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

Best Practices for Cybersecurity: *Encryption*

Because agents and brokers handle consumers' personally identifiable information (PII) daily, it's important that they encrypt files containing PII so that any unauthorized individual cannot access them. Encryption can be utilized on any device, including computers, laptops, smartphones, and tablets, and it's a best practice to encrypt any file containing PII.

Protecting PII with Encryption

Agents and brokers should protect consumers' PII that is stored on their devices. This can be done by:

- Being aware of what information is stored on your devices and who has access to it.
- Deleting any unnecessary PII from your devices.
- Encrypting PII that is kept on your devices or sent via email, over a wireless network, or through the internet.
- Using encryption when remote access is used on your device (e.g., if a company troubleshoots your software remotely).
- Overwriting the data so unauthorized individuals won't be able to access the information.
- For more information, see this resource.

Encryption Best Practices

- If you are the owner of an agency, train your employees on how to properly encrypt sensitive data on their devices.
- Ensure you know how to encrypt the data on your devices.
- Ensure the encryption is configured correctly. If it isn't, the information will not be protected.
- Have a plan in mind if encryption fails or PII is leaked.

Encryption Best Practices

Encryption is essential because it adds an extra layer of security to PII. You can assure your clients that you are protecting their information and that their files and data will be securely stored on your device.

Encryption and Ransomware

Although encryption is an important tool agents and brokers can use to protect information, cybercriminals can use ransomware to encrypt your files and make it impossible for you to access them. Ransomware can be transmitted to your device by downloading, clicking on, or visiting a malware-embedded link, attachment, or website. Victims of ransomware typically won't know their files have been encrypted maliciously until it has already happened.

To avoid this malicious encryption, agents and brokers should:

Always keep their systems, software, and applications up to date.	Download antivirus software onto their devices.	Regularly back up their data.

For more information on ransomware and how to avoid it, see this resource.

This communication was printed, published, or produced and disseminated at U.S. taxpayer expense. If you have any questions or concerns, please contact the Agent/Broker Email Help Desk at FFMProducer-AssisterHelpDesk@cms.hhs.gov.

Updated: June 2023