

THE MODERN IDV PLAYBOOK FOR CANADIAN LEGAL PROFESSIONALS



A practical guide to building a defensible, audit-ready approach
to identity verification in Canadian legal and real estate workflows



INTRODUCTION

Legal professionals are being asked to verify identity in an environment where remote transactions, synthetic identities, title fraud, AI-enabled document manipulation, and heightened anti-money-laundering scrutiny are converging. Simply ticking an identity-verification checkbox is no longer sufficient: the process must be appropriate, consistent, documented, and defensible if the matter is later questioned.

For Canadian law firms, notaries, and conveyancing teams, identity verification has shifted from a procedural onboarding step to a core risk-control function. Law Society rules continue to emphasize client identification and verification, source-of-funds inquiry, ongoing monitoring, recordkeeping, and withdrawal where fraud or illegal conduct is suspected. Client expectations have changed too. They increasingly expect digital, mobile, and remote experiences, so firms need processes that satisfy their professional obligations without creating unnecessary friction, administrative burden, or compliance gaps.

This playbook explains what is changing, what is at stake, where traditional approaches break down, what a defensible IDV process should include, and how firms can embed identity verification into the workflows they already use.

EXECUTIVE SUMMARY



IDV is risk management, not just onboarding.

Firms need to show that verification was completed using reliable methods, with the evidence properly retained.



The threat has changed faster than most processes.

Synthetic identities, compromised personal data, AI-manipulated documents, and account takeover routinely defeat manual review — and reported fraud losses are climbing.



Identity is only half the picture.

Where clients are organizations, firms must also identify directors and beneficial owners, the area regulators are watching most closely.



Defensibility depends on workflow design.

The strongest programs combine clear intake triggers, risk-based escalation, reliable sources, structured records, privacy controls, and audit-ready reporting.



Integration matters.

IDV is easier to apply consistently when it is embedded into the conveyancing or matter workflow rather than managed as a disconnected step.



1. WHY IDV IS UNDER SCRUTINY

Legal professionals in Canada are operating in a more scrutinized environment. Real estate transactions, trust accounts, corporate structures, and high-value transfers remain attractive to bad actors, and legal professionals sit at the centre of many of these workflows.

Law Societies continue to regulate lawyers' anti-money-laundering obligations, while federal and international bodies pay closer attention to professional intermediaries and the sectors most exposed to money laundering, fraud, and sanctions evasion. In October 2024, FINTRAC issued a Special Bulletin identifying the legal profession as a money-laundering and sanctions-evasion vulnerability, citing trust accounts, real estate, corporate formation, and beneficial-ownership structures.

That exemption is not absolute — British Columbia notaries are reporting entities under the federal regime — and the broader carve-out for legal professionals stems from the 2015 Supreme Court of Canada decision placing their AML oversight with the Law Societies rather than FINTRAC.

Internationally, FATF — the global anti-money-laundering watchdog — is conducting its Fifth Round Mutual Evaluation of Canada, with findings expected in 2026. Observers widely expect a focus on Canada's effectiveness against money laundering and on sectors viewed as vulnerable, including professional intermediaries such as lawyers. The direction is clear: identity verification is increasingly a point of regulatory, operational, and professional risk.

KEY MOMENTS DRIVING CHANGE

WHEN	WHAT CHANGED
2015	The Supreme Court of Canada confirms that Law Societies — not FINTRAC — regulate lawyers' anti-money-laundering compliance, establishing the profession's carve-out from federal reporting.
2019	Federation model rules are amended to allow identity verification without being in the client's physical presence.
2023–2024	The Federation requires lawyers to use technology capable of authenticating government-issued photo ID when verifying identity remotely — a decisive shift toward digital IDV.
June 2024	FINTRAC issues a sanctions-evasion bulletin; the federal beneficial-ownership registry comes online.
October 2024	FINTRAC publishes a Special Bulletin identifying the legal profession as a money-laundering and sanctions-evasion vulnerability.
February 2025	The Federation issues further guidance on the use of authentication technology for remote verification.
2025–2026	FATF conducts its Fifth Round Mutual Evaluation of Canada.
2026	Anticipated FATF findings are expected to shape the next wave of AML and IDV reform.



2. HOW FRAUD HAS CHANGED AND WHAT IT COSTS FIRMS

The fraud confronting legal professionals today rarely looks like crude forgery. It is layered, data-driven, and built to pass the checks firms have always relied on. The most common patterns include:



Synthetic identities — real and fabricated details combined into a convincing identity that can clear basic checks.



Impersonation using compromised data — leaked or purchased personal information used to pose as a legitimate client in a remote transaction.



Manipulated and AI-generated documents — genuine-looking templates and photo swaps that defeat visual inspection.



Social engineering and account takeover — attackers hijacking a client's email or phone to redirect funds or alter instructions.



Layered attempts — cases where each element looks legitimate in isolation, and the inconsistencies only emerge when the data points are assessed together.

The scale is significant and growing. The Canadian Anti-Fraud Centre recorded \$643.7 million in reported fraud losses in 2024 — and because only a fraction of fraud is ever reported, the true figure is far higher. Real estate and title fraud, in particular, have risen sharply year over year, with individual title-fraud cases frequently in the hundreds of thousands of dollars.

WHAT IS AT STAKE FOR THE FIRM

A failed or poorly documented verification is no longer just a compliance gap. It can mean funds disbursed to a fraudster, an errors-and-omissions or LawPRO claim the firm cannot defend, an inability to answer an insurer, auditor, or Law Society when asked how identity was confirmed, and lasting reputational damage. As the methods of fraud have shifted, so has the cost of getting it wrong — and increasingly that cost lands on the firm.

3. WHERE TRADITIONAL VERIFICATION BREAKS DOWN

Most identity-verification habits in legal practice were built for a different environment: clients met in person, often already known to the firm, presenting physical documents that were hard to fake. That environment has changed. Files are opened remotely, many clients are met once or not at all, and the documents presented can be manufactured to a standard that defeats the naked eye. The methods themselves remain valid; what tends to break down is the way they are applied. In practice, traditional approaches fail at four predictable points:

 **Visual inspection.** Manual review assumes a fraudulent document will look wrong. Advances in imaging, printing, and AI-assisted manipulation now let a forged or altered ID appear authentic — often carrying real, stolen data behind it — so nothing on the face of the document signals a problem.

 **Inconsistent execution.** When verification depends on individual judgment, it varies from lawyer to lawyer, clerk to clerk, and office to office. The same matter type can be handled several different ways, leaving gaps that surface only when a file is later questioned.

 **Fragmented recordkeeping.** Evidence is scattered across email, scanned attachments, screenshots, and disconnected systems. Even when the work was done properly, the firm may be unable to reconstruct what was checked, when, and why.

 **Remote and hybrid relationships.** Processes designed around a client across the desk do not translate cleanly to remote closings, yet the obligation to verify, and to document that verification, is unchanged.

The common thread is that a verification can be genuinely completed and still be difficult to defend later. Closing that gap is less about adding steps than about making the process consistent, evidenced, and repeatable.





4. RED FLAGS LEGAL TEAMS SHOULD WATCH FOR

Fraud rarely announces itself in a single sign; more often it appears as a pattern of urgency, inconsistency, avoidance, and unusual instruction:



The client resists verification or refuses to provide required information.



The client insists on unusual urgency without a clear reason.



Contact information changes shortly before closing or a movement of funds.



Email, phone, address, or identity details do not align across sources.



A third-party controls communication or appears to be directing the client.



Identification appears valid, but supporting data conflicts with the client's stated profile.



The client is hard to reach by normal channels but responsive through a new or unusual one.



Instructions involve rapid disbursement, changes to payment details, or unexplained source-of-funds concerns.

A strong process does not assume every red flag means fraud. It ensures red flags are documented, reviewed, escalated, and resolved before the firm proceeds.

5. PERSPECTIVES FROM THE FIELD

Dye & Durham works with digital identity-verification partners across the legal-technology ecosystem. The following perspectives reflect how providers working closely with legal and real estate professionals see identity risk, verification practice, and workflow expectations evolving.

TREEFORT TECHNOLOGIES

Based on Treefort's experience as the first-to-market digital identity verification solution available for Canadian legal professionals and high-risk real estate transactions.



Fraud today requires verifying the person, not just the document: The cases raising the greatest concern today often involve legitimate personal information paired with manipulated or falsified credentials that appear authentic in isolation. Treefort has observed fraudsters making repeated attempts using real compromised identity data, with inconsistencies only becoming visible when the document, the individual presenting it, and broader fraud indicators are assessed together. To date, Treefort's verification platform has contributed to the detection of tens of millions of dollars in potential title fraud by focusing on verifying the individual behind the identity rather than reviewing the document alone.



Defensible compliance depends on more than completing a verification: Completing a verification is only part of the compliance obligation. Increasingly, firms must be able to demonstrate that identity was verified using reliable methods and that required records were captured and maintained. Treefort supports all three Law Society-recognized verification methods and fully satisfies the record-keeping requirements associated with the Credit File Method, helping firms strengthen compliance processes while reducing administrative burden.



Accessibility and adoption matter just as much as technology: As firms move toward remote and digital onboarding, accessibility has become a critical part of risk management. Treefort has observed that verification processes are most effective when they accommodate a wide range of client demographics, technical abilities, and device preferences. Methods that create unnecessary barriers can introduce delays and additional administrative work for firms. Allowing clients to complete verification from anywhere in the world without installing software helps reduce friction while maintaining strong security and compliance standards.

COMMON MISCONCEPTIONS ABOUT IDV

- "All digital ID solutions offer the same assurance". In reality, verification methods, fraud detection capabilities, and compliance alignment can vary significantly between providers.
- "Completing a verification eliminates compliance risk". In practice, regulators expect firms to show the process was reliable, risk-based, and documented, not merely finished.
- "Digital IDV" is just document scanning." Effective verification weighs fraud and AML indicators and consistency across data points, not only the image on an ID.

FCT

Drawing on FCT's experience in digital identity verification, title insurance, fraud-risk mitigation, and real estate transactions.



The document can be genuine on its face and still be false.

After three decades in real estate fraud prevention, the pattern FCT points to is the photo swap: a fraudster places their own image on an otherwise authentic-looking template built from stolen or synthetic data. A client can sit across the desk, present ID that shows their photograph, pass a visual review — and still be misidentified. From a transaction standpoint, the control that holds up is validating the information against trusted external sources, because while AI can manipulate what appears on a document, the underlying data still has to reconcile.



Expectations are shifting toward connected verification.

In real estate and lending workflows, identity work is increasingly expected to link to the rest of the file — results tied to the order and to title insurance, and retrievable later by file number, client name, or email — so verification is consistent across transactions rather than re-keyed, and available if the matter is reviewed.



In high-stakes matters, layered authentication is the baseline.

“Good” is no longer a single check. It combines authenticating the document, confirming the person presenting it, and corroborating against independent sources, with stronger signals where the stakes justify them. For example, reading data directly from a passport's chip rather than a photo of the page. Throughout, sensitive identity data is handled securely and kept under the client's control, because stewardship is part of what makes the result trustworthy.

Across both perspectives, the common thread is that defensible IDV depends less on any single check and more on consistency, corroboration, and the ability to demonstrate how identity was verified.



6. VERIFYING INDIVIDUALS: THE THREE METHODS

Canadian Law Society rules recognize three methods for verifying an individual's identity: the government-issued photo ID method, the credit file method, and the dual process method. Each can be completed in person or remotely. Where verification is not done face to face, the Federation of Law Societies now requires the use of technology capable of authenticating the photo ID. A firm may also rely on an agent to apply a method on its behalf — but the firm remains responsible for the result and the record. The appropriate method depends on the client, the matter, the risk profile, and the applicable professional obligations.

Where does digital IDV fit? It is not a fourth method.

It is how firms now carry out the recognized ones — most visibly the government-issued photo ID method performed remotely, where technology authenticates the document and a biometric check confirms the holder, and also the credit file and dual process methods, which rely on electronic connections to credit bureaus and independent sources. The value of a digital solution is not that it bypasses the rules, but that it executes them consistently and captures the required evidence automatically.

Government-issued photo ID

This method requires reviewing an authentic, valid, government-issued photo ID and recording the document type, number, issuing jurisdiction, and expiry date. In person, it is straightforward — but visual inspection is an increasingly unreliable foundation as fraud tactics grow more sophisticated. Done remotely, it requires technology that confirms the document is authentic and that the person presenting it matches, for example through liveness and facial-comparison checks. Common challenges: scheduling in-person meetings solely for ID; reliance on human judgment for authenticity; inconsistent documentation across staff and offices; and a limited audit trail beyond internal notes or scans.

Credit file method

This method confirms identity using information from a Canadian credit bureau. It is widely accepted but not universally applicable; it does not work well for clients with limited or no credit history, new Canadians, or younger clients, and it depends on consistent capture of the required reference information.

Dual process method

The dual process method draws on two independent, reliable sources to verify identity. It offers flexibility and is commonly used for remote verification, but it raises recurring questions: which sources qualify as reliable and independent, how to capture the required reference numbers, how to maintain documentation across multiple systems, and how to demonstrate compliance on review.



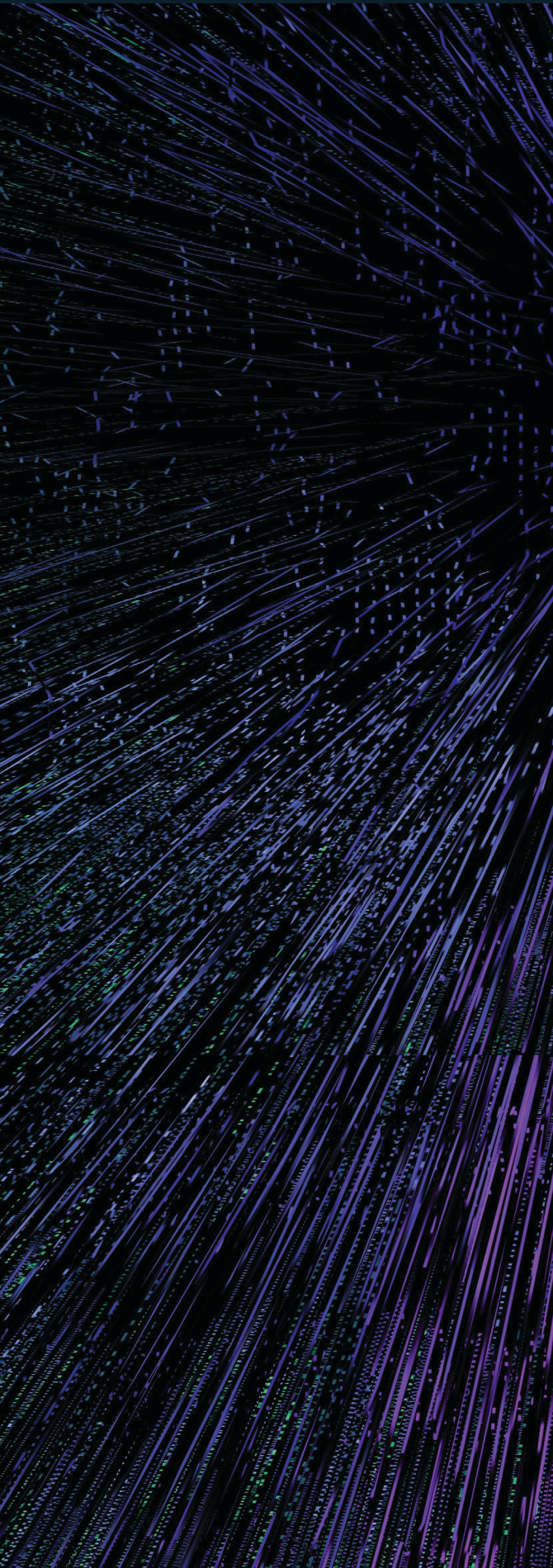


PRACTICAL TOOL: METHOD COMPARISON

METHOD	BEST SUITED WHEN	KEY RISK	WHAT TO CAPTURE
Government-issued photo ID	The client can be reviewed in person or remotely using technology that authenticates the document and confirms the holder.	Visual inspection alone can miss sophisticated forgeries and manipulated documents.	Document type, number, issuing jurisdiction, expiry, authentication evidence, and verification date.
Credit file	The client has an established Canadian credit history.	Does not work for new Canadians, younger clients, or thin credit files.	Source, reference details, date, result, and any exception handling.
Dual process	Two independent, reliable sources can corroborate identity details.	Uncertainty over which sources qualify and how to document them.	Source names, reference numbers, dates, matching data points, and reviewer decision.

THE COMMON CHALLENGE

Across all three methods, firms face the same underlying issue: consistency and defensibility. Manual processes are hard to apply uniformly; records end up in different places; key details get omitted; and audit trails are incomplete. Law Society rules are explicit about what must be captured for each method, from document details and reference numbers to source information and verification dates — and gaps in recordkeeping can undermine otherwise valid verification. The goal is to standardize the process, automate record capture where possible, and preserve a defensible audit trail without adding unnecessary administrative burden.



7. VERIFYING ORGANIZATIONS AND BENEFICIAL OWNERS

Verifying the individual in front of you is only half the picture. A great deal of real estate and high-value legal work runs through corporations, trusts, and partnerships. FINTRAC's October 2024 bulletin and FATF's scrutiny both centre on corporate structures and beneficial ownership, because opacity about who ultimately owns or controls an entity is what makes it useful for laundering and fraud.

Where the client is an organization, the rules expect firms to do more than confirm a signatory's ID. In practice that means:



Identify and confirm the organization — its name, address, and nature of business, and its existence (for example, through a confirming record such as a certificate of incorporation or registry search).



Identify directors and beneficial owners — the directors (*for corporations*) and the names, addresses, and occupations of individuals who own or control, directly or indirectly, 25% or more of the organization.



Take reasonable measures to confirm ownership and control — and keep a record of the ownership and control structure, and of how it was confirmed.

Treat opaque, unusually layered, or shifting ownership structures as escalation triggers rather than administrative hurdles. Where beneficial ownership cannot be obtained or confirmed, that difficulty is itself a risk signal, and one a regulator or auditor will expect to see addressed.

8. WHAT DEFENSIBLE IDV LOOKS LIKE

A defensible IDV approach is one that can withstand scrutiny from a client, insurer, regulator, auditor, court, or internal reviewer. It is not defined by one technology or one provider; it is defined by the quality and consistency of the process. In practice, a firm should be able to show:



Appropriate method selection based on the client, matter, risk profile, and applicable rules.



Reliable evidence from independent, valid, current, and traceable sources.



Consistent execution across lawyers, clerks, offices, and transaction types.



Clear exception handling when verification fails, produces inconsistencies, or requires escalation.



Structured recordkeeping so the firm can retrieve the evidence, result, date, and rationale later.



Privacy and security controls for sensitive personal information, including biometric or digital-identity data where applicable.

The objective is simple: if someone asks how identity was verified, the firm should be able to answer clearly, consistently, and with evidence.

9. CHOOSING AND EVALUATING AN IDV PROVIDER

As firms evaluate IDV approaches, independent standards are becoming an important signal of trust, reducing reliance on vendor claims alone. In Canada, the Digital ID & Authentication Council of Canada (DIACC) Pan-Canadian Trust Framework (PCTF) provides a benchmark for trusted digital identity, and many Law Societies refer members to the DIACC PCTF list when recommending identity verification providers. Certifications such as SOC 2 also speak to a provider's security and data handling controls. Certification under a recognized framework signals that a provider meets defined criteria for security, privacy, and reliability.

Privacy, biometrics, and Québec

Privacy obligations deserve particular attention where biometrics are involved. Under Québec's Law 25, an organization that creates a database of biometric characteristics must declare it to the Commission d'accès à l'information (CAI) at least 60 days before it is brought into service, and the CAI can modify, suspend, or prohibit its deployment. French-language requirements also apply. Even firms that do not practise in Québec can be affected — for example, where clients are referred to or from Québec notaries — so it is worth understanding how a provider handles these obligations.

Practical tool: questions to ask an IDV provider

-  Which Law Society verification methods does the solution support?
-  What evidence is captured automatically, and what must staff capture manually?
-  How are failed, incomplete, or inconclusive verifications handled?
-  Can reports be exported or retrieved for audit, claim, or internal review?
-  Where is personal information stored, and who can access it?
-  Does the solution support bilingual or Québec-specific requirements where needed?
-  Is the provider certified under the DIACC Pan-Canadian Trust Framework (PCTF)?
-  What certifications, attestations, or independent controls support the provider's claims?
-  How does it integrate with conveyancing, matter





10. FROM PROCESS TO PLATFORM: EMBEDDING IDV IN UNITY®

The next stage of IDV is embedding verification inside legal and conveyancing workflows, so that it becomes a consistent, visible, and documented step in the matter lifecycle rather than a disconnected task. When IDV is integrated into a platform such as Unity®, firms can manage identity verification in the same environment where the work already happens:



Initiate IDV from the matter or client workflow.



Reduce duplicate data entry and manual handoffs.



Keep verification status visible to the team.



Associate verification reports and results with the transaction.



Support consistent, firm-wide processes across high-volume real estate matters.



Make retrieval easier if the file is later reviewed, audited, or questioned.

Crucially, this is not a new method of verification but a way to apply the recognized ones. The partner IDV solutions integrated into Unity® — Treefort and FCT — perform the Law Society methods, capture the required evidence automatically, and link it to the matter, so the regulator-recognized process and the firm's day-to-day workflow become the same thing.

By integrating partner IDV solutions into the workflow, Unity® helps firms move from ad hoc verification to a standardized, matter-linked process. The practical takeaway is simple: IDV should not live outside the transaction; it should sit where legal professionals already manage the file, the client, the closing, and the associated risk.

11. PUTTING IT INTO PRACTICE

Whether you are building or reviewing your IDV processes, the path is the same. These four steps take a firm from assessment to an embedded, defensible process:

1. **Assign an owner and map the current state:** Give one person — a partner or compliance lead — responsibility for the program, then map how identity is verified today across matter types, for individuals and for organizations and their beneficial owners, and where the records live.
2. **Set a firm standard:** Define when verification is triggered, which method applies by matter type, what evidence must be captured and retained (including beneficial ownership), and how red flags are escalated.
3. **Choose and connect a digital solution:** Select one that fits the firm's compliance, privacy, accessibility, and workflow-integration needs, and tie its results to the matter record.
4. **Pilot, then roll out:** Prove the approach on one practice group or matter type, confirm the firm can retrieve a complete verification record on demand, then extend it firm-wide and review periodically as fraud tactics, standards, and Law Society guidance evolve. Map how identity verification is performed across matter types, including organizations and beneficial owners.



CONCLUSION: RAISING THE BAR ON IDV

Identity verification is no longer just an onboarding exercise. As fraud becomes more sophisticated and expectations around compliance, documentation, and accountability continue to rise, IDV is increasingly becoming a core component of risk management and professional responsibility.

Legal professionals are being asked not only to verify identity, but to demonstrate that appropriate steps were taken, what evidence was collected, and why their approach can be trusted.

Firms that take a structured, defensible approach—covering both individuals and the organizations behind them, and embedding verification into everyday practice—will be better positioned to reduce risk, improve consistency, and respond with confidence when their work is scrutinized.

Practical Tool: **Defensible IDV checklist**

- ☐ Has the firm identified when verification is required for the matter?
- ☐ Was the verification method appropriate for the client and risk level?
- ☐ Were required data points captured completely and accurately?
- ☐ Were the sources independent, reliable, valid, and current?
- ☐ Was the verification date recorded?
- ☐ Were failed, incomplete, or inconsistent results escalated?
- ☐ For organizations, were directors and beneficial owners identified and confirmed?
- ☐ Are records retained with the matter or easily linked to it?
- ☐ Can the firm retrieve the verification record quickly during an audit, claim, or review?
- ☐ Are privacy, consent, storage, and access controls documented?