INTUIT
professional tax solutions

Tax Compliance FAQs:

Common Questions Answered for Year-End Preparation

Pre-peak season is when compliance questions move from theory to impact. The e-signature workflows you establish, the encryption you configure, and the consent processes you implement now become your operating reality once the busy season arrives.

This is the moment to confirm your compliance posture: Should you switch to electronic signatures? Do your encryption standards meet current requirements? When do PTIN renewals need to happen?

These aren't theoretical questions. They're decision points that determine whether your firm operates in compliance or discovers gaps mid-season, when correction is expensive.

Pre-peak season already feels packed, but answering these tax compliance FAQs now prevents peak-season crises. You still have time to implement solutions, test them, and confirm they work before filing season removes your flexibility.

Here are the answers you need now.

What are the IRS requirements for e-signature compliance on tax returns?

IRS Revenue Procedure 2000-31 and Publication 1345 govern e-signature compliance tax returns.

YOUR PROCESS MUST MEET FOUR REQUIREMENTS:

01 Authenticate the signer's identity.

02 Maintain signature integrity so it can't be tampered with after signing.

03 Ensure non-repudiation so the signature can't be denied later.

04 Use secure transmission to protect data during signing.

Most modern tax platforms include IRS-compliant e-signature capabilities built in. The system authenticates signers through knowledge-based questions or secure portal access, maintains integrity through tamper-evident technology, and transmits data via encrypted connections that meet IRS security standards.

But compliance depends on configuration, not just having the feature available.

How to validate your process:

- Enable e-signature functionality in your software settings.
- Configure client portal access with secure authentication methods.
- Test the complete workflow using sample returns from signature request through completed signing.
- Verify signature certificates include required IRS elements like timestamp and authentication method.
- Document your e-signature procedures for regulatory inquiries.

Firms that test their e-signature workflow during pre-busy season sometimes discover they're collecting signatures but not capturing the authentication method in the certificate. The signatures are technically invalid under IRS standards even though clients are signing properly. Fixing the configuration during the validation window prevents issues before real filings are affected.

Test your e-signature process before busy season when you still have time to fix configuration issues. Once peak season begins, every signature matters.

IRS Standard: Revenue Procedure 2000-31, IRS Publication 1345

BENEFIT

Reduces client friction during signing while maintaining full compliance and audit readiness for e-signature compliance tax returns.

How long must we retain client tax returns and supporting documentation?

The IRS requires three years minimum from filing date. Professional standards recommend seven years to cover the full statute of limitations including extensions. State requirements sometimes demand longer, and those supersede federal minimums.

HERE'S THE PRACTICAL REALITY:

- Three years protects you from routine audits.
- Seven years protects you from everything else, including amended returns, fraud investigations, and malpractice claims that surface years after you thought a file was closed.

Most modern systems handle retention automatically. Returns and supporting documents stay accessible throughout required periods without manual tracking or the risk of a hard drive failure destroying your records. The system applies retention policies by document type and maintains records according to schedules you configure once.

How to validate retention:

- Review your current policy against IRS minimums and state requirements where you practice.
- Configure automated retention rules for returns, source documents, and correspondence.
- Test that archived documents remain accessible throughout the retention period without degradation.
- Document your retention policy in writing, including destruction procedures for records exceeding retention requirements.

Firms that review their retention policies during year-end preparation sometimes discover the policy exists on paper but isn't applied automatically. Staff are manually deciding what to keep and what to delete. Enforcement becomes inconsistent, and some client files develop gaps that would create problems during an audit.

Automated retention eliminates the "did we keep that?" question when it matters most.

IRS Standard: IRC Section 6001, IRS Publication 552

BENEFIT

Eliminates manual tracking and ensures audit readiness throughout required preservation periods.

Is multi-factor authentication required for tax preparation software?

Not technically required by the IRS for all users, but practically essential. IRS Publication 4557 strongly recommends MFA as part of comprehensive security measures. The IRS does require it for Electronic Filing Identification Number holders accessing the e-Services portal. Many state boards now require it as part of data security rules for licensed professionals.

HERE'S WHAT MATTERS MORE THAN THE REQUIREMENT:

99%

Reduces unauthorized access risk by roughly 99% compared to password-only systems. If someone gets your password through a phishing email or data breach, MFA stops them at the second verification step.

Compliant MFA requires two separate factors from different categories:

Something you know like a password, something you have like a phone or security key, or something you are like a fingerprint.

SMS codes, authenticator apps, and hardware tokens all work when properly implemented and can't be bypassed.

How to implement:

- Enable MFA for all users regardless of whether it's technically required.
- Select authentication methods appropriate for your team's technology and remote work patterns.
- Establish backup authentication procedures for device loss scenarios.
- Document MFA requirements in your firm security policy.
- Train staff on proper authentication and protection of authentication devices.

Firms that enable MFA during pre-peak validation can block credential stuffing attacks when peak season begins. Audit logs often show dozens of failed login attempts that stop at the MFA layer. Without that secondary verification, attackers would gain access using stolen credentials.

IRS Standard: IRS Publication 4557, e-Services security requirements

BENEFIT

Critical protection for remote work environments and demonstrates security due diligence during audits.

What encryption and data protection standards must our tax software meet?

IRS Publication 4557 requires encryption for data at rest when stored and in transit when transmitted between systems. Practically, this means AES-256 encryption for stored data and TLS 1.2 or higher for transmitted data between users and servers.

HERE'S WHAT YOU ACTUALLY NEED TO VERIFY:

Your software encrypts all **client data automatically**, and **web-based platforms** use secure connections when data moves between your system and the cloud or between users.

Most modern platforms use bank-level encryption meeting IRS requirements for both storage and transmission. Your job isn't implementing the encryption, it's verifying it's actually working.

How to validate:

- Verify your software uses encryption meeting IRS Publication 4557 requirements through vendor documentation.
- Confirm web-based platforms use secure connections by looking for "https" in the address bar, not "http."
- Check that the security certificate is valid by clicking the lock icon in your browser.
- Test that client portal communications show encrypted connections when clients access their information.
- Document your encryption approach in compliance records.

Firms sometimes assume their platform is encrypted because it's cloud-based. During year-end validation, you might discover your client portal is using an expired security certificate. Clients could be accessing sensitive data over unencrypted connections for weeks before anyone notices.

Verify encryption, don't assume it.

IRS Standard: IRS Publication 4557, FIPS 140-2

BENEFIT

Protects client's personally identifiable information and meets regulatory requirements under tax compliance FAQs.

What are the current PTIN requirements?

All paid tax return preparers must have an active Preparer Tax Identification Number before preparing returns for compensation. PTINs must be renewed each year for the upcoming filing season, and renewal is required even if none of your information has changed since the prior year.

The timing matters. If you wait until the last part of the year, you're competing with thousands of other preparers for IRS processing bandwidth. Renewals can take weeks during peak periods.

How to stay compliant:

- Audit all preparer PTINs in your firm during the off-season to identify upcoming expirations.
- Document PTIN information for each preparer including renewal dates.
- Verify expiration dates through the IRS PTIN system.
- Configure your software to include the correct PTIN on every preparer's returns automatically.
- Schedule renewals for all preparers well before the year-end rush to avoid processing delays.
- Test with sample returns before filing season to catch configuration errors.

Firms that test during pre-peak season sometimes discover preparers have expired PTINs still configured in their system. Every return associated with those preparers would be rejected during filing season.

IRS Standard: IRS Circular 230

BENEFIT

Prevents filing delays from expired PTINs and ensures all preparers meet requirements throughout the season.

When do we need signed disclosure consent forms from clients?

IRC Section 7216 requires written consent before you can use or disclose client tax return information for purposes beyond return preparation. This includes **sharing information** with third-party service providers like payroll processors, **using data for firm marketing**, or **discussing returns** with anyone not directly involved in preparation like family members or business partners.

Compliant consent forms must identify the specific recipient by name or category, specify the exact purpose of disclosure, state the duration of consent with specific dates or events, and inform clients of their right to refuse or revoke consent.

Review current engagement letters and consent forms against IRC 7216 requirements.

Store signed consents with client records for at least three years per IRS requirements.

Update forms to include all required elements in clear language.

Train staff on when consent is required versus permitted uses that don't need additional authorization.

Implement secure consent collection using electronic signatures through client portals or traditional paper signatures.

Many firms discover their engagement letters mention data sharing but don't meet the specific IRC 7216 requirements for duration, revocation rights, or recipient identification.

IRS Standard: IRC Section 7216, Treasury Regulation 301.7216

BENEFIT

Protects from inadvertent disclosure violations and maintains client trust through transparent consent processes.

What are the current IRS e-file requirements for tax professionals?

Tax professionals who prepare 11 or more individual income tax returns annually must file electronically unless granted a hardship waiver. This requirement applies to the total returns prepared by each individual preparer, not just returns for which they're compensated. The threshold applies per preparer, not per firm.

If you prepare 10 returns, you're exempt. If you prepare 11, every return must be e-filed.

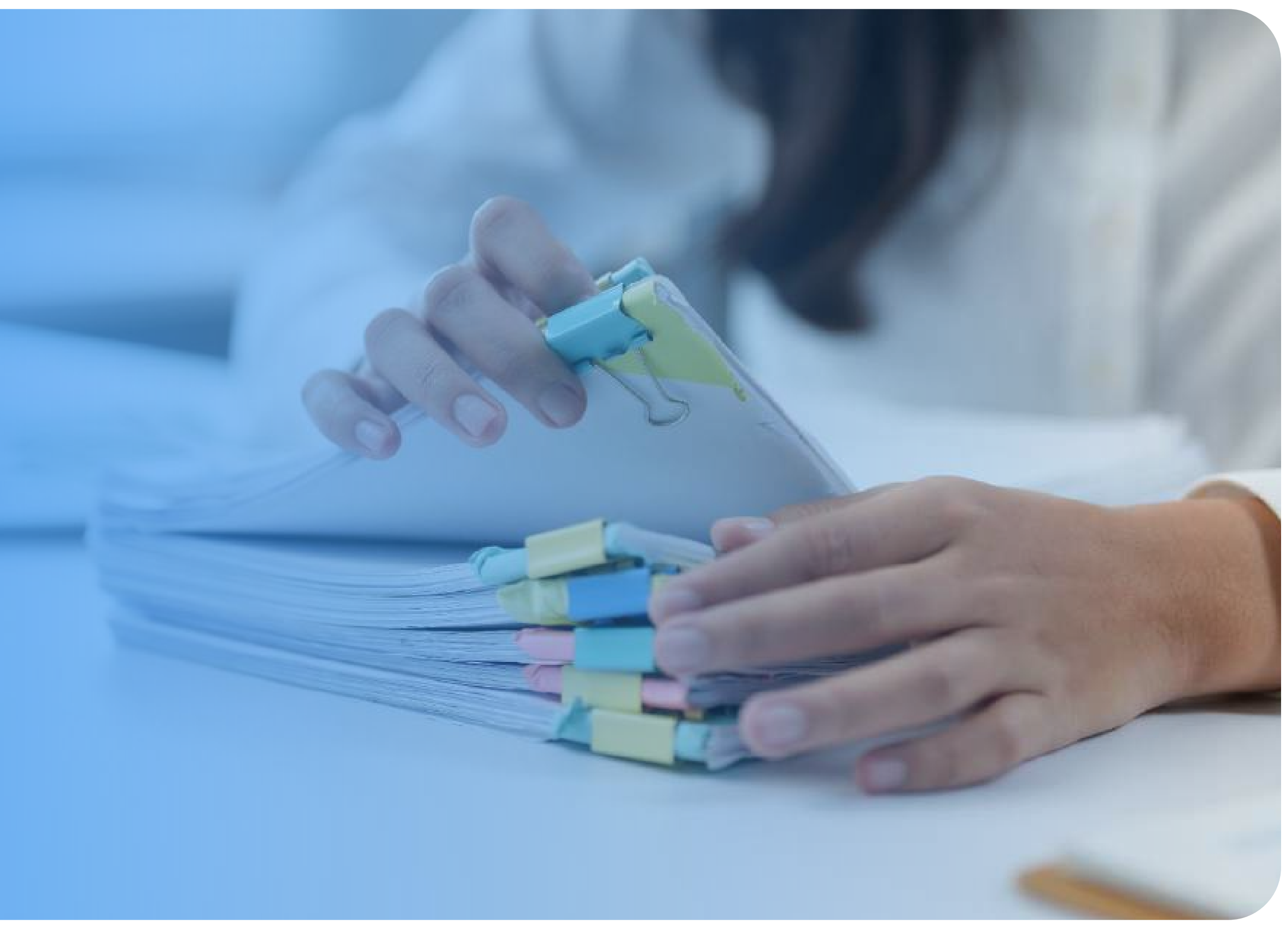
- Count returns prepared by each preparer in your firm to determine who meets the 11-return threshold.
- Apply for an Electronic Filing Identification Number if your firm doesn't already have one using Form 8633.
- Complete the IRS suitability check including fingerprinting and background verification.
- Configure your software with your EFIN for electronic filing capability.
- Test e-file connectivity and transmission before filing season using IRS test environments.

The application process takes time. If you're approaching the threshold and don't have an EFIN yet, start the process early in pre-peak season.

IRS Standard: IRS Revenue Procedure 2007-40, IRS Publication 3112

BENEFIT

Ensures compliance with mandatory e-file requirements and enables faster refund processing for clients.



Why These Questions Can't Wait Until The New Year

Pre-peak decisions about compliance lock in for the entire filing season. Once you establish e-signature workflows, configure data protection settings, or implement consent procedures, changing them mid-season disrupts operations across your entire team.

- **Compliance gaps** can scale quickly across many returns.
- An **improperly configured e-signature** process affects every client who signs electronically.
- **Inadequate encryption** exposes every return you prepare.
- **Missing PTIN renewals** delay every filing by affected preparers.

What starts as a single configuration error multiplies into firm-wide risk exposure.

Fixing configuration issues mid-season often leads to operational delays. Stopping production to reconfigure compliance features means delayed filings, confused staff, and frustrated clients. It's like realizing your safety equipment doesn't work during an emergency instead of during the drill.

Year-end preparation is the window to ask questions, implement answers, and validate that everything works correctly. Once peak season begins, you lose the flexibility to adjust compliance infrastructure without affecting production.

Quick Reference: Compliance Resources

When you need to verify something or dive deeper into a specific requirement, these resources provide authoritative guidance:

IRS Publications:

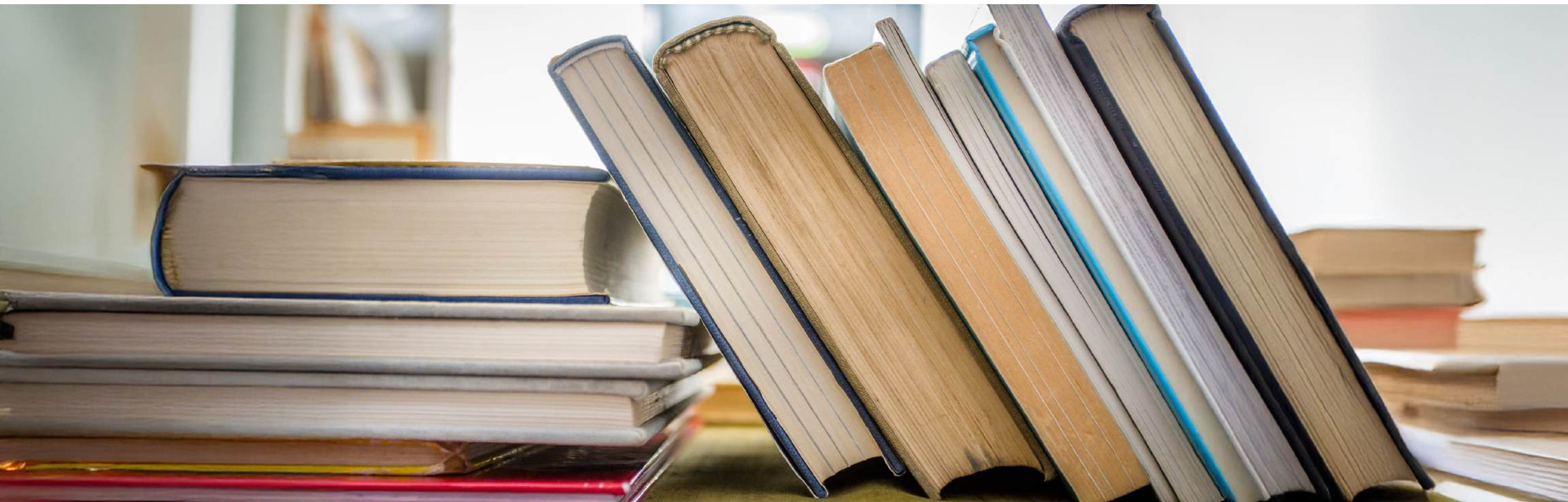
- Publication 4557: Safeguarding Taxpayer Data
- Publication 1345: Handbook for Authorized IRS e-file Providers
- Publication 552: Recordkeeping for Individuals
- Circular 230: Regulations Governing Practice Before the IRS
- Publication 3112: IRS e-file Application and Participation

Online Resources:

- IRS.gov/Tax-Professionals for current guidance and updates
- e-Services portal for EFIN and PTIN management
- Your software vendor's compliance documentation and support

Professional Resources:

- State board of accountancy data security requirements
- Professional liability insurance compliance guidelines
- Industry association best practice guidance



What This Means for Your Firm

Pre-peak season is the decision window. Configuration determines whether compliance features actually protect your firm or just exist on paper. Features are built into most modern platforms, but proper setup and validation ensure effectiveness.

You have roughly **8-10 hours of compliance validation work** ahead if you haven't tested these areas recently. That's a small investment compared to discovering gaps once peak season begins while you're processing client returns under deadline pressure.

How ProConnect Tax Supports Tax Compliance FAQs

The seven tax compliance FAQs in this guide address common questions firms face during pre-peak preparation. But having the right answers isn't enough. You need a platform that operationalizes them.

01

E-signature compliance requires IRS-compliant authentication, integrity measures, and secure transmission meeting Revenue Procedure 2000-31 standards. ProConnect Tax handles all of this automatically through built-in e-signature workflows. Client portal access authenticates signers securely. Signature certificates include required IRS elements like timestamps and authentication methods. Transmission uses encrypted connections meeting IRS security standards.

02

Data retention happens automatically based on policies you configure once. Set retention rules for returns, source documents, and correspondence, and the system applies them consistently. Documents remain accessible throughout required periods without manual tracking. When the IRS requires seven years of retention, your platform enforces it systematically.

03

Multi-factor authentication integrates directly into your login process. Enable MFA for all users, and ProConnect handles authentication through SMS codes or authenticator apps. The secondary verification layer protects against credential theft and unauthorized access without requiring separate security tools.

04

Encryption meets IRS Publication 4557 requirements for data at rest and in transit. Your client data stays protected through AES-256 encryption for stored information and TLS protocols for transmission. SSL certificates maintain secure connections automatically. You verify encryption is working rather than implementing it manually.

05

PTIN configuration ensures every preparer's returns include their current PTIN automatically. Update preparer information once in your system settings, and every return filed by that preparer carries the correct identification. When PTINs renew, update the configuration and all subsequent returns reflect the current information.

06

E-file connectivity for federal and state returns routes through integrated transmission systems. Test federal e-file through IRS acceptance environments. Validate state e-file separately for each jurisdiction. The platform manages transmission protocols, acknowledgment retrieval, and rejection handling.

07

Consent documentation for IRC Section 7216 compliance integrates with your engagement process. Client portal workflows can collect required consents electronically with proper signature authentication. Store signed consents with client records where they're accessible for regulatory inquiries.

This guide provides the knowledge framework. ProConnect Tax provides the platform infrastructure that makes compliance systematic rather than manual.