

Welcome to a special spring edition of CBH Compliance Matters!

We are experiencing exceptional and remarkable times as we deal with the COVID-19 pandemic. We want to thank all of our providers and agency staff who continue to provide much needed services to our members. To our members, we and our provider network remain committed to ensuring that you have access to needed, high-quality behavioral health care during these challenging days.

We think it is important to pause from our normal Compliance Matters material and provide the most up-to-date information possible about potential scams and schemes to protect our members, staff, and providers. While we are amazed at the resiliency and flexibility of our staff, providers, and members, we also know that a small number of individuals around the world will look to exploit the anxiety and uncertainty of this crisis. The following articles will provide our best guidance right now on how to avoid those potential pitfalls. Before we start, we also wanted to assure our providers and members of a few key pieces of information.

- CBH and CBH Compliance remain operational 24/7 via telecommuting
- CBH Compliance has suspended all new audit activities through at least the end of April 2020
- We have extended the deadline for submitting staff rosters to at least May 1, 2020
- Our Compliance hotlines remain open and staffed as normal (more information in the pages that follow)
- We will continue to provide updates as we have them on the efforts of our partners at the Federal and State levels in easing access to needed services
- We have paused recoupments of previously identified overpayments until further notice

Our goal is to allow our providers to devote their full attention to meeting the needs of our members. If you have any questions or requests, please reach out to us by contacting the Compliance e-mail address at CBH.ComplianceContact@phila.gov or by calling our Compliance hotline at 800-229-3500.

KNOW YOUR SOURCE

First things first: always know your source.

Before we get into a discussion of what we've heard about emerging fraud schemes aimed at exploiting the COVID-19 crisis, let's cover some basics. Before acting on or forwarding information, you should always know your source. Only rely on information from trusted sources. Granted, we may be a bit a biased, but one of your first stops should be CBH's website. Right now, we are providing daily updates on the [COVID-19 landing page of our website](#). Our Communications Department is working hard to make sure that you have access to the latest information that we have.

Questions about the virus itself?

Trust sites like the [CDC](#), the [Pennsylvania Department of Health](#), or the [Philadelphia Department of Public Health](#). Their COVID-19 pages contain information about the virus at all levels.

Did Aunt Jane post news about COVID-19 on her Facebook page?

Verify that information by going to a trusted and knowledgeable source, like those linked above. Nothing against Aunt Jane, but you wouldn't go to the CDC website about that awesome family recipe for chocolate chip cookies, right? By the same token, you should rely on specialized resources like the CDC for COVID-19 information.

Questions about where to access behavioral health services right now?

Many of our providers have, in the interest of safety to both their staff and our members, restricted access to their physical, brick-and-mortar locations. Our advice is to call your provider or our Member Services department for help. Our providers are [listed here on our website](#), and an up-to-date list of provider operational changes can be found [on our coronavirus landing page](#) under "Operational Changes of Treatment Providers." Our Member Service Representatives are available 24/7 by calling 888-545-2600. While we are working hard to ensure access and continuity of care, there are bound to be challenges, and our Member Service Representatives are the best choice to assist you.

Finally, do you or your members worry about receiving telehealth and using up limits on calls or data on your phone?

Many telecommunication providers have announced an ability to waive overages and/or service suspensions during the current COVID-19 crisis. We encourage you to check with your telephone and/or data provider for the latest information and reach out to their customer service representatives if additional help is needed. This [PCWorld article](#) details some of the unprecedented actions already reported to have been taken by these companies, but, again, verify with your own company.

So, remember: always verify that your information is coming from trustworthy sources.

COVID-19 FRAUD SCHEMES

Throughout history, times of stress and anxiety have been shown to bring out both the best and worst in people. Disasters, both human-related and natural, tend to lead to increases in blood donations, for example.¹ Unfortunately, these periods also bring out the small minority of people looking to profit from the fear and anxiety of the time.² Those of us involved in the detection and prevention of fraud often talk about the fraud triangle. This theory, from criminologist Donald Cressey, states that for fraud to occur, three elements must be present: opportunity, pressure/motivation, and rationalization. While rationalization is typically thought to be internally driven, times of widespread stress and anxiety can provide boosts to both opportunity (individuals relax typically normal safety measures searching for answers/resources) and pressure/motivation (shortages, layoffs, financial stress).

We are currently in the midst of an unprecedented time. Western societal norms such as handshakes and going to work are being, at least temporarily, set aside in favor of social distancing and telecommuting. These changes bring with them anxiety and stress that can lessen our normal defenses and increase opportunities for fraudsters. Make no mistake, there are individuals around the globe looking to exploit this crisis. We are already hearing about early schemes related to the COVID-19 pandemic. We want to share as much information as possible to keep you safe from these predators. The first part

¹ See [this story from the World Health Organization](#) or [this story from the Washington Post](#).

² See, for instance, [this ABC story about a 9/11 scandal](#), or [this Washington Examiner article about years of Hurricane Katrina fraud](#).

of remaining safe is to get your information from trusted sources. Important steps to help guide you to appropriate sources were provided earlier in this issue. How many of you checked out even one of the links cited in this article?

Here are some current fraud schemes related to COVID-19 and simple steps to help protect yourself from them.

Coronavirus Phishing Attacks

Cyber fraudsters have employed phishing attacks for some time as a method to gain entry into otherwise secure systems. Phishing does not involve long, foggy-memory nights listening to your favorite jam band. Rather, it is the use of electronic communications (email or texts primarily) that mask fraudulent communication by appearing to come from legitimate senders. Examples in the COVID world include fraudsters sending emails that appear to be from sources like the CDC or WHO. They then redirect you to a site where you are asked to enter email addresses and passwords, for example. Once you enter the information, it is stored for later use by the fraudsters to hack into accounts.³

How do you avoid falling for a phishing attack?

1. Be suspicious of **any** unsolicited emails or text messages. Did you ask for help from the CDC? No? They are likely not going to “cold call” you via email.
2. Make sure your anti-virus protections are up to date, just in case.
3. Trust your source! If in doubt, don’t click on the link. Instead, go to the legitimate site and check for information there. If still in doubt, click on a link **on the trusted site**—often titled “Contact Us”—for further clarification.
4. Trust your gut and use common sense. If you happen to click on the link, and you are asked for things like Social Security Numbers, email addresses, or passwords, think “why would they need that information?” or “would the CDC really expect me to enter that information here?” The answer for those questions is “they don’t need or want that information, they are busy fighting a literal virus” and “no, they would not.”

³ See an example [here from Mimecast](#) and [here from Kaspersky](#).

5. You can also hover over links on most computers and it will show you the actual address that you are going to be directed to. This is a last step, in general, since reputable sites are not going to ask you to click on links and enter personal information—so just don't click. Go straight to the source through a trusted site.

Bogus COVID-19 Related Products

These go back at least as far as snake oil salespeople. The snake oil salesman was a staple in the Old West if you believe spaghetti westerns. Certainly, there were more than a few peddlers of the latest cure-all that amounted to nothing more than water or alcohol. In today's world, snake oil salespeople don't ride into your life on a stage coach but rather on TV, through emails, or in bogus social networking claims. Already we are seeing the Federal Trade Commission having to issue warning letters for products making unproven claims.⁴ Keep these things in mind:

1. As of today (March 29, 2020) there are no cures or vaccines for COVID-19. That is likely to change in short order, maybe even by the time this gets published. You will hear about it through trusted media sources, and it will be distributed through trusted medical networks (doctors, pharmacies, etc.).
2. COVID-19 related testing is increasing by the day. But again, as of this writing, testing is limited for those in the most need and with a physician's examination.⁵ If we arrive at a time when testing is more widely available, information will be shared through trusted means of communication, not via an unsolicited email or late night advertisement.
3. Got a hot tip on a stock for this small penny stock company in Pocatello that has developed a foolproof vaccine from spuds? Yeah, hard pass. Be wary of folks attempting to pressure you into purchases of stocks with claims like "it can't lose" or "guaranteed return on investment." Be extra wary when they are unsolicited "tips."
4. If you see something that claims to have results that seem too good to be true, they probably are. Avoid them. And, better yet, report them. Our friends in the Department of Justice have [a page set up to](#)

⁴ See this [press release from the FDA](#) or this [Consumer Reports report](#).

⁵ Members must still be seen/screened by a health care professional, per the [Pennsylvania Department of Health](#).

[talk about fraud related to COVID-19](#) and contact information where you can report suspected COVID-19 fraud.

COVID-19 Related Price Gouging

Technically, this isn't necessarily fraud. But, in most jurisdictions, it is still illegal. We have heard reports of hoarding of necessary supplies and individuals attempting to resell them at steep mark-ups to profit from the perceived shortage.⁶

The solution for this is both simple and difficult. Don't buy products at inflated prices. I know that is easier said than done in many cases, but demand fuels this behavior. If we can eliminate the demand, the price gougers will be left with inventory they can't unload, and the behavior will eventually extinguish itself. You should also report suspected price gouging. Most—if not all—states have units set up to handle cases of price gouging. In Pennsylvania, report it to the Attorney General at pricegouging@attorneygeneral.gov.

Business Operations-Related Fraud

With so many staff working from home, in many cases for the first time, our typical protections from fraud are stressed. The FBI is concerned that business emails are at risk for widespread abuse and issued a warning early in March.⁷ Be wary of emails that appear to be from coworkers asking for a check to be cut immediately, for passwords to be shared, or to set up payment accounts for new employees. Trust your gut again. And, even though you're working from home, pick up the phone and call your CEO, HR manager, and/or CFO to verify before acting. Any communication that seems to place undue pressure for a quick response should be viewed as suspect even in the best of times. For our providers, make sure your supervisors and executives are staying in contact with line staff. Hopefully, you already had a strong compliance plan, but review it to make sure the new remote work environment has not created any previously unknown weaknesses.

These are truly remarkable times. Remain vigilant and don't allow stress and anxiety to beat your common sense. "Trust but verify," more than ever, should be words to live by. And make no mistake, I have spent some time giving you a glimpse into the schemes that are being perpetrated by a small group. Most people are looking to help, and they are all around you. From

⁶ See [this WFAA article](#) or [this Grand Forks Herald article](#).

⁷ Read [a Secure World article about it here](#).

the health care professionals, to our Member Service and Provider Relations Representatives, to free Samosas for health care workers in England.⁸

CBH Compliance is here to help in any way we can to fight and avoid COVID-19-related fraud. If you have questions or concerns, please let us know by calling our hotline at 800-229-3050 or by email at CBH.Compliancehotline@phila.gov.

⁸ Read [a CNN article about it here](#).