SmartVault

Quick Guide to FTC's Safeguards Compliance

In this brief guide, you'll learn

- Why the Rule is important
- What you need for compliance
- How to make compliance simple

Why the Rule's Important

As an accounting professional, you handle a tremendous amount of information that cybercriminals are eager to access. You're legally obligated to protect this data from getting into the wrong hands.

The FTC's Safeguards Rule Protects Data

The Federal Trade Commission (FTC) enacted the Standards for Safeguarding Customer Information – the Safeguards Rule – in 2003 to help businesses protect consumer and customer data. The Safeguards Rule stems from the Gramm-Leach-Bliley Act (GLBA), which is the United States law requiring financial institutions to protect the integrity, confidentiality, and security of customer data. You have until June 9, 2023 to comply.

Cybersecurity is Getting More Complex

Cybersecurity is about protecting electronic data from criminals or unauthorized use. There are many ways hackers and unauthorized users can access your information, and their technology and techniques are getting stronger every day. Don't make the mistake of thinking it'll never happen to your business.

In fact, many cybercriminals are focusing on practices just like yours. They know you handle a lot of information and that you're less likely to have sophisticated cybersecurity programs that larger businesses have.

But there is good news is: There are ample ways you can protect your data, including simple measures that are fast to implement. A smart decision is to use software that'll do the complicated cybersecurity work for you.

With the FTC's Safeguards Rule, now it's not just a matter of doing what's best for your customers or business. It's also about complying with the law.

You have until June 9, 2023 to comply. With penalties up to $46,000 per day, you can't afford to risk non-compliance.

What You Need for Compliance

The Safeguards Rule requires you to implement the strongest security safeguards the accounting industry has ever seen.

Accounting businesses with nonpublic personal information (NPI) of at least 5,000 individuals – whether those records are physical paper or digital files – must comply. The Rule requires you to have a security plan and various security measures to protect NPI.

> **So what is NPI?** It covers a broad type of information, like names, addresses, phone numbers, income information, Social Security numbers, and credit history. It can be difficult to tell what's covered, so experts encourage businesses to treat all customer information as NPI.

Safeguards Checklist

You must create a plan and implement various measures, including these:

- Set granular access to files and folders, and who can view, create, edit, or delete them.
- Periodically see who has access and revoke or change their permissions as needed.
- Encrypt data in transit and at rest.
- Ensure systems have multi-factor authentication (MFA) as part of the login process.
- Dispose of customer information no later than two years after you have used it.
- Monitor and keep a log of users' activity when accessing customer information.

*This is not an exhaustive list of requirements. See the Safeguards Rule for full list.

Protecting your data is a large obligation to meet, but it doesn't have to be complicated. Use a cloud-based document management system and client portal to implement these required safeguards. Plus, you'll have powerful tech helping you run your business.

SmartVault

How to Make Compliance Simple

Partner with a vendor that takes the responsibility of protecting your information seriously. SmartVault's document management system and client portal are built with bank-level security and compliance in mind.

Here's how SmartVault helps with compliance:

Access Controls
Set granular access to files and folders, and who can view, create, edit, or delete them. Quickly see who has access and revoke or change their permissions.

Encryption at Rest and Transit
SmartVault automatically encrypts your data in transit and at rest using bank-level standard AES-256 bit encryption.

Multi-Factor Authentication (MFA)
SmartVault has MFA, which requires users to log in with their email address, password, and a verification code.

Information Disposal
Admins can remove a customer's data in just a few steps.

Activity Monitoring
SmartVault automatically tracks all user activity, including when they upload, download, delete, or change a folder, vault, or document. This report is an authoritative record that no one can edit.

Reliable Security
You're responsible for ensuring the data is safe on your selected vendor's software. You can rest assured it is with SmartVault.

Join over 30,000 accounting professionals who confidently protect their data with SmartVault.

Learn more: smartvault.com ►