Whitepaper on Cybersecurity for Tax Professionals: The FTC/GLBA Safeguards Rule, IRS Data Security Requirements & NY SHIELD Act

June 2021

securex

CYBERSECURITY +
HIPAA COMPLIANCE

455 Oak Glen Road
Howell, New Jersey 07731

Phone / 732.285.4702
info@securexcyber.com
securexcyber.com

Table of Contents

455 Oak Glen Road
Howell, New Jersey 07731

Phone / 732.285.4702
info@securexcyber.com
securexcyber.com

Prologue: Why Cybersecurity & Compliance (Should) Mean Everything to Every Tax Professional

You are a business owner. You are a CPA or EA. Your business has been prospering for many years.

Now it's storytime:

You are sitting back in your chair, wrapping up your day's work, and sending off one last email. You grin with satisfaction, knowing that soon you will be able to leave your office and spend some quality time with family, pursue your favorite pastime, or simply relax. Your email suddenly doesn't work. The tax return pdf you were looking over a minute ago, ready to send, won't open. None of your files will open. Nothing works. Your entire business is dead in the water. Your IT says a ransomware attack hit you, and it's too late to stop it. The hacker demands you pay an exorbitant fee and *trust them* to return everything to normal. They eventually start cashing in on your clients' tax returns, one by one. **You are forced to take out a pen and paper and a printed contact list if you are fortunate to have one,** and you start to call **every single client**. Feeling ill with shame, you tell them the terrible news and that they should report the theft of their SSN and personal information to the Social Security Office, the IRS, their identity theft protection service, or whoever can help them now. You suffered a data breach and a ransomware cyberattack.

Since 2016 approximately **4,000** of these types of ransomware attacks happen **every day** in the US. You have been making that gamble every day, and you just lost. Now, the only thing ringing in your ears is what Benjamin Franklin said, "An ounce of prevention is worth more than a pound of cure." But it's too late.

To this point, in March 2020, the NYSHIELD Act came into effect for New York State business and to all companies **nationwide** that have customer information of residents of New York State. **No exceptions.**

The new law is also a case in point that all businesses, **everywhere**, need to be aware of cybersecurity best-practices, both in their internal operations and their interactions with the other companies. In 2020, even amidst the global crisis, "ignorance is bliss" in cybersecurity and compliance, is now *passe.*

The new Act requires you to:

- Report data breaches to your clients and other agencies.
- **Conduct a thorough and accurate risk assessment of your internal and external risks.**

- **Create and implement security policies and procedures to reduce those risks**
- Provide ongoing training, review, and monitoring of your security environment.
- New York State can issue fines up to $200,000 in the event of a breach for failure to comply.

Besides the healthcare industry, **nobody** has as much sensitive-nonpublic information as Tax Professionals, CPAs, EAs, Wealth & Investment Advisors, and other financial institutions. These businesses come in all shapes and sizes, from single practitioners to dozens of employees or more. The risks don't change. Each owner, regardless of their business's size, needs to know what their risks are. They need a plan to reduce these risks and protect against reasonably anticipated threats. If a team of elite hackers chose to target a business persistently, they would get almost anyone. Still, nobody wants to be the "low hanging fruit" for all the myriads of experienced or amateur hackers or even automated threats that scour the internet 24/7/365, looking for targets. Even a petty thief can steal a laptop with a password and find someone who can get in if it's not secured.

Even with robust security, you may need to **prove to the Government** that you **assessed and managed your risks** and have the **appropriate policies and procedures**. Otherwise, you risk more severe consequences. This documentation needs to meet compliance laws that apply to financial institutions, such as the FTC (GLBA) Safeguards Rule, IRS Security Requirements, NYDFS Cybersecurity Rule, possibly HIPAA, and more.

It's **vital** to engage a professional who uses **experience, expertise**, and **detective work** to remove your **stress and pain**, who will provide for your security and compliance, **regardless of your size.**

A Word from our Chief Cybersecurity Compliance Consultant

I seek to make others' lives better. Life is filled with puzzles that I work to solve and that detective work is my go-to approach to removing your pain. Ultimately, I want to help others rise up and be self-sufficient.

As the Chief Cybersecurity Compliance Consultant at Securex, I help remove pain relating to the compliance of HIPAA, GLBA, New York Shield and NYDFS regulations from companies of all sizes. My inclination is to service my clients in 3 ways: Firstly, being that the industry and laws are really vague, I choose to meet and exceed the needs to help minimize your risk and avoid unnecessary and easily preventable pain. Secondly, I provide a solution that can be

tailored to each scenario and threat, through providing multiple tiers of service, to accommodate everyone's needs. Lastly, everything I do is to help remove pain and worry and as stressful as cybersecurity and compliance are, I will take good care of you.

Here for you,

Ariel Sandell | Chief Cybersecurity Compliance Consultant

CHSP CHITSM CPCIP | Microsoft Technology Associate: Security Fundamentals

Servicing HIPAA, GLBA, IRS, NYSHIELD and NYDFS | Certified in HIPAA + PCI-DSS + Healthcare IT Security Management + HIPAA Risk Assessment + HIPAA Disaster Recovery

(Read on to continue our whitepaper on security and the various compliance requirements...)

About GLBA, IRS & NYSHIELD Requirements

FTC/GLBA Requirements

Companies that deal with nonpublic financial information must comply with the Gramm-Leach-Bliley Act (also known as GLBA). The United States Federal Trade Commission (FTC) oversees GLBA regulations and compliance.

The FTC has levied millions of dollars in fines upon discovering a lack of compliance with this rule, as well as additional legal liabilities. Penalties can include imprisonment for up to 5 years, steep fines, or both. Fines can be up to $100,000 for each violation; officers and directors can be fined up to $10,000 for each violation.

Most business leaders think GLBA has only to do with privacy and confidentiality alone, which is the focus of attorneys. However, at Securex, our focus and specialty are with the lesser known but critically important **GLBA Safeguards Rule** *(also known as the FTC Safeguards Rule)*. These companies, which deal with nonpublic financial information, must have the physical, network, and business process security measures in place, as well as follow them to ensure compliance with the rule. **The rule also requires them to conduct a thorough and accurate Risk Assessment.** Based on the assessment, they are required to create a detailed written **Information Security Program.**

The GLBA Safeguards Rule requires that organizations create and implement a written Information Security Program based on each organization's size and complexity. The rule contains general guidelines for safeguards in the following areas:

1. Appointment of an Information Security Officer
2. Risk Assessment
3. Employee Management & Training
4. Information System (Computer) Security
5. Monitoring Systems to Detect and Manage System Failures and Security Incidents
6. Security Requirements for Third-Party Vendors
7. Periodical Monitoring, Testing and Revisions to the Information Security Plan

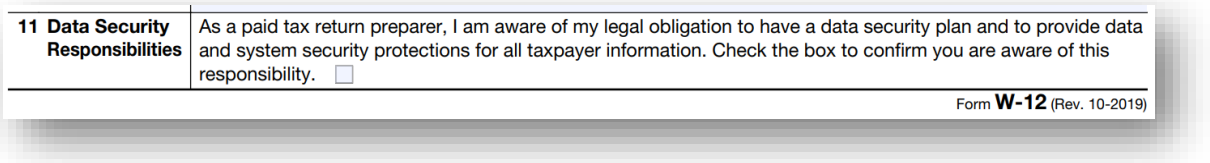
As with many regulations, the laws may be written very generally and open to interpretation. Several Government sources and cybersecurity best-practices govern how to cover these areas to meet the requirements.

Some examples of these safeguards include: encrypting computers with customer information, encryption of data being sent over a network, anti-malware safeguards, internal auditing of system activity, employee security training, testing & revision of security safeguards, agreements from your third-party vendors to maintain the security of your customer's information, two-factor authentication and more.

IRS Requirements

According to the IRS, accountants, who prepare or assist in preparing federal tax returns for compensation, must have a valid PTIN (Preparer Tax Identification Number), which is renewed by the IRS annually. When renewing a PTIN, the IRS requires the applicant to have a "data security plan," which according to the IRS, is satisfied through having a written Information Security Program **that complies with the GLBA Safeguards Rule** (mentioned above). (See further in this whitepaper and the related links for more information.)

Below is an excerpt from the IRS Form W-12 "IRS Paid Preparer Tax Identification Number (PTIN)":



11 Data Security Responsibilities	As a paid tax return preparer, I am aware of my legal obligation to have a data security plan and to provide data and system security protections for all taxpayer information. Check the box to confirm you are aware of this responsibility. ☐

Form **W-12** (Rev. 10-2019)

Additionally, the IRS requires anyone classified as an "e-filer', to create and implement a written security plan.

According to the IRS, gaps in a data security plan can result in sanctions and penalties under the Federal Trade Commission and the Internal Revenue Code. Refer to the IRS ***Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns (page 6):***

"All persons and entities who receive taxpayers' personal information can use Publication 4557, Safeguarding Taxpayer Data, A Guide for Your Business, to help determine their data privacy and security needs and implement safeguards to protect them. Publication 4557 includes information about security standards and best practice guidelines to safeguard consumer information such as personal tax data, with links to several resources including National Institute of Standards and Technology (NIST) publications. Failing to take necessary steps to implement or correct your security program may result in sanctions from the FTC. Failures that lead to an unauthorized disclosure may subject you to penalties under sections 7216 and/or 6713 of the Internal Revenue Code (I.R.C.). Providers appoint an individual as a Responsible Official who is responsible for ensuring the firm meets IRS e-file rules and requirements. Providers with problems involving fraud and abuse may be suspended or expelled from participation in IRS e-file, be assessed civil and preparer penalties or be subject to legal action."

NOTE: *E-Filers may have additional security and procedural requirements relating to submitting tax return to the IRS. These procedures may relate to accounting practices such as*

signatures, timely filing on behalf of clients and other accounting practices, etc. and are not covered in this assessment or ensuing recommendations, etc. E-filers that are also Online Providers, Intermediate Service Providers or Software Developers (which involves creating or managing commercially available accounting software for clients) have additional security requirements mandated by the IRS, which add-on to GLBA requirements. For a more detailed description of the various types of e-filers, as well as their related accounting practice requirements, refer to the ***Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns*** (page 7) and the guide on ***IRS e-file Participation and Application*** *(page 7 & 5)*

(Your category may be found by entering your name into the IRS index here: https://www.irs.gov/e-file-providers/authorized-irs-e-file-provider-locator-service-for-tax-professionals .)

(More information on the IRS, PTIN & the GLBA (FTC) Information Security Program can be found in the following links: FTC link, IRS link

NOTE: The links in this document provide more information on the GLBA (FTC) Safeguards Rule & IRS requirements. It does not contain a complete list of all Government & cybersecurity recommendations for security & compliance with GLBA. Additional valuable security & compliance recommendations based on IRS, Government & cybersecurity recommendations, are provided in our GLBA Package, as well as the documentation for the risk assessment and security plan required for compliance.

NYSHIELD

Additionally, on March 21st, 2020, NY Senate Bill S5575B, which passed last year, was put into effect. This law is the "Stop Hacks and Improve Electronic Data Security Act" (also known as the NY SHIELD Act). **NYSHIELD requires all businesses with nonpublic personal information of residents of New York State (including businesses in other states) to have security safeguards for their data.** The Act also expands on what information must be protected. It expands on current State laws for reporting data breaches & HIPAA breaches, including fines in excess of $200,000, as well as legal liability imposed by the State. The Act

explicitly states that compliance with a security framework implemented under GLBA or HIPAA (as well as other frameworks) will satisfy security safeguard requirements.

More information on the new Act and its requirements can be found here and to our article in Accounting Today.

By being GLBA compliant, your business will have a robust data security plan required to meet your IRS and NYSHIELD security & compliance needs.

NYDFS

For financial institutions in New York State *regulated by the New York Department of Financial Services (such as banks, trusts, insurance companies, mortgage brokers and firms,* and others), another regulation requires a risk assessment with specific standards as well as special security policies and procedures: the NY Department of Financial Services Cybersecurity Rule (NYDFS Cyber). The State passed this law in 2017. Financial Institutions in NY State must comply with it. The Government hasn't provided any enforcement action until recently. For financial institutions with 10 or more employees, or other factors, continuous security monitoring or bi-annual vulnerability scanning and annual penetration testing may also be required, among other safeguards and reporting requirements.

CPAs and Tax Preparers are generally exempt from this requirement (as they are generally not regulated by the NYDFS, see this article for more info regarding CPAs and NYDFS). They may have clients who require compliance with this rule and must have a properly written and implemented security plan, to service those clients.

For more information on NYDFS and the recent action, see here.

How Securex Can Help you Meet All The Above Requirements in One Package

At **Securex**, we use our training and experience in cybersecurity & risk assessment (as well as our expertise in healthcare security & compliance) to provide your firm with the framework needed to comply with GLBA.

(It should be noted that companies such as accountants, which store client information relevant their healthcare clients, may also need to comply with healthcare security regulations, such as HIPAA/HITECH.)

So that you can comply with the GLBA Safeguards Rule, IRS requirements, NYSHIELD and to help you comply with NYDFS requirements, Securex provides our **GLBA Information Security Package** to help you meet and exceed your compliance & security requirements. This package includes:

- GLBA Risk Assessment report using information gathered from detailed questionnaires and interviews. To collect the information, we provide an interview with a key member of your management and your IT support. Intake meetings can range from one to two hours. We provide the intake questionnaire ahead of time, to help save time. (The interview covers whether specific security safeguards were implemented in your organization or not. Based on the information provided, we will document additional risk information accordingly. For example (for illustrative purposes only, actual questions may vary), you may be asked to check off whether ALL of the firm's customer information has its "data-at-rest" encrypted (data stored on individual systems or computers). If only some computers or systems have their data-at-rest encrypted, the response is left blank (you may add comments nearby if needed). On the documentation which discusses risk information, we flag that you did not implement the safeguard of encrypting customer information while the data is at rest.
- A written GLBA Information Security Program that incorporates the GLBA documentation requirements, Risk Assessment documentation, and additional security & compliance recommendations.
- The list of the recommended safeguards, as well as a list for your IT.
- A list of instructions and a follow-up meeting on the use of the documents we provide. The guidance also covers information on Risk Management. In the event of a compliance investigation, the Government may ask for documentation of "Risk Management." You do not fully implement a new security plan in a day. Risk Management is a process by which you plan the implementation of new security safeguards, giving priority to those issues that contain the most risk. The instructions also cover how to document your Risk Management (such as time projections for installing new software and safeguards, etc.). For example, a risk with a high priority should have a timeline (which you decide) for how long it will take to implement the safeguard (in a reasonable amount of time). An example would be (for illustrative purposes only), is that a high risk, such as unencrypted computers/laptops, will take two weeks to correct.)
- Next, you collaborate with your IT, so you can conveniently implement your Information Security Program in a way that suits your specific needs (see below for more information). If you do not have an IT support team, ask us about additional options.

More Information About Our Services and Our Security and Compliance Philosophy

- As mentioned above, the actual legal text of GLBA provides several general guidelines for the required Risk Assessment and Information Security Plan, and it encourages organizations to tailor a security program to the size and scope of their business. Also mentioned above is that the FTC, IRS, and other sources also provide security recommendations to help comply with the GLBA Safeguards Rule. At Securex, our philosophy for compliance is straightforward. When the Government requires compliance, rather than following the exact legal wording of the law (which is often open to interpretation) we encourage you to follow the Government's recommendations, as well as other expert advice. At Securex, we draw on these recommendations to help you meet and exceed your compliance needs while maintaining robust security. We want you to have reasonable security to protect against reasonably anticipated threats.
- Our GLBA Information Security Package allows you to meet your baseline requirements for the required GLBA Risk Assessment and Information Security Plan documentation while receiving valuable expert recommendations for your organization's entire security infrastructure. **We use auditing standards which are used by the Government in their own audits of organization's GLBA Risk Assessment and compliance**. We want you to have reasonable security to protect against reasonably anticipated threats.
- We provide a comprehensive plan (which may vary based on each organization), which you can implement and customize as needed, based on your business size. We generally keep the recommendations vendor-neutral, that way you can work with your IT support or internally to find the best fit for you. At times we provide some vendor-specific recommendations. For example:
    - When we recommend monitoring for computer security updates (such as Windows updates), we keep that vendor-neutral because, for a firm with 1-10 computers, this may be done differently than how a firm should do it with dozens of computers. Your IT support can then help you implement the best fit for you.
    - The fact that not all computers which store customer information are encrypted, we may flag as a risk. Failure to encrypt customer information sent over a network, we also flag as a risk. We recommend encryption of customer information sent over a network, we provide a few options and may specify a few software names. You can decide what the best fit for your needs in your circumstances is. We put all our recommendations into your Information Security Plan, as procedures. We also put in the various other GLBA requirements into your plan. That way, your Information Security Plan is ready-to-go.

Additional Services for Tax Professionals and Financial Institutions

- To help single-person practitioners, we provide a simple template option as a smaller package which they can use to assess and document their own risks and safeguards and to develop their written security plan. However, our services are primarily targeting firms that have someone to go to for their IT needs (e.g., installing new software, etc.). we also can provide the option of IT remediation as well for those that do not have their own IT implement their security plan.
- For the GLBA Information Security Package, we use information about your security, which your organization provides to us through intake interviews and questionnaires. Some larger firms may prefer a more in-depth, independent assessment.
- To help meet and exceed your security and compliance requirements, we offer an additional package. In this other package, we independently gather your security information and assess your entire security infrastructure through our investigative techniques.
- We use onsite scanning of your networks and computers, in-depth interviews with your staff, investigate individual computers, and may even perform onsite visits to assess your security environment. Using these methods, we gather the necessary information to evaluate your security posture in even greater detail and can provide even more specific and targeted recommendations. We present our findings in clear and concise reports.
- You gain valuable security information and solid proof of your compliance when you see what is going on in your individual computers and networks.
- The scans and investigations can uncover external network vulnerabilities in your firewall, security patching, access anomalies, and more.
- An in-depth security assessment relevant to your organization's security and compliance is especially important for firms with several employees, computers, and facilities.
- For financial institutions in New York State *regulated by the New York Department of Financial Services (such as banks, trusts, insurance companies, mortgage brokers and firms,* and others), another regulation requires a risk assessment with specific standards as well as special security policies and procedures: the NY Department of Financial Services Cybersecurity Rule (NYDFS Cyber). The State passed this law in 2017. Financial Institutions in NY State must comply with it. The Government hasn't provided any enforcement action until recently. For financial institutions with 10 or more employees, or other factors, continuous security monitoring or bi-annual vulnerability scanning and annual penetration testing may also be required, among other safeguards and reporting requirements. CPAs and Tax Preparers are generally exempt from this requirement (as they are generally not regulated by the NYDFS, see this article for more info regarding CPAs and NYDFS). They may have clients who require compliance with this rule and must have a properly written and implemented

security plan, to service those clients. For more information on NYDFS and the recent action, see here.

- Another regulation requiring you to perform a specific type of risk assessment is the HIPAA Security Rule. CPAs that are considered "HIPAA Business Associates" of healthcare providers need to comply with the HIPAA Security Rule.
- Options for maintenance of your security and compliance through online training, simulated "phishing attacks" and more.

Visit us at securexcyber.com or schedule a free consultation here, to get started on your path to security + compliance, with Securex.

The Security Experts ™
