Colorado HB 24-1130 Evidence Readiness Checklist

Colorado Biometric Privacy — Colo. Rev. Stat. § 6-1-1314

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

This checklist applies the Clavira Biometric Evidence Standard (BES-1) to the evidentiary expectations of Colorado House Bill 24-1130, codified at Colo. Rev. Stat. § 6-1-1314, effective July 1, 2025. It is designed to help legal, compliance, and technical teams assess operational evidence readiness — not merely policy existence. Each section maps to statutory requirements and to the evidence architecture controls described in BES-1 and the companion Colorado HB 24-1130 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 Colorado biometric privacy 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. Several provisions involve interpretive questions that require primary-source verification; these are flagged in the Counsel Verification Queue at the end of this document.

1. Applicability & Scope Assessment

Colorado's biometric provisions create a biometric-specific applicability pathway for controllers that control or process biometric identifiers or biometric data. Where the controller does not otherwise meet the general CPA volume thresholds, organizations should assess with counsel the practical extent to which Part 13 and cross-referenced CPA duties apply to the biometric program specifically rather than to the broader privacy program.

Colorado's statutory definition of "consumer" excludes individuals acting in an employment context and job applicants. C.R.S. § 6-1-1314 separately reintroduces employer and employee biometric obligations within its own provisions. The organization's analysis separately addresses: (a) consumer and household-context biometric processing, and (b) employee and prospective employee biometric processing under § 6-1-1314(6).

All biometric use cases have been identified and documented, including access control, timekeeping, safety systems, authentication, and identity verification.

All processors and vendors involved in biometric workflows have been identified, and the organization's role — controller, processor, or both — has been determined for each processing activity.

Evidence Readiness: A versioned biometric data flow map exists showing every system, vendor, data type, and processing role involved in biometric processing for Colorado residents. The map distinguishes consumer-context from employee-context processing and is updated when workflows change.

2. Written Biometric Policy

C.R.S. § 6-1-1314(2) places the written policy obligation on controllers. Processors have a separate incident protocol duty under § 6-1-1314(3). The policy must exist and be effective before biometric collection begins — not adopted retroactively.

Controllers must adopt a written biometric privacy policy covering biometric identifiers and biometric data. The policy should establish a retention schedule with concrete time windows tied to defined trigger events, include destruction guidelines specifying method and timing for permanently destroying biometric identifiers and associated records, and incorporate a biometric-specific breach-response protocol referencing C.R.S. § 6-1-716.

The policy documents an annual review requirement — assessing whether continued retention of biometric identifiers remains necessary, adequate, and relevant for the original purpose. The annual review is a deletion trigger, not a standalone administrative exercise: if the review determines retention is no longer necessary, deletion must occur within 45 days (extendable to 90 days with documented justification).

A determination has been made as to whether the policy must be publicly available or may remain internal. Consumer-facing biometric programs require public availability. Employee-only programs may remain internal.

Processors must maintain incident response protocols and controller notification procedures per C.R.S. § 6-1-1314(3) and applicable contracts.

Evidence Readiness: Records exist demonstrating the policy's adoption date and that it was effective before biometric collection began. Policy version history is maintained. The version of the policy in effect at the time of each collection event is preserved and auditable. Annual review determinations are documented at the time the review occurs — not reconstructed at the time of a regulatory inquiry.

3. Pre-Collection Notice

C.R.S. § 6-1-1314(4)(a)(I) requires controllers to satisfy § 6-1-1308 privacy notice duties and provide a biometric identifier notice before collecting or processing a consumer biometric identifier. The biometric identifier notice requirement addresses processor sharing specifically — it is distinct from general CPA third-party disclosure requirements, which are governed by the privacy notice.

Before collecting any consumer biometric identifier, clear and accessible notice is provided stating: that a biometric identifier is being collected; the specific purpose or purposes of collection; the length of time the biometric identifier will be retained; and whether the biometric identifier will be shared with a processor and the specific purpose for that sharing. This biometric identifier notice requirement applies to consumer biometric identifiers; employee notice obligations arise under § 6-1-1314(6) and are addressed separately in Section 4.

Separately, the organization's general CPA privacy notice covers required third-party sharing disclosures where applicable. These are two distinct disclosure obligations and are not treated as interchangeable. Notices are tailored to each biometric use case. Versioned copies of notices used at the time of each collection event are retained.

Evidence Readiness: For each individual, a notice artifact exists showing the version of the notice presented and the timestamp of presentation — prior to the first collection event. Notice version control enables reconstruction of exactly what each individual was told at the time of consent.

4. Consent Management

Under Colorado law, a biometric identifier is a data element (e.g., fingerprint, voiceprint, facial template). Biometric data is one or more biometric identifiers used for identification purposes. In practice, most biometric deployments involve identification and therefore require opt-in consent. Consent mechanics differ between consumer and employee populations.

Consumer Consent

Opt-in consent is obtained before collecting or processing biometric data. Consent is freely given, specific, informed, and unambiguous — broad terms of use, passive actions, and dark patterns do not satisfy Colorado's consent definition. Consent is recorded and timestamped before the first biometric use. New consent is obtained for any material changes in purpose.

Employee and Applicant Consent

Consent is obtained before collecting or processing employee biometric identifiers. Where consent is required as a condition of employment, this is permitted only for specific purposes: secure access, timekeeping, workplace safety or security, or public safety in emergencies.

Biometric data is not retained for current employee location tracking or for tracking time spent using a hardware or software application. C.R.S. § 6-1-1314(6)(a)(I) expressly prohibits these uses even where employment-conditioned consent is otherwise permissible.

Consent captured during hiring or onboarding is not relied upon as the sole basis for satisfying the employee consent requirement. Where implementing rules require consent in a different form, sequence, or employment-context presentation, the organization preserves evidence that consent was obtained in the required manner before the first biometric collection or processing event.

All other biometric uses require voluntary consent with no retaliation for refusal. Employee notices and consent records are retained and accessible.

Evidence Readiness: For each individual — consumer or employee — a timestamped consent record exists showing opt-in consent was captured before the first biometric collection or processing event. The consent record is linked to the notice version presented and to the declared processing purpose. Consent scope and purpose are documented in a way that demonstrates the use prohibition — including no current employee location tracking and no time-on-application tracking — was respected through system design, logging, and review controls, not merely by policy. This sequencing is demonstrable by timestamp — consistent with the Contemporaneous Attestation Principle (BES-1, Principle 2).

5. Retention & Deletion Controls

C.R.S. § 6-1-1314(2)(a)(III) imposes specific deletion triggers. The statute's use of "last interacted" as a trigger is not defined; the organization's interpretation is documented and applied consistently. See Counsel Verification Queue.

Biometric collection dates and last interaction dates are tracked per individual.

Biometric identifiers are deleted or destroyed 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).

The annual review process is conducted and documented on at least an annual basis. Review determinations — including the determination date and the outcome — are recorded at the time the review occurs.

Deletion actions are logged and verifiable. Litigation holds or statutory exceptions are documented with their basis and expected duration.

Evidence Readiness: Deletion events are recorded as verifiable deletion certificates at the time of destruction, covering source records and other deletion-scope records within the organization's control. Where vendors are involved, written confirmation of deletion is obtained covering source records and, where applicable, relevant derived work product subject to contractual or legal deletion obligations.

6. Sale, Disclosure & Sharing Restrictions

Biometric identifiers are not sold, leased, or traded.

Where biometric identifiers are acquired from another party, the organization has confirmed that all statutory conditions for that acquisition are satisfied and documented.

Disclosure or redissemination of biometric identifiers 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. The basis relied upon for each disclosure event is documented.

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

7. Security Safeguards

Reasonable administrative, technical, and physical safeguards appropriate to the sensitivity of biometric data are implemented, consistent with the statutory standard of care and with applicable Colorado privacy-program duties.

Biometric templates and related data are encrypted at rest and in transit where feasible. Role-based access controls and multi-factor authentication are enforced for biometric systems. Detailed access, modification, and activity logs for biometric systems are maintained and can be exported for review.

Colorado Attorney General rulemaking under § 6-1-1314(7) is monitored. The AG is authorized to impose security standards more stringent than current statutory requirements in consultation with state IT and regulatory agencies. Existing standards are treated as a floor, not a ceiling. Organizations should monitor promulgated rules, not draft proposals, when assessing binding obligations.

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).

8. Processor & Vendor Management

Vendor contracts are necessary but not sufficient. Evidence of ongoing oversight — reconcilable against institutional records — is expected in regulatory review. C.R.S. § 6-1-1305(5) specifies required processor contract elements.

Processor contracts address: deletion or return of biometric data at the end of services unless retention is required by law; audit rights including the option for independent annual audits; security obligations; and subprocessor controls.

Processor contracts prohibit sale, lease, trade, or unauthorized disclosure of biometric identifiers and limit processing to specified purposes only.

Processors are contractually required to notify controllers of biometric security breaches in the most expedient time possible under C.R.S. § 6-1-716.

Controllers notify affected Colorado residents within 30 days of determining a breach occurred. Resident breach notice includes at minimum the elements required by C.R.S. § 6-1-716(2)(a.2). A copy of the notice template used and evidence of the send date are retained. If a breach affects 500 or more Colorado residents, the Colorado Attorney General is notified within 30 days.

Written confirmation of deletion is obtained from processors covering both source records and derived work product upon termination of biometric data processing.

Vendor compliance is periodically reviewed — not assumed from contractual terms alone. Executed agreements, audit reports, incident-notification records, and deletion confirmations are retained as evidence artifacts.

Evidence Readiness: Vendor-side compliance events — consent, deletion, and disclosure — are reconciled against institutional records (BES-1 Principle 5, SIEM Reconciliation). Processor deletion confirmations are tracked and auditable. Incident notification records include the determination timestamp and the controller notification timestamp.

9. Consumer Biometric Access Rights (Where Applicable)

The organization has assessed whether it meets the thresholds triggering consumer biometric access rights under § 6-1-1314(5): processes personal data of 100,000 or more consumers per year; processes personal data of 25,000 or more consumers per year and derives revenue or discounts from the sale of personal data; controls or is controlled by another entity under common branding; or is a joint venture or partnership of two or fewer businesses sharing consumers' personal data. These rights are threshold-dependent and should not be assumed to apply uniformly to every controller processing biometric data.

Where thresholds are met, responses to biometric access requests include the required elements under § 6-1-1314(5)(a): the category and description of biometric data held; the source of the biometric data; the purpose for collection and processing and associated personal data; and the identity of third parties to whom biometric data has been disclosed and the purposes of those disclosures.

Access requests are processed using CPA response timing and appeal mechanics: responses within 45 days, extendable by an additional 45 days with notice; a documented appeals process for denied requests; and consumer notice of the right to contact the Colorado Attorney General where relevant.

Request intake, authentication method, response content, response timing, and appeal records are maintained. Records of complied-with requests are retained for at least 24 months consistent with implementing rules.

10. Enforcement Awareness

Enforcement under Part 13 is exclusively by the Colorado Attorney General and district attorneys. There is no private right of action under C.R.S. § 6-1-1314. Violations are treated as deceptive trade practices for enforcement purposes. Civil investigative demands and subpoena authority under the Colorado Consumer Protection Act framework may apply.

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. Counsel should confirm whether any cure concept applies to a specific compliance issue.

Civil penalties range from $2,000 to $20,000 per violation, capped at $500,000 per series of violations.

The organization's compliance posture is documented and reviewable — capable of being compiled and presented in response to an Attorney General inquiry or civil investigative demand.

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, annual review determinations, 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 tied to a defined trigger, 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.

Annual review determinations are recorded at the time the review occurs. Deletion initiation and completion timestamps are tied to the specific trigger event that initiated the deletion obligation.

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

Anchor to Ledger (where implemented)

Cryptographic hashes of attested events are anchored to an append-only ledger to strengthen tamper-evidence. This is an optional enhancement — Colorado does not require ledger anchoring. Tamper-evident mechanisms can help demonstrate chronology integrity; they do not, by themselves, establish that substantive legal requirements were met.

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

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, annual review determination records, 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 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 including missing vendor confirmations, annual review determinations without a corresponding deletion initiation record within the required window, and vendor disclosure events not reflected in governed records.

Retention overruns — data remaining beyond the 24-month window or 45/90-day post-determination window without a documented exception — are flagged automatically.

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.

Counsel Verification Queue

The following interpretive questions involve statutory language or cross-statute interaction that requires primary-source verification by qualified legal counsel. Open questions are preserved here rather than resolved in the checklist body so the document does not overstate unsettled law.

"Last interacted" for deletion timing. C.R.S. § 6-1-1314 uses "last interacted with the controller" as a deletion trigger but does not define the term. The organization's interpretation of what constitutes a qualifying interaction — 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. This interaction can affect how organizations classify incidents and determine applicable notice obligations. 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 for breach notification purposes.

"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 (referenced inside § 6-1-1314(4)(a)(I)) should be implemented as biometric-only obligations versus broader CPA program duties should be confirmed with counsel.