In This Issue:

Page 1: CISA's *Protect Myself from Cyber Attacks*
Page 2: Relevant CARF standards
Page 3:
Page 4: Required training for December, Professional Accomplishments, and HR Corner by Kacie Enyart

MARIC Healthcare

PROFESSIONAL DEVELOPMENT

DECEMBER 2021

VOL.8 ISSUE 3: PROGRAM CYBERSECURITY: HOW TO USE TECHNOLOGY SAFELY BY: ANN JAMIESON

DECEMBER ISSUE: PROGRAM CYBERSECURITY: HOW TO USE TECHNOLOGY SAFELY

PROTECT MYSELF FROM CYBER ATTACKS

U.S. Federal Cybersecurity and Infrastructure Security Agency

The Department of Homeland Security plays an important role in countering threats to our cyber network. We aim to secure the federal civilian networks, cyberspace and critical infrastructure that are essential to our lives and work.

The National Cybersecurity and Communications Integration Center's (NCCIC) mission is to reduce the risk of systemic cybersecurity and communications challenges in our role as the Nation's flagship cyber defense, incident response, and operational integration center. Since 2009, the NCCIC has served as a national hub for cyber and communications information, technical expertise, and operational integration, and by operating our 24/7 situational awareness, analysis, and incident response center.

The following preventative strategies are intended to help our public and private partners proactively look for emails attempting to deceive users into "clicking the link" or opening attachments to seemingly real websites:

- **Never click on links in emails.** If you do think the email is legitimate, whether from a third party retailer or primary retailer, go to the site and log on directly. Whatever notification or service offering was referenced in the email, if valid, will be available via regular log on.
- **Never open the attachments**. Typically, retailers will not send emails with attachments. If there is any doubt, contact the retailer directly and ask whether the email with the attachment was sent from them.
- **Do not give out personal information** over the phone or in an email unless completely sure. Social engineering is a process of deceiving individuals into providing personal information to seemingly trusted agents who turn out to be malicious actors. If contacted over the phone by someone claiming to be a retailer or collection agency, do not give out your personal information. Ask them to provide you their name and a call-back number. Just because they may have some of your information does not mean they are legitimate!

Other practical tips to protect yourself from cyberattacks:

- **Set secure passwords and don't share them with anyone**. Avoid using common words, phrases, or personal information and update regularly.

- **Keep your operating system, browser, anti-virus and other critical software up to date**. Security updates and patches are available for free from major companies.
- **Verify the authenticity of requests from companies or individuals by contacting them directly**. If you are asked to provide personal information via email, you can

independently contact the company directly to verify this request.

- **Pay close attention to website URLs**. Pay attention to the URLs of websites you visit. Malicious websites sometimes use a variation in common spelling or a different domain (for example, .com instead of .net) to deceive unsuspecting computer users.
- **For e-Mail,** turn off the option to automatically download attachments.
- **Be suspicious of unknown links or requests sent through email or text message**. Do not click on unknown links or answer strange questions sent to your mobile device, regardless of who the sender appears to be.

Stop. Think. Connect.
The Stop.Think.Connect. Campaign is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online.

Tips
Most people use passwords that are based on personal information and are easy to remember. However, that also makes it easier for an attacker to guess or "crack" them.

Although intentionally misspelling a word ("daytt" instead of "date") may offer some protection against dictionary attacks, an even better method is to rely on a series of words and use memory techniques, or mnemonics, to help you remember how to decode it.

For example, instead of the password "hoops," use "IlTpbb" for "[I] [l]ike [T]o [p]lay [b]asket[b]all." Using both lowercase and capital letters adds another layer of obscurity. Your best defense, though, is to use a combination of numbers, special characters, and both lowercase and capital letters. Change the same example we used above to "Il!2pBb." and see how much more complicated it has become just by adding numbers and special characters.

RELEVANT CARF STANDARDS

1.J. Technology

Description
Guided by leadership and a shared vision, CARF-accredited organizations are committed to exploring, and, within their resources, acquiring and implementing technology systems and solutions that will support and enhance:

- Business processes and practices
- Privacy and security of protected information
- Service delivery
- Performance management and improvement
- Satisfaction of persons served, personnel and other stakeholders

1.J.2. The organization implements a technology and systems plan that:
a. Is based on:
(1) Its current use of technology and data
(2) Identification of gaps and opportunities in the use of technology
b. Includes:
(1) Goals
(2) Priorities
(3) Technology acquisition
(4) Technology maintenance
(5) Technology replacement
(6) Resources needed to accomplish goals
(7) Timeframes

1.J.3. The organization implements policies and procedures in the following areas:
a. Acceptable use
b. Backup/ recovery
c. Business continuity/ disaster recovery
d. Security, including:
(1) Access management
(2) Audit capabilities
(3) Data export and transfer capabilities
(4) Decommissioning of physical hardware and data destruction
(5) Protection from malicious activity
(6) Remote access and support
(7) Updates, configuration management, and change control.

1.J.5. The organization provides documented training to personnel:
a. On cybersecurity
b. On technology used in performance of their job duties
c. Including initial and ongoing training

STANDARDS FOR SERVICE DELIVERY USING INFORMATION AND COMMUNICATION TECHNOLOGIES (TELEHEALTH STANDARDS)

Description
Depending on the type of program, a variety of terminology may be used to describe the use of information and communication technologies to deliver services; e.g., telepractice, telehealth, telemental health, telerehabilitation, telespeech, etc. Based on the individual plan for the person served, the use of information and communication technologies allows providers to see, hear, and/or interact with persons served, family/support system members, and other providers in remote settings. The use of technology for strictly informational purposes, such as having a website that provides information about the programs and services available, is not considered providing services via the use of information and communication technologies.

The provision of services via information and communication technologies may:

- Include services such as assessment, monitoring,

prevention, intervention, follow-up, supervision, education, consultation, and counseling.

- Involve a variety of professionals such as case managers/ service coordinators, social workers, psychologists, speech-language pathologists, speech-language pathologists, occupational therapist, physical therapist, physicians, nurses, rehabilitation engineers, assistive technologists, and teachers.

- Encompass settings such as:

o Hospitals, clinics, professional offices, and other organization-based settings.
o Schools, work sites, libraries, community centers, and other community settings.
o Congregate living, individual homes, and other residential settings.

1.J.6. The organization implements written procedures:
a. That address:
1) Consent of the person served.
2) Audio recording, video recording, and photographing the person served.
3) Decision making about when to use information and communication technologies versus face-to-face services.
b. To confirm that all necessary technology and/or equipment is available and functions:
1) Prior to the start of service delivery.
2) As needed throughout services.
3) At the:
a) Originating site.
b) Remote site.

1.J.7. As appropriate, personnel who deliver services via information and communication technologies receive competency-based training on equipment:
a. Features.
b. Setup.
c. Use.
d. Maintenance.
e. Safety considerations.
f. Infection control.
g. Troubleshooting

Intent Statements
For service delivery to be effective, personnel are trained to use equipment and technology to deliver services and to guide persons served, members of the family/ support system, and others in the remote setting on its use.

Infection control addresses equipment used at the originating site and the remote site. For example:

- Equipment that touches any part of the body or is used to look into someone's eyes, ears, or mouth is properly sanitized between each use.

- The person served and family members are instructed in proper handwashing technique; shielding coughs and sneezes; and the use, if necessary, of gloves or masks to minimize risks associated with sharing equipment.

- When the person served is using a computer at a school or library, the keyboard, mouse, and headset are cleaned appropriately before they are used.

1.J. 8. As appropriate, instruction and training are provided:
a. To:
1) Persons served.
2) Members of the family/ support system.
3) Ohers.
b. Equipment:
1) Features.
2) Setup.
3) Use.
4) Troubleshooting.

1.J.9. Service delivery includes:

a. Personnel to provide assistance with accessing services provided by the organization.
b. Based on identified need:
1) An appropriate facilitator at the site where the person served is located.
2) Modification to:
a) Treatment techniques.
b) Equipment.
c) Materials.
d) Environment of the remote site, including:
(i) Accessibility.
(ii) Privacy.
(iii) Usability of equipment.

1.J.10. Prior to the start of each session:

a. All participants in the session are identified.
b. The organization provides information that is relevant to the session.

Examples: Information may be shared on the credentials of the provider, structure and timing of services, recordkeeping, scheduling, contact between sessions, privacy and security, potential risks, confidentiality, billing, rights and responsibilities, etc.

1.J.11. The organization maintains equipment in accordance with manufacturers' recommendations.

1.J.12. Emergency procedures address the unique aspects of service delivery via information and communication technologies, including:

a. The provider becoming familiar with the emergency procedures of the remote site if the procedures exist.
b. Identification of local emergency resources, including phone numbers.

When the person served is located at an organization or a community setting, the provider becomes familiar with the

procedures of that setting in the event there is an emergency involving the person served. In the absence of emergency procedures for the setting where the person served is located, or when the person served is at home, the provider has immediate access to emergency contact information for the person served and information on local emergency resources, including their phone numbers..

MANDATORY TRAINING

There are two required trainings this month:

1. **Telemental Health Practice**

Only for counselors providing telehealth counseling or planning to in the future.
Access at:
https://ce4less.com/Telemental-Health-Practice-Psychologist-Ceu
The certificates must be submitted to your Program Director who will send them after collecting all to Wendy@marichealth.com.

2. For All Employees:

Cybersecurity training will be provided by Albert Rios, Maric Healthcare's Director of Professional Development and Justin Fisher, Maric Healthcare's Information Technology Coordinator. The training is titled "Cybersecurity Training", and this is the training agenda:

- Overview of cybersecurity
- The risks of cyberattacks
- Explore how we combat cybersecurity at an organization-level
- Best practices to protect yourself and your organization from social engineering attacks
- How to identify a phishing attack

Please use this link to register for one of the three offerings of this live webinar: https://bit.ly/3k21cCZ.

When you register you will see a notification "This webinar is offered several times". Select the date and time that works best for you." It will give you three choices, all in Central time:

1. Wednesday, December 8: 11:30AM to 1:00PM
2. Thursday, December 9: 10:00AM to 11:30AM
3. Wednesday, December 15, 12:00PM to 1:30PM

You will need to scroll down to find and select the date you prefer.

All employees must register themselves and attend this live webinar. This is mandatory.

A sign-in sheet will be provied by your Program Director, who will submit all completed sign-in sheets to Wendy.

Human Resource Corner

END OF THE YEAR PREP

As the end of 2021 quickly approaches, this is a great time to take a few moments to make sure all your personal information is correct in Paycor. With tax forms and W2s set to be delivered early next year – please take some time to review the following information:

- Mailing address
- Phone numbers
- Email addresses

This is also a great time to review your Tax Status and Withholdings for 2022.

Consider reviewing the following:

- Marital Status
- Dependent Withholdings
- Deductions
- Extra Withholdings

These changes can all be made in Paycor. Addresses and contact information can be updated under "Personal Information," and tax information can be updated under "Compensation" and "Taxes." If you prefer, you may also email HR at Kacie.enyart@marichealth.com to make updates.
From everyone here at the Maric office – we wish you all a very safe and happy holiday season!

Kacie Enyart, SHRM-CP
Human Resource Generalist

Professional Accomplishments

Please join me in congratulating our colleagues for their amazing professional accomplishments:

In Brentwood, TX, Alicia Trapp has earned her LCDC (Licensed Chemical Dependency Counselor)**!**

Congratulations! Way to go!!!!