BlueOrange Alert:
Guidance for Patients & Residents for Telehealth Services

GUIDANCE FOR PATIENTS/RESIDENTS AS RECIPIENTS OF TELEHEALTH SERVICES

Patients/Residents who are the recipients of telehealth services from their providers should consider the following to ensure that their personal health information is protected as best as possible, especially during this COVID-19 public health emergency. Certain HIPAA provisions have been waived temporarily by the government; therefore, it is especially important that patients/residents do their best to protect their mobile devices (smart phones, tablets, and computers) as well as their private conversations during these telehealth visits.

Some things to consider during the scheduled telehealth visit:

1. Ask your provider if they are using a HIPAA-compliant technology platform, such as:
   - Skype for Business
   - Updox
   - VSee
   - Zoom for Healthcare
   - Doxy.me
   - Google G Suite Hangouts Meet
2. If the application is not HIPAA-compliant, make sure it is **non-public facing**, such as:
   - Apple FaceTime
   - Facebook Messenger video chat
   - Google Hangouts video
   - Skype
   - Zoom (provided it has privacy settings including a unique meeting ID and password)
3. **Do not** use any public-facing products such as Facebook Live, Twitch or TikTok, etc.
4. Find a quiet, private space to have your visit, even if you are at home in case the provider wants to discuss particularly sensitive information or look at your body.
5. Ask your provider at the end of the visit to e-prescribe any medication and verify the pharmacy where you will pick it up.
6. If there is anything you think you need the provider for in person, as them about it and they will use their professional judgement to keep you safe and healthy.
7. When your visit is over, make sure you completely close out of the application from your device.

In addition, be aware there are a lot of scams and hackers trying to prey on vulnerable people during this crisis – so these are good precautions to take in general:

Specifically:

- Malicious text messages are promising information about coronavirus to trick users and penetrate your smart device.
- Phishing attacks are using subjects such as "Covid-19", "Coronavirus" "WHO," and "Community" to trick the user to open the email.
- Files dubbed as Coronavirus information (PDF, MP4, and Docx) are carrying malware and ransomware.
- More remote users and more internet use leave more opportunities for the bad guys.

What can you do to protect yourself?

1. If you don't have antivirus on your smartphone, now is the time to get it—and be careful opening texts.
2. Take a trust-but-verify approach to all emails.
3. Do not open attachments unless you are sure you know the sender.
4. Don't click on links from external emails.
5. Never give your personal information to anyone online (or over the phone) and beware of fake web sites that look like the real thing.
6. Be careful about any emails that have the following words in the subject or body of a message: as "Covid-19," "Coronavirus" "WHO," and "Community".
7. Be on the lookout for emails pretending to be from the CDC or related to federal economic stimulus checks.
8. Beware of fraudulent web sites offering to sell personal protective gear or treatments for COVID-19.
9. Do not click on fraudulent links to make donations to supposed COVID-19 foundations.
10. Always verify the source of emails and texts by opening a new browser or calling from your phone back to the organization.

About BlueOrange Compliance:

BlueOrange Compliance specializes in assisting healthcare organizations navigate HIPAA and HITECH privacy and security requirements. Complex, ever-changing healthcare regulations and increasing risks make it difficult for organizations to stay in front of emerging cyber threats. As a single source, we equip every client with affordable, practical, comprehensive privacy and security solutions, including multiple sources of information to help manage risk. Our clients have peace of mind knowing they are compliant and prepared for potential breaches and adverse audits. BlueOrange Compliance provides this alert for educational purposes only without warranty and specialized advice should be sought about your specific circumstances.