CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
CENTER FOR CONSUMER INFORMATION & INSURANCE OVERSIGHT

# Protecting Consumer Information and Practicing Cybersecurity Hygiene

Agents and brokers play a critical role in protecting consumer personally identifiable information (PII) in the Health Insurance Marketplace®. As cybersecurity breaches are a growing threat for small businesses, this tip sheet provides practical guidance for agents and brokers to implement cybersecurity hygiene in their daily work.

## Tips for Cybersecurity Hygiene

Cybersecurity hygiene is a set of practices that should be performed regularly to maintain the security of your devices and networks to keep sensitive client data secure and protect it from theft and attacks. These practices include:

- **Backups:** Regularly back up important files to a separate, secure location that would remain safe in case of a cybersecurity breach.
- **Awareness & Education:** Learn how to avoid phishing scams and how to prevent malware attacks. Agents and brokers should also share this information with their employees.
- **Encryption:** Use encryption to protect sensitive data in files and on devices.
- **Password hygiene:** Maintain good password hygiene by requiring unique passwords, employing password managers, reviewing the frequency with which passwords are updated, and using multi-factor authentication (MFA) to make it more challenging for hackers to gain unauthorized access. Since long passwords are stronger, agents and brokers should use passwords that are 8 to 12 characters long.
- **Patch management:** Always keep software up to date and install security patches on both company-owned devices and personal devices used for work.
- **Security software:** Install security software to defend systems against malware such as ransomware, spyware, worms, rootkits and Trojans. Also, run regular scans to flag unusual activity.

## Best Practices for Protecting Personally Identifiable Information (PII)

In Person:

- Secure hard-copy consumer consent forms in a locked location.
- During consumer appointments, utilize private spaces to ensure privacy.
- Dispose of PII in a manner consistent with FFM rules and retention requirements.

Electronic:

- Do not send or forward emails with PII to personal email accounts.
- Do not use unauthorized mobile devices to access PII.
- Store PII securely in a password-protected file on a password-protected computer to which only authorized individuals have access.

Paper:

- Ensure any originals of consumers' records are returned before they leave your office and only make copies for yourself or others if necessary to carry out required duties.
- Keep a supply of manila folders to give to consumers with their documents inside to keep them in one place and shield the contents from view.