Colorado HB 24-1130 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-CO-IG-1.0

This guide interprets how Colorado House Bill 24-1130 — codified at Colo. Rev. Stat. § 6-1-1314, effective July 1, 2025 — applies evidence expectations to biometric governance programs. It applies the Clavira Biometric Evidence Standard (BES-1) to the evidentiary obligations arising under Colorado law. It is intended to support legal, compliance, and technical teams responsible for biometric system governance and compliance documentation.

This guide is provided for informational purposes only and does not constitute legal advice. Organizations should consult qualified legal counsel when assessing Colorado biometric privacy obligations. 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.

Section 1: Scope & Coverage

Colorado HB 24-1130 amends the Colorado Privacy Act (CPA) by adding Part 13, codified at C.R.S. §§ 6-1-1301 through 6-1-1314. The biometric-specific obligations are contained in § 6-1-1314, effective July 1, 2025.

Applicability. Colorado's biometric provisions create a biometric-specific applicability pathway beginning July 1, 2025. Where a controller controls or processes biometric identifiers or biometric data, Part 13 may apply even if the controller does not otherwise satisfy the general CPA volume thresholds. Where applicability arises through the biometric-based gateway rather than the general CPA thresholds, organizations should confirm with counsel the practical extent to which related CPA duties apply to the biometric program specifically versus the broader privacy program.

Key definitions. Colorado distinguishes between two related but distinct categories:

A *biometric identifier* is a technologically processed, measured, or analyzed biological, physical, or behavioral characteristic usable for uniquely identifying an individual — including fingerprints, voiceprints, retina or iris scans, and facial geometry templates. Photographs, audio recordings, and video recordings are excluded unless processed for identification purposes.

Biometric data is one or more biometric identifiers used or intended to be used for identification purposes. This distinction matters operationally: biometric identifiers are the raw data elements; biometric data is the category that triggers sensitive data classification and opt-in consent requirements under the CPA. Most biometric deployments in practice involve identification and therefore constitute biometric data.

Consumer vs employee scope. Colorado's statutory definition of "consumer" excludes individuals acting in an employment context and job applicants. C.R.S. § 6-1-1314 separately addresses employer and employee biometric obligations within § 6-1-1314(6). Organizations must conduct a separate analysis for consumer-context and employee-context biometric processing, as the applicable obligations — particularly around consent — differ materially.

Exemptions. GLBA-regulated entities and HIPAA-covered health information carry forward existing CPA exemptions. These exemptions are fact-specific. GLBA-based exemptions may not extend to third-party vendors depending on entity, activity, and role in processing. Applicability should be validated with counsel.

Section 2: Written Biometric Policy

Statutory requirement. C.R.S. § 6-1-1314(2) places the written biometric policy obligation on controllers. The policy must exist and be effective before biometric collection begins; it should not be adopted retroactively after collection has already started.

Required policy elements. The statute requires a written biometric policy that includes a retention schedule, destruction guidelines, and a biometric-specific security-breach response protocol tied to C.R.S. § 6-1-716. The policy must also address annual review of whether continued retention remains necessary, adequate, and relevant for the original purpose.

Annual review as deletion trigger. The annual review is not merely an administrative exercise. If the review determines that continued retention is no longer necessary, adequate, or relevant, deletion must occur within 45 days, extendable to 90 days with documented justification.

Public-availability distinction. Whether the policy must be public depends on the population served. Consumer-facing biometric programs require public availability. Employee-only programs may remain internal.

Processor distinction. Processors have separate incident-protocol duties under § 6-1-1314(3) and applicable contracts. The written biometric policy obligation is a controller duty.

Evidentiary significance. Because the policy must predate collection, its adoption date is itself an evidence artifact. A policy that cannot establish when it came into effect relative to the start of biometric collection cannot demonstrate sequencing compliance. Policy version history, effective-date records, and publication timestamps are first-class evidence artifacts under BES-1.

Section 3: Pre-Collection Notice

C.R.S. § 6-1-1314(4)(a)(I) requires controllers to satisfy § 6-1-1308 privacy notice duties and to provide a biometric identifier notice before collecting or processing a consumer biometric identifier.

The biometric identifier notice addresses collection, retention, and processor-sharing specifics for consumer biometric identifiers. It is distinct from the broader CPA privacy notice, which governs third-party disclosure and general transparency duties more broadly. These are related but separate disclosure obligations and should not be treated as interchangeable.

Scope of this notice. This biometric identifier notice requirement applies to consumer biometric identifiers. Employee notice obligations arise separately under § 6-1-1314(6) and are addressed in Section 5. The biometric identifier notice addresses processor sharing specifically — it is a distinct obligation from the general CPA privacy notice, which governs third-party disclosures more broadly. These are two separate disclosure obligations that should not be conflated in a single notice.

Notice version control. Notices must be tailored to each biometric use case. Versioned copies of notices used at the time of each collection event must be retained. This is not a general documentation best practice — it is an operational prerequisite for demonstrating that the required notice was in fact provided before collection began.

Evidentiary significance. The notice obligation is sequencing-dependent: notice must precede consent, and consent must precede collection. A notice artifact that cannot establish its presentation timestamp — relative to the consent event and the first collection event — cannot demonstrate compliance with the sequence. Under the Contemporaneous Attestation Principle (BES-1, Principle 2), notice artifacts must be generated at the moment of presentation, not reconstructed afterwards.

Section 4: Consent Management

Consumer consent. Biometric data — one or more biometric identifiers used for identification purposes — is classified as sensitive data under the CPA. Processing biometric data requires opt-in consent before collection or processing. Consent must be freely given, specific, informed, and unambiguous. Broad terms of use, passive actions, and dark patterns do not satisfy Colorado's consent definition. New consent is required for any material changes in purpose.

Consent sequencing. The sequence is strict: notice → consent → collection. This is not a policy commitment — it is a statutory sequencing obligation. The Contemporaneous Attestation Principle requires that a timestamped consent record exist before the first collection event, linked to the notice version presented. 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.

Employee and applicant consent. § 6-1-1314(6) governs employer use of employee biometric identifiers. Employers may make consent a condition of employment only for specific, enumerated purposes: secure access control, timekeeping, workplace safety or security, and public safety in emergencies.

Biometric data may not be retained for current employee location tracking or for tracking time spent using a hardware or software application — even where employment-conditioned consent is otherwise permissible. This prohibition is explicit in § 6-1-1314(6)(a)(I) and will be a focal point in regulatory review.

Consent captured during hiring or onboarding should not be assumed to satisfy the employee consent requirement where the implementing rules require consent in a different form, sequence, or employment-context presentation. Organizations should validate the required form and timing under 4 CCR 904-3 and preserve the consent timestamp relative to the first collection event.

All biometric uses outside the enumerated employment purposes require voluntary consent. There may be no retaliation for an employee's refusal to consent to non-enumerated uses.

Evidentiary significance. For each individual — consumer or employee — a timestamped consent record must exist demonstrating opt-in consent was captured before the first collection event. The consent record must be linked to the notice version presented and to the declared processing purpose. The prohibition on current employee location tracking and time-on-application tracking should be demonstrable through system design, logging, and review controls — not by policy assertion alone. In practice, the evidence architecture should be configured to make such uses detectable if they occur, consistent with BES-1 SIEM Reconciliation.

Section 5: Retention & Deletion

Deletion triggers. C.R.S. § 6-1-1314(2)(a)(III) establishes deletion on or before the earliest of: the initial purpose being satisfied; 24 months after the consumer's last interaction with the controller; or within 45 days of an annual review determination that storage is no longer necessary, adequate, or relevant (extendable to 90 days with documented justification).

"Last interaction" ambiguity. The statute uses "last interacted with the controller" as a deletion trigger but does not define the term. Organizations should document their interpretation of what constitutes a qualifying interaction — particularly in mixed consumer and employee programs — and apply it consistently. This is a live interpretive question that requires counsel verification.

Annual review as deletion trigger. The annual review is not a general governance exercise — it is a statutory mechanism that can initiate a binding deletion obligation. When a review determines that continued retention is no longer necessary, the 45-day clock begins. The review determination date and the deletion completion date are both evidence artifacts that must be preserved.

Derived work product. Where biometric processing produces derived records, models, or algorithms connected to the biometric workflow, organizations should evaluate with counsel whether deletion obligations, contractual controls, and remediation expectations extend to that work product. Analogous federal enforcement posture makes this a material risk consideration even where the state statute does not spell out every derived-work-product scenario. Where vendors hold derived work product, written confirmation of deletion covering both source records and relevant derived work product should be obtained where legally and operationally appropriate.

Evidentiary significance. Deletion is not complete without a verifiable deletion certificate — a timestamped record of the destruction event tied to the trigger that initiated it. Retention clock configurations must be auditable against the documented retention schedule. Annual review determinations must be recorded at the time the review occurs, not reconstructed at the time of a regulatory inquiry.

Section 6: Disclosure & Sale Restrictions

Statutory requirement. Biometric identifiers may not be sold, leased, or traded. Disclosure or redissemination is prohibited unless one of the following statutory bases applies: the individual has consented to the specific disclosure; disclosure is necessary to complete a financial transaction requested by the individual; sharing with a processor is necessary for the original consented purpose; or disclosure is required by law.

Operational implication. Organizations should document the disclosure basis relied upon for each disclosure or processor-sharing event and preserve the governing consent scope and processor relationship supporting that disclosure.

Evidentiary significance. An audit trail of all biometric disclosures — or documented confirmation that no disclosures occurred — should be maintained and be reconcilable against consent records and processor contracts.

Section 7: Security Safeguards

Statutory requirement. Controllers must implement reasonable administrative, technical, and physical safeguards appropriate to the sensitivity of biometric data, consistent with the standard of care within the controller's industry and with C.R.S. § 6-1-1305(4) and § 6-1-1308(5).

Recommended control posture. A defensible security posture typically includes encryption at rest and in transit where appropriate, role-based access restriction, strong authentication for privileged access, structured logging, incident-response procedures, and evidence-preservation controls sufficient to demonstrate how the biometric program operated.

Regulatory-change caution. Colorado Attorney General rulemaking under § 6-1-1314(7) is ongoing. Existing obligations should be treated as the current floor, and organizations should monitor promulgated rules rather than draft proposals when assessing binding requirements.

Section 8: Processor & Vendor Management

Processor contracts must address: deletion or return of biometric data at the end of services; audit rights; security obligations; and subprocessor controls, consistent with C.R.S. § 6-1-1305(5).

Processors must notify controllers of biometric security breaches in the most expedient time possible under § 6-1-716. Controllers must notify affected Colorado residents within 30 days of determining a breach occurred. If a breach affects 500 or more Colorado residents, the Colorado Attorney General must be notified within 30 days.

Resident breach notice must include at minimum the elements required by C.R.S. § 6-1-716(2)(a.2). Controllers should document whether a given incident involves biometric identifiers, biometric data used for identification, or other personal data categories — as the breach statute's definition of "biometric data" may be narrower than the definition in § 6-1-1314. Counsel should confirm the applicable definition for breach notification purposes.

Vendor compliance should be periodically reviewed, not assumed from contractual terms alone. Executed agreements, audit reports, incident-notification records, and deletion confirmations should be retained as evidence artifacts supporting BES-1 Principle 5 — Vendor Reconciliation.

Section 9: Consumer Biometric Access Rights

For qualifying entities meeting the thresholds in § 6-1-1314(5), responses to biometric access requests must include: the category and description of biometric data held; the source of the biometric data; the purpose for collection and processing; and the identity of third parties to whom biometric data has been disclosed and the purposes of those disclosures. These rights are threshold-dependent and should not be assumed to apply uniformly to every controller processing biometric data.

Access requests are processed using CPA response timing: within 45 days, extendable by an additional 45 days with notice. A documented appeals process must exist for denied requests. Records of complied-with requests must be retained for at least 24 months.

Section 10: Enforcement

Enforcement under Part 13 is exclusively by the Colorado Attorney General and district attorneys. There is no private right of action under § 6-1-1314. Violations are treated as deceptive trade practices under the Colorado Consumer Protection Act framework.

The general CPA cure provision has sunset. A limited notice-to-cure mechanism exists for specified minors-related provisions through December 31, 2026, but biometric requirements under § 6-1-1314 are not included in that enumerated cure structure as currently enacted. Civil penalties range from $2,000 to $20,000 per violation, capped at $500,000 per series of violations.

The absence of a private right of action distinguishes Colorado from Illinois BIPA, which provides a direct private right of action with per-violation statutory damages. Colorado's enforcement model concentrates risk in regulatory investigation and AG action rather than class litigation — but AG enforcement can proceed without notice or opportunity to cure.

Section 11: Why HB 24-1130 Is an Evidence Problem

Colorado's biometric framework is structured around time-bound sequencing obligations. Notice before collection. Consent before use. Policy before possession. Annual review as deletion trigger. Breach notification within 30 days. Access request response within 45 days.

Each of these obligations has a chronological dimension. The compliance question is not only whether an organization has the right policies — it is whether those policies were operationally implemented in the right sequence, and whether that sequence can be demonstrated after the fact.

This is the evidence burden that HB 24-1130 creates.

Operational logs — SIEM outputs, vendor dashboards, IAM records — 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, and within the required timeframes. They are not structured for export as time-ordered, reviewable evidence.

The gap between what operational logs produce and what regulatory scrutiny 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. Colorado's sequencing obligations — notice before consent, policy before possession, annual review before deletion window expires — 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 collection event.
- **Consent receipts** linking timestamped opt-in consent to the notice version and declared processing purpose, prior to enrollment.
- **Retention schedule documentation** demonstrating the policy was in effect at the time of collection — not adopted retroactively.
- **Annual review records** documenting the determination date, the outcome, and the deletion initiation timestamp where applicable.
- **Deletion certificates** recording the destruction event, the trigger that initiated it, and written vendor confirmation where applicable.
- **Disclosure logs** reconcilable against consent scope and processor contracts.

These are not aspirational controls. They are the artifacts that a regulatory examination or AG investigation would request in order to reconstruct whether Colorado's sequencing obligations were met.

Implementing an Evidence Layer for HB 24-1130 Compliance

HB 24-1130's requirements — particularly those governing notice sequencing, consent timing, annual review obligations, and deletion triggers — create an implicit expectation of provable execution, not just documented intent.

A defensible biometric compliance posture under Colorado law typically requires an evidence layer that can:

- Record biometric-related events with clear timestamps and jurisdictional 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 deletion actions tied to the specific trigger that initiated them.
- Produce exportable records suitable for internal review, AG inquiry, or audit.

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. It produces the four BES-1 integrity primitives — Event Attestation, Anchor to Ledger, Proof Bundle, and SIEM Reconciliation — as operational outputs.

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 Colorado law.

Counsel Verification Queue

The following interpretive questions involve statutory language or cross-statute interaction that requires primary-source verification by qualified legal counsel.

"Last interacted" for deletion timing. The statute uses "last interacted with the controller" as a deletion trigger but does not define the term. The organization's interpretation — particularly in mixed consumer and employee programs — should be documented and validated with counsel.

Breach statute definition of "biometric data." C.R.S. § 6-1-716 uses a definition of "biometric data" within the breach notification statute that may be narrower than the definition in § 6-1-1314. Controllers should document whether a given incident involves biometric identifiers, biometric data used for identification, or other personal data categories for breach classification purposes. Counsel should confirm the applicable definition.

"Biometric-only" controller scope. For entities that fall within Part 13 applicability through the biometric-based gateway in § 6-1-1304(1)(a)(II) but do not otherwise meet general CPA thresholds, the practical extent to which § 6-1-1308 duties should be implemented as biometric-only versus broader CPA program duties should be confirmed with counsel.