

# CODE42 + GLBA

Code42's Insider Risk Management solution, Incydr, supports customer compliance with GLBA requirements, giving organizations the critical data risk detection and response capabilities needed to protect their customers' private information. Incydr provides a powerful data protection foundation that contributes to a long-term GLBA compliance strategy and prepares organizations to meet evolving regulations and complex compliance requirements.

## What is GLBA?

The Gramm-Leach-Bliley Act (GLBA) is also known as the Financial Modernization Act of 1999. It is a United States federal law that requires financial institutions to explain how they share and protect their customers' private information. GLBA applies to all businesses, regardless of size, that are "significantly engaged" in providing financial products or services. This includes, for example, mortgage brokers, payday lenders, nonbank lenders, real estate appraisers, and professional tax preparers.

The GLBA requires financial institutions ensure the confidentiality and security of customers' nonpublic personal information (NPI), which includes Social Security numbers, credit and income histories, credit and bank card account numbers, phone numbers, addresses, names, and any other personal customer information received by a financial institution that is not public.

## What are the possible penalties for non-compliance?

- Financial institutions found in violation face fines of \$100,000 for each violation
- Individuals in charge found in violation face fines of \$10,000 for each violation
- Individuals found in violation can be put in prison for up to 5 years

## What are some of the key requirements?

GLBA expands customer rights for financial institutions, including:

- Customers' NPI must be secured against unauthorized access
- Customers must have the ability to opt out of NPI sharing with other 3rd parties
- User activity must be tracked, including any attempts to access NPI
- Entities must create a written information security plan describing the program to protect their customers' NPI

## GLBA utilizes the “Safeguards Rule” to outline primary data protection requirements for organizations, including:

- Designate one or more employees to coordinate its information security program
- Design and implement a safeguards program and regularly monitor and test it
- Select service providers that maintain appropriate safeguards. Make sure your contract requires them to maintain safeguards and oversee their handling of NPI
- Identify and assess the risks to NPI in each relevant area of the company’s operation and evaluate the effectiveness of the current safeguards for controlling these risks
- Institutions must pay special attention to employee management and training, information systems, and security management

## How does Code42 enable our customers to comply with GLBA?

Code42 enables customers to comply with GLBA and protect customer NPI. See how your employees move data across vectors — Incydr detects web upload, USB, Airdrop and cloud sync activity for all employees. Employees do not need to be on VPN for their file activity to be monitored. Trusted activities are filtered out to reveal only the activities that indicate potential risk to data — so you can take action quickly to mitigate risk and noncompliance and avoid associated penalties and other impacts, including reputational damage.

All data transferred to Code42 is encrypted at rest and in transit. Data is not used by Code42 for any purpose other than as agreed upon for the provision of our products and services.

Code42’s Master Services Agreement incorporates an Information Security Addendum (ISA), which includes Code42’s commitments to safeguard your data.

[READ THE ISA](#)



Corporate Headquarters  
100 Washington Avenue South  
Minneapolis, MN 55401  
612.333.4242  
code42.com

Code42 is the Insider Risk Management leader. Native to the cloud, Code42 Incydr rapidly detects data loss, leak, theft and sabotage as well as speeds incident response – all without lengthy deployments, complex policy management or blocking employee productivity. With Code42, security professionals can protect corporate data and reduce insider threats while fostering an open and collaborative culture for employees. Backed by security best practices and control requirements, Code42’s Insider Risk solution is FedRAMP authorized and can be configured for GDPR, HIPAA, PCI and other regulatory frameworks.

More than 50,000 organizations worldwide, including the most recognized brands in business and education, rely on Code42 to safeguard their ideas. Founded in 2001, the company is headquartered in Minneapolis, Minnesota, and backed by Accel Partners, JMI Equity and Split Rock Partners. Code42 was recognized by Inc. magazine as one of America’s best workplaces in 2021. For more information, visit [code42.com](http://code42.com). (WP2110307)