential liability for collection practices predating current governance programs.

Per-event accrual. In *Cothron* v. *White Castle System, Inc*., 2023 IL 128004, the Illinois Supreme Court held that a separate claim accrues each time biometric data is scanned or transmitted without a prior, separate informed consent. This accrual theory is partially mitigated by the SB 2979 damages cap, but the underlying accrual principle remains relevant for understanding exposure scope.

Section 8: Interplay with Other Laws

GLBA. Financial institutions subject to GLBA benefit from a statutory exemption, but courts have interpreted its scope based on whether the entity and activity fall within GLBA's Title V coverage. Exemption applicability to vendors is fact-dependent and should be validated with counsel.

Other state laws. BIPA does not preempt other state privacy laws. Organizations operating in multiple states must assess compliance with all applicable biometric statutes.

Labor law. *McDonald* v. *Symphony Bronzeville*, 2022 IL 126511 confirms BIPA is not preempted by Illinois workers' compensation law.

Arbitration. Arbitration provisions and class-action waivers may affect BIPA litigation exposure, but enforceability depends on the specific agreement language, formation record, and applicable judicial treatment. Organizations relying on arbitration provisions to manage BIPA exposure should validate enforceability with counsel.

Litigation exception. BIPA does not block discovery or admissibility in court proceedings (Section 25(a)).

Section 9: Why BIPA Is an Evidence Problem

BIPA's structure is sequencing-dependent. Notice must precede consent. Consent must precede collection. A retention schedule must exist upon possession of biometric data. Deletion must occur when purpose is satisfied or within a defined window. These are not aspirational standards — they are statutory prerequisites whose timing courts have treated as dispositive to the violation analysis.

The private right of action, with no harm requirement and a five-year statute of limitations, means that evidentiary gaps are not theoretical risks. They are the mechanism through which liability is established. An organization that cannot demonstrate the required sequence — notice, then consent, then collection — faces the same exposure as one that never obtained consent at all.

Operational logs — SIEM outputs, vendor dashboards, IAM records, timekeeping system exports — are frequently insufficient to satisfy this burden on their own. They record that events occurred. They do not establish that events occurred in the required sequence, under the required consent scope, or within the required retention timeframes. Generic security logs showing proper data handling have been found insufficient when policies did not exist at the time of collection. Vendor dashboards showing current system state do not establish what consent was in place at the moment of each scan.

The gap between what operational logs produce and what BIPA litigation or regulatory review demands is not a technology failure. It is an evidence architecture gap. Operational logs document activity; Event Attestation, Proof Bundles, and SIEM Reconciliation provide the structured evidence needed to demonstrate sequence, scope, and lifecycle execution in a reviewable form.

The Contemporaneous Attestation Principle (BES-1, Principle 2) holds that records generated before or at the moment of the governed event carry materially stronger evidentiary weight than records reconstructed after the fact. BIPA's sequencing obligations — notice before consent, consent before collection, retention schedule upon possession — are each enforcement points where contemporaneous documentation is operationally decisive.

An evidence architecture aligned with BES-1 addresses this gap by producing, at minimum:

- **Notice artifacts** demonstrating the version of notice presented and the timestamp of presentation, prior to each consent event.
- **Consent receipts** linking timestamped written releases to the notice version and declared processing purpose, prior to the first collection event.
- **Retention schedule documentation** demonstrating the policy was in effect upon possession — not adopted retroactively.
- **Deletion certificates** recording the destruction event and the trigger that initiated it, including written vendor confirmation where applicable.
- **Disclosure logs** reconcilable against consent scope and vendor contracts.

- **SIEM reconciliation records** cross-referencing operational logs against attested events to surface gaps, drift, or unauthorized use.

These are not aspirational controls. They are the artifacts that BIPA litigation discovery and regulatory inquiry would request in order to reconstruct whether statutory obligations were met.

Section 10: Implementing an Evidence Layer for BIPA Compliance

BIPA's requirements — particularly those governing notice, written consent, purpose limitation, retention, and destruction — create an implicit expectation of provable execution not just documented intent. In audits, regulatory inquiries, or litigation, organizations may be asked to produce evidence showing how these obligations were satisfied in practice.

- A defensible biometric compliance posture under BIPA typically requires an evidence layer that can:
- Record biometric-related events with clear timestamps and context.
- Bind each event to the applicable consent scope, declared purpose, and policy version in effect at the time.
- Demonstrate adherence to retention limits and document destruction actions tied to the specific trigger that initiated them.
- Produce exportable records suitable for internal review, litigation discovery, or regulatory response.

Clavira is a reference implementation of this integrity-layer model: a metadata-only sidecar system designed to work with existing biometric vendors and systems of record.

Clavira does not ensure compliance or replace legal judgment. It can help organizations demonstrate how their biometric programs operated when those programs are reviewed, challenged, or questioned under BIPA.

Counsel Verification Queue

The following interpretive questions involve statutory language or evolving case law that requires primary-source verification by qualified legal counsel.

SB 2979 retroactivity. Courts are split on whether the damages cap under SB 2979 applies to claims accrued before the amendment's effective date. Organizations should not assume the cap applies to pre-amendment conduct without counsel verification.

GLBA exemption scope. The GLBA exemption under BIPA Section 25(c) is fact-specific. Whether it applies to a given entity and activity — and whether it extends to third-party vendors — should be validated with counsel, particularly for FinTech, payment processors, and non-bank financial entities whose GLBA status may be contested.

Extraterritorial application. Where biometric collection involves out-of-state processing or out-of-state entities, whether the relevant conduct and injury occurred primarily and substantially in Illinois requires a fact-specific analysis.

Arbitration and class action waivers. Enforceability varies by court and by the specific language of the agreement. Organizations relying on arbitration provisions to manage BIPA exposure should verify enforceability with counsel.