Remote Employee/Virtual Agent Compliance Checklist

The checklist below will assist you in remaining compliant should you or your agency make the decision to work remotely or switch to virtual appointments.

Computers and/or tablets that store, send or enter client data and personal information

- ☐ Must be fully encrypted
- ☐ Must be password protected
- ☐ Must have up to date virus protection
- ☐ Must have security firewalls in place
- ☐ You must logout every time you walk away from the device
- ☐ Under no circumstance should you save passwords on your computer

Email Protocols

- ☐ Your email must be encrypted, or password protected if any personal information is being sent

Phone Systems

- ☐ Call forwarding can be a beneficial tool should your office or agency need to transition to remote protocol
- ☐ Cloud based phone systems are ideal for this type of setup.

Writing Business Virtually or Non-Face to Face - Reminders and Tips

- ☐ Find out what carriers allow non-face to face enrollment
- ☐ Make sure you have a Permission to Contact from your clients, remember, no cold calling on MA or PDP plans
- ☐ You are free to call on your current clients
- ☐ Acquire a SOA virtually on products and plans it is required for
- ☐ A full presentation is still required to take an online application
- ☐ If mailing a paper application, MAPD or PDP application must be submitted to the carrier within 24 hours after agent has received it back from the client