



Cybersecurity Requirements for NY Licensed Agents Key Dates for 2020 Filings

Certification of Compliance Due - April 15, 2020

All Covered Entities and licensed persons who are not fully exempt from the Cybersecurity Regulation are required to submit a Certification of Compliance no later than April 15, 2020 (extended from February 15, 2020), attesting to their compliance for the 2019 calendar year.

[Click Here](#) for detailed instructions from the Department of Financial Services (DFS) on how to file a Certification of Compliance.

Notices of Exemption - You Do Not Need to File Again if You Filed in 2019

Any DFS regulated entity or licensed person who filed a Notice of Exemption previously will not need to refile a Notice of Exemption. If there has been changes, then the entity or individual should update their status accordingly.

Note: Even if you filed a Notice of Exemption, you might have to submit a Certification of Compliance to demonstrate that you were in compliance with the portions of the regulation that apply to you.

Reminder: Any DFS regulated entity or licensed person that was entitled to an exemption should have already filed an Initial Notice of Exemption prior to February 15, 2019. Professional Group Plans sent information via email with details and instructions on how to file prior to this deadline (See page 2 for our Cybersecurity Background Summary).

To Submit Your Cybersecurity Regulation filings sign in to the DFS Cybersecurity portal and choose the appropriate option: <https://myportal.dfs.ny.gov/web/cybersecurity>

The screenshot displays the NYS DFS CyberSecurity 23 NYCRR 500 Regulation portal. At the top, there is a navigation bar with links for Services, News, Government, and Local. Below this is the Department of Financial Services logo and the text 'SECURE PORTAL'. The main content area is titled 'NYS DFS CyberSecurity 23 NYCRR 500 Regulation' and is divided into three columns: Exemption, Compliance, and Event. Each column contains a description of the action and a 'Begin' button. The Exemption section includes a list of actions: File new Notice of Exemption, Amend previously filed Notice of Exemption, and Terminate previously filed Notice of Exemption. The Compliance section includes the action 'Submit a Certification of Compliance'. The Event section includes the action 'Submit Notice of a Cybersecurity Event'. At the bottom of the page, there is a 'HELP AND INFORMATION' section with links for 'Portal Help' and 'Visit Us'.



Cybersecurity Requirements for NY Licensed Agents Background Information and Exemption Details

Cybersecurity Regulations became effective on March 1, 2017 and provide that any individual or nongovernmental partnership, corporation, branch, agency, association or other entity operating under a license under New York insurance laws (among others) ("Covered Entities") are required to formally assess their cybersecurity risks and maintain a cybersecurity program to address such risks. Under these Regulations, Covered Entities are required to comply with a number of detailed requirements. **Smaller entities and individuals are entitled to file for a limited exemption eliminating some of the more complex, costly requirements.**

Cybersecurity Regulations Limited Exemptions

Covered Entities are entitled to a limited exemption if the Covered Entity has:

- Fewer than 10 employees, including any independent contractors, of the Covered Entity or its affiliates located in New York or responsible for business of the Covered Entity; **OR**
- Less than \$5,000,000 in gross annual revenue in each of the last three fiscal years from New York business operations of the Covered Entity and its affiliates; **OR**
- Less than \$10,000,000 in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all affiliates.

What are covered entities still required to do with a limited exemption?

- Establish and maintain a cybersecurity program and written cybersecurity policy;
- Limit user access privileges to information systems;
- Conduct a periodic risk assessment of information systems;
- Implement written policies and procedures to ensure security of information systems that are accessible by third party service providers;
- Limit data retention; and
- Report any cybersecurity events to DFS within 72 hours.

Covered Entities that already comply with HIPAA's Security Standards may already be performing the above requirements.

For More Information visit the Cybersecurity Resource Center:

https://www.dfs.ny.gov/industry_guidance/cybersecurity

Contact Your PGP Representative if you have any questions.

LI: 631.951.9200 • NYC: 212.840.4949 • NJ: 908.276.9399 • CT: 203.413.2740

www.pgpbenefits.com