Region 7 Healthcare Coalition

80 Livingston Blvd, Ste. 106
Gaylord, MI 49735
O: (989) 748-4975 24/7 Line: (989) 732-5141

Guidance and Links Newsletter

For Healthcare Partners

October 2022, Issue No. 2

Guidance and Links Newsletter 1

COALITION UPDATES 3

Communication Drills 3

MICHIGAN DEPARTMENT OF HEALTH AND HUMAN SERVICES (MDHHS) UPDATES 4

FEMA UPDATES 4

Federal Emergency Management Agency (FEMA) Releases Local Elected and Appointed Officials Guide: Roles and Resources in Emergency Management - October 18, 2022 4

CMS UPDATES 5

ASPR UPDATES 5

CENTERS FOR DISEASE CONTROL AND PREVENTION (CDC) UPDATES 5

COVID-19 UPDATES 6

IMMUNIZATIONS 6

HOSPITAL 6

EMS 6

LONG TERM CARE 7

MDHHS Long Term Care Facility COVID Response Call 10/18/22 7

DIALYSIS 7

Dialysis Meeting Schedule 2022-2023 7

BEHAVIORAL & MENTAL HEALTH 7

ADULT FOSTER CARE & HOMES FOR THE AGED 8

PEDIATRIC CHAMPIONS- HOSPITAL & EMS 8

Midwest EMSC Pediatric Champion Symposium 8

Pediatric Champion ED Office Hours Continue with Another EIIC Presentation -- October 25, 2022 9

Securing Resources During a Disaster: A Pediatric Dashboard Orientation and Test Drive – October 25, 2022 9

SPECIAL PATHOGENS 10

Infection Prevention and Control: Incorporating Lessons Learned in Managing Special Pathogens -- November 7, 2022 10

BURN SURGE & MEDICAL SURGE UPDATES 11

VOLUNTEERS AND MICHIGAN VOLUNTEER REGISTRY UPDATES 11

CYBERSECURITY 11

Cybersecurity Awareness Month 2022: Using Strong Passwords and a Password Manager 12

VMware vCenter Server Bug Disclosed Last year Still Not Patched 13

All Windows Versions Can Now Block Admin Brute- Force Attacks 14

HC3 Sector Alert: Microsoft Exchange Zero-Day Actively Exploited in Attacks 14

HC3 Sector Alert: Abuse of Legitimate Security Tools and Health Sector Cybersecurity 15

Adobe Releases Security Updates for Multiple Products 15

Microsoft Releases October 2022 Security Updates 16

Microsoft October 2022 Patch Tuesday Fixes Zero- Day Used in Attacks, 84 Flaws 16

Customer Guidance for Reported Zero-Day Vulnerabilities in Microsoft Exchange Server 17

Multiple Vulnerabilities in Google Chrome Could Allow for Arbitrary Execution Code 17

SUPPLY CHAIN 18

↑ Back to Table of Contents

Personal Protective Equipment and Personal Protective Technology Product Standardization for a Resilient Public Health Supply Chain : A Workshop 18

RESOURCES / RESEARCH / OTHER **19**

2023 AmeriCorps Funding Opportunity Available - January 4, 2023 19

IMPORTANT DATES **19**

UPCOMING EVENTS & TRAINING **20**

Region 2 North Healthcare Coalition 2023 Regional Conference - February 15, 2023 20

Contact Us **20**

COALITION UPDATES

Communication Drills

UPDATED: Region 7 Healthcare Coalition Communication Drills are scheduled as follows:

	Frequency	**Dates & Time**
All Partners	Biannual	1st Wednesday of November 2022 and May 2023

↑ Back to Table of Contents

MICHIGAN DEPARTMENT OF HEALTH AND HUMAN SERVICES (MDHHS) UPDATES

FEMA UPDATES

Federal Emergency Management Agency (FEMA) Releases Local Elected and Appointed Officials Guide: Roles and Resources in Emergency Management - October 18, 2022

FEMA recently released the Local Elected and Appointed Officials Guide: Roles and Resources in Emergency Management. This guide provides an executive-level introduction to emergency management concepts and principles for local senior officials and identifies local senior officials' roles and responsibilities for incident emergency management before, during, and after disasters. The guide also explains how to access additional resources. FEMA will host a series of 60-minute webinar sessions to provide an overview of the guide and associated quick reference guide and checklists. The sessions will include facilitated discussions with stakeholders. Advance registration is required. To register, click on the link to one of the following sessions.

- Register – 10:00 AM ET Tuesday, October 18

↑ Back to Table of Contents

CMS UPDATES

ASPR UPDATES

CENTERS FOR DISEASE CONTROL AND PREVENTION (CDC) UPDATES

↑ Back to Table of Contents

COVID-19 UPDATES

IMMUNIZATIONS

HOSPITAL

EMS

↑ Back to Table of Contents

LONG TERM CARE

MDHHS Long Term Care Facility COVID Response Call 10/18/22

The next LTC COVID Response Call is scheduled for Tuesday, October 18 from 10-11:30am.

Dial-in: 1-888-251-2949

CODE: 7323681#

- Long Term Care Facility COVID Response Call 10.18.22.pdf

DIALYSIS

Dialysis Meeting Schedule 2022-2023

- ~~September 27, 2022- 10-11 am~~
- December 27, 2022- 10-11 am (will likely reschedule due to holiday)
- March 28, 2023- 10-11 am
- June 27, 2023- 10-11 am

BEHAVIORAL & MENTAL HEALTH

↑ Back to Table of Contents

ADULT FOSTER CARE & HOMES FOR THE AGED

PEDIATRIC CHAMPIONS- HOSPITAL & EMS

Midwest EMSC Pediatric Champion Symposium

Nov 3 is an EMS focused afternoon – There are EMS CEs for Nov 3

- Direct registration link: https://us06web.zoom.us/webinar/register/WN_kyRliSssR26V8mWwIzmdNw

Nov 4 is an ED focused afternoon – There are CEs for nurses and physicians for Nov 4

- MUST first create Children’s Hospital of MN education account; then sign up for the symposium
- https://cmn.education.childrensmn.org/clinician-education/login
- The third PDF is instructions for physicians and nurses to create an account with Children’s of MN to receive the free CEs and locate the symposium within the system.

↑ Back to Table of Contents

Ideally, both opportunities can be shared with our State leaders and PECCs (Pediatric Champions). This event went very well last year, and thus we expanded to include education and CE opportunities for ED providers this year based on that!

Very excited to be able to offer this to our providers and champions!

Click here to download the Nov. 2 flyer

Click here to download the Nov. 3 Flyer

Click here to download the Account Instructions

Pediatric Champion ED Office Hours Continue with Another EIIC Presentation -- October 25, 2022

HPP and the EMS-C programs have worked in partnership with the EMSC Innovation and Improvement Center (EIIC) on a series for the Pediatric Office Hours breaking down the Pediatric Disaster Preparedness Toolkit for hospitals. (https://emscimprovement.center/education-and-resources/toolkits/pediatric-disaster-preparedness-toolbox/). The October topic is Pediatric Surge Capacity. If you are interested in joining these educational sessions, please register at the following link: https://www.surveymonkey.com/r/MIpedchecklist you will then be sent a link to the presentation.

EIIC MIseries_savedate.pdf

Securing Resources During a Disaster: A Pediatric Dashboard Orientation and Test Drive – October 25, 2022

Below is the flyer for the Region V for Kids virtual demonstration and user-level exercise of the EMResource Pediatric Dashboard. The dashboard provides a single source of in-patient, pediatric resource information. Participants from Illinois, Indiana, Michigan, Minnesota, Ohio or Wisconsin interested in pediatrics,

↑ Back to Table of Contents

emergency management, disaster response and/or medical data systems to participate.

Securing Resources Save the Date ne .pdf

SPECIAL PATHOGENS

Infection Prevention and Control: Incorporating Lessons Learned in Managing Special Pathogens -- November 7, 2022

After nearly three years responding to the COVID-19 pandemic, hospitals and other healthcare facilities have learned many lessons about the management of special pathogens and essential infection prevention and control practices. The U.S. Department of Health and Human Services (HHS) Administration for Strategic Preparedness and Response's Technical Resources, Assistance Center, and Information Exchange (ASPR TRACIE) and the National Emerging Special Pathogens Training and Education Center (NETEC) invite you to learn more about some of those lessons. Speakers will share their perspectives on how our approach to outbreaks has changed since the pandemic began. They will address issues such as infection prevention for healthcare workers and patients and mitigating disease spread. Speakers will also highlight newly developed tools and resources. This webinar will take place November 7 at 2:00 pm ET. Register today!

↑ Back to Table of Contents

BURN SURGE & MEDICAL SURGE UPDATES

VOLUNTEERS AND MICHIGAN VOLUNTEER REGISTRY UPDATES

CYBERSECURITY

↑ Back to Table of Contents

Cybersecurity Awareness Month 2022: Using Strong Passwords and a Password Manager

This week’s Cybersecurity Awareness Month theme is using strong passwords and a password manager. Connie LaSalle, a senior technology policy advisor for U.S. Department of Commerce's National Institute of Standards and Technology(NIST), offers four specific ways to mitigate your cybersecurity risks online while discussing the importance of adopting strong passwords.Read more about her interview on NIST.gov.

Mitigating risk, whether you are an individual or a business, comes down to a few buckets of action that translate across contexts

- understand your environment (e.g., people their preferences and needs, assets for which you are responsible or upon which you are reliant, etc.)
- understand risks to your environment
- take action to manage risks based on their relevance to your environment and your priorities
- have a backup plan when something unexpected happens

Just like in the physical world around us, we should all be aware of our surroundings online. Social engineering attacks, phishing, mis/disinformation campaigns, scams, and many other nefarious activities are increasingly sophisticated and common, so being a skeptical consumer of information is generally a good rule of thumb. For groups and individuals who may be at high risk of targeted attacks or harassment, both online and offline, it is especially important to monitor your digital footprint and be conscientious about which technologies (and people) you decide to trust with your information. Read more about her interview on NIST.gov.

↑ Back to Table of Contents

VMware vCenter Server Bug Disclosed Last year Still Not Patched

VMware informed customers today that vCenter Server 8.0 (the latest version) is still waiting for a patch to address a high-severity privilege escalation vulnerability disclosed in November 2021. This security flaw (CVE-2021- 22048) was found by CrowdStrike's Yaron Zinar and Sagi Sheinfeld in vCenter Server's IWA (Integrated Windows Authentication) mechanism, and it also affects VMware's Cloud Foundation hybrid cloud platform deployments. Attackers with non-administrative access can exploit it to elevate privileges to a higher privileged group on unpatched servers. VMware says this flaw can only be exploited by attackers using a vector network adjacent to the targeted server as part of high-complexity attacks requiring low privileges and no user interaction (however, NIST NVD's CVE-2021-22048 entry says it's exploitable remotely in low-complexity attacks). VMware has evaluated the bug's severity as Important, meaning that exploitation results in the complete compromise of confidentiality and/or integrity of user data and/or processing resources through user assistance or by authenticated attackers. Although the company released security updates in July 2022 that only addressed the flaw for servers running the latest available release at the time (vCenter Server 7.0 Update 3f), it retracted the patches 11 days later because they didn't remediate the vulnerability and caused Secure Token Service (vmware-stsd) crashes while patching . VMware has determined that vCenter 7.0u3f updates previously mentioned in the response matrix do not remediate CVE-2021-22048 and introduce a functional issue. Learn more on bleepingcomputer.com.

↑ Back to Table of Contents

All Windows Versions Can Now Block Admin Brute- Force Attacks

Microsoft announced that IT adminstrators can now configure any Windows system still receiving security updates to automatically block brute force attacks targeting local administrator accounts via a group policy. Microsoft added this policy as they say Windows does not currently apply Account Lockout policies to "local administrators," allowing threat actors to repeatedly brute force passwords for these accounts. Microsoft revealed that the same account lockout policy is now available on any Windows system where the October 2022 cumulative updates are installed. "In an effort to prevent further brute force attacks/attempts, Microsoft is implementing account lockouts for Administrator accounts. Beginning with the October 11, 2022 or later Windows cumulative updates, a local policy will be available to enable local administrator account lockouts. Learn more on bleepingcomputer.com

HC3 Sector Alert: Microsoft Exchange Zero-Day Actively Exploited in Attacks

Researchers have identified two zero-day vulnerabilities in Microsoft Exchange Server 2013, 2016, and 2019 that are being actively exploited in the wild. Threat actors gain initial access through the following vulnerabilites: CVE-2022-41040, which is a Server-Side Request Forgery (SSRF) vulnerability, and CVE[1]2022-41082, which allows remote code execution (RCE) when PowerShell is accessible to the attacker. Microsoft Exchange is used in the Healthcare and Public Health (HPH) sector and therefore poses a significant threat. Review the Health Sector Cybersecurity Coordination Center (HC3) Sector Alert for more detail.

↑ Back to Table of Contents

HC3 Sector Alert: Abuse of Legitimate Security Tools and Health Sector Cybersecurity

Cobalt Strike is a commercial adversary simulation software that is marketed to red teams but is also stolen and actively used by a wide range of threat actors from ransomware operators to espionage-focused Advanced Persistent Threats (APTs). It was Created in 2012 by Raphael Mudge; one of the first widely-available red team frameworks. Cobalt Strike is used maliciously by several state-sponsored actors and cybercriminal groups, many of whom pose a significant threat to the health sector. Review the Health Sector Cybersecurity Coordination Center (HC3) Sector Alert for more detail.

Adobe Releases Security Updates for Multiple Products

Adobe has released security updates to address multiple vulnerabilities in Adobe software. An attacker can exploit some of these vulnerabilities to take control of an affected system.

CISA encourages users and administrators to review Adobe Security Bulletins and apply the necessary updates.

- Adobe Cold Fusion APSB22-44
- Adobe Acrobat and Reader APSB22-46
- Adobe Commerce and Magneto Open Source APSB22-48
- Adobe Dimension APSB22-57

↑ Back to Table of Contents

Microsoft Releases October 2022 Security Updates

Microsoft has released updates to address multiple vulnerabilities in Microsoft software. An attacker can exploit some of these vulnerabilities to take control of an affected
system.

CISA encourages users and administrators to review Microsoft’s October 2022 Security Update Summar y and Deployment Information and apply the necessary updates

Microsoft October 2022 Patch Tuesday Fixes Zero- Day Used in Attacks, 84 Flaws

For October 2022 Patch Tuesday, Microsoft released 84 patches which includes 11 categorized as critical and two zero-days, one of which is known to be actively exploited. The actively exploited zero-day is tracked as 'CVE-2022-41033 - it's a privilege escalation vulnerability in in the Windows COM+ (Windows component services) event service. The second zero day is tracked as 'CVE-2022-41043, which is a Microsoft Office Information Disclosure Vulnerability. There are still no patches released for the two recently-announced Exchange vulnerabilities (ProxyNotShell):

Learn more on bleepingcomputer.com

↑ Back to Table of Contents

Customer Guidance for Reported Zero-Day Vulnerabilities in Microsoft Exchange Server

Microsoft is investigating two reported zero-day vulnerabilities affecting Microsoft Exchange Server 2013, Exchange Server 2016, and Exchange Server 2019. The first one, identified as CVE-2022-41040, is a Server-Side Request Forgery (SSRF) vulnerability, and the second one, identified as CVE-2022-41082, allows Remote Code Execution (RCE) when PowerShell is accessible to the attacker. Currently, Microsoft is aware of limited targeted attacks using these two vulnerabilities. In these attacks, CVE-2022-41040 can enable an authenticated attacker to remotely trigger CVE-2022-41082. It should be noted that authenticated access to the vulnerable Exchange Server is necessary to successfully exploit either vulnerability. Microsoft Security Threat Intelligence teams have provided further analysis of observed activity along with detection and hunting guidance in a Microsoft Security blog. They are working on an accelerated timeline to release a fix. Until then, we're Microsoft is providing mitigations guidance below to help customers protect themselves from these attacks. Microsoft Exchange Online has detections and mitigations to protect customers. As always, Microsoft is monitoring these detections for malicious activity and will respond accordingly if necessary to protect customers. Learn more on microsoft.com

Multiple Vulnerabilities in Google Chrome Could Allow for Arbitrary Execution Code

Multiple vulnerabilities have been discovered in Google Chrome, the most severe of which could allow for arbitrary code execution. Google Chrome is a web browser used to access the internet. Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution in the context of the logged on user. Depending on the privileges associated with the user an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose

↑ Back to Table of Contents

accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights. Learn more on cisecurity.org.

SUPPLY CHAIN

Personal Protective Equipment and Personal Protective Technology Product Standardization for a Resilient Public Health Supply Chain : A Workshop

A planning committee of the National Academies of Sciences, Engineering, and Medicine will organize a public workshop to examine standards gaps related to personal protective equipment (PPE) and personal protective technology (PPT) and explore innovative approaches and technologies to update and streamline the U.S. standardization system for PPE and PPT in support of supply chain resiliency. In this context, PPT includes PPE worn by individuals (e.g., gowns, gloves, goggles, face shields, head covers, respirators, shoe covers, and surgical masks) and the technical methods (e.g., fit testing methods), processes, techniques, tools, and materials that support the development and use of PPE.

This workshop will provide the opportunity to engage and exchange knowledge and ideas among key stakeholders—including policy makers, manufacturers, users, and relevant technical contributors—and to facilitate discussion on opportunities to improve the effectiveness, safety, supply stability, and accessibility of PPE/PPT designed for use in U.S. health care settings, by critical infrastructure workers, and by the general public. Learn more about the workshop on nationalacademies.org.

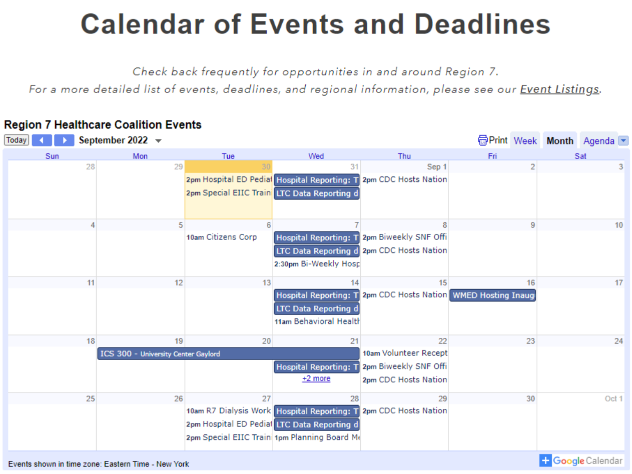
↑ Back to Table of Contents

RESOURCES / RESEARCH / OTHER

2023 AmeriCorps Funding Opportunity Available - January 4, 2023

AmeriCorps, in partnership with CDC, launched the 2023 AmeriCorps State and National Grants, a $400 million investment to engage new communities and individuals in public health, recruiting, and building a new workforce ready to respond to the nation's public health needs. Funding is open to nonprofit, faith-based, tribal, and community-based organizations; higher education institutions; and state, local, and territorial government entities, including local public health departments. Applications must be submitted by 5:00 PM ET on Wednesday, January 4, 2023. For additional guidance, contact AmeriCorpsGrants@cns.gov.

IMPORTANT DATES



Calendar of Events and Deadlines

Check back frequently for opportunities in and around Region 7.
For a more detailed list of events, deadlines, and regional information, please see our Event Listings.

Region 7 Healthcare Coalition Events

Sun	Mon	Tue	Wed	Thu	Fri	Sat
28	29	30 2pm Hospital ED Pediat 2pm Special EIIC Train	31 Hospital Reporting: T LTC Data Reporting d	Sep 1 2pm CDC Hosts Nation	2	3
4	5	6 10am Citizens Corp	7 Hospital Reporting: T LTC Data Reporting d 2:30pm Bi-Weekly Hosp	8 2pm Biweekly SNF Offi 2pm CDC Hosts Nation	9	10
11	12	13	14 Hospital Reporting: T LTC Data Reporting d 11am Behavioral Health	15 2pm CDC Hosts Nation	16 WMED Hosting Inaug	17
18	19 ICS 300 - University Center Gaylord	20	21 Hospital Reporting: T +2 more	22 10am Volunteer Recept 2pm Biweekly SNF Offi 2pm CDC Hosts Nation	23	24
25	26	27 10am R7 Dialysis Work 2pm Hospital ED Pediat 2pm Special EIIC Train	28 Hospital Reporting: T LTC Data Reporting d 1pm Planning Board Me	29 2pm CDC Hosts Nation	30	Oct 1

Events shown in time zone: Eastern Time - New York

All important dates can be found on the calendar on the Region 7 website. You can add or print these items directly from our calendar.
www.miregion7.com/events

The Region 7 HCC Events Calendar is subject to change. Please keep an eye open for any updates to calendar invites or check back on our website or email us for the current schedule.

↑ Back to Table of Contents

UPCOMING EVENTS & TRAINING

Region 2 North Healthcare Coalition 2023 Regional Conference - February 15, 2023

Region 2 North will be hosting the 2023 Regional Conference on February 15, 2023. Please see attached flyer for more details on the conference.

R2N_Conference_2023_Save_The_Date_Flyer.pdf

Contact Us

Region 7 Healthcare Coalition
80 Livingston Blvd, Ste. 106
Gaylord, MI 49735

24/7 Regional Medical Coordination Center
Activation Line: *989-732-5141*
Office: (989) 748-4975
Fax: (989) 748-4980
Regional Coordinator: C: (989)370-3583 E: rc@mir7hcc.com
Assistant Regional Coordinator: C: (989) 370-5013 | E: arc@mir7hcc.com
Website: https://www.miregion7.com/

Like and Subscribe for more on our Social Media Channels!

Follow us on Facebook! Follow us on LinkedIn!

Follow us on Instagram! Follow us on Twitter!

↑ Back to Table of Contents