Wyoming Hospital Association

February 25, 2022

Wyoming Hospital Association

News briefs

U.S. Declares Start of Russia's Invasion of Ukraine, Introduces Sanctions; "Cyber Shields Up," Says CISA

On February 22nd, President Biden announced that Russia's invasion of Ukraine has begun, with Russian military assets crossing into Ukraine's eastern provinces under the guise of a "peacekeeping" mission. The U.S. government and NATO allies immediately responded to Russia's actions with a series of economic and military sanctions. Now there is a concern that Russia may retaliate against the U.S. and allied nations with disruptive cyber-attacks in furtherance of its military and political objectives.

The American Hospital Association (AHA) is closely monitoring the potential for increased cyber risks to the U.S. health system stemming from the ongoing military operations in the Russia/Ukraine region. In light of previous attacks and potential threats, the Cybersecurity and Infrastructure Security Agency last week issued a related-and-rare cyber "Shields Up" warning to the U.S. private sector, including health care, based upon the increased cyberthreat posed by the Russian government.

As part of AHA's efforts, John Riggi, the association's national advisor for cybersecurity and risk, and a former senior executive in the FBI's cyber division, remains in close coordination with the FBI, CISA and the Department of Health and Human Services regarding related threats which may pose a risk to U.S. health care.

There are three concerns for the field, each stemming from the possibility that Russia/Ukraine geopolitical tensions result in increased Russian-borne cyberthreats:

- hospitals and health systems may be targeted directly by Russian-sponsored cyber actors;
- hospitals and health systems may become incidental victims of, or collateral damage to, Russian-deployed malware or destructive ransomware that inadvertently penetrates U.S. health care entities; and
- a cyberattack could disrupt hospitals' mission-critical service providers.

AHA's concerns are heightened by the Russian military's previous behavior of utilizing cyber weapons in support of military actions against Ukraine; such behavior ultimately inflicted disruptive collateral damage to the U.S. health care system, resulting in the U.S. government's 2020 indictment of six Russian military intelligence officers for the development and deployment of the destructive NotPetya malware three years prior. The malware was initially launched against Ukraine and subsequently spread globally, disrupting operations at a major U.S. pharmaceutical company, a major U.S. health care communications company and U.S. hospitals.

Hospitals and health systems should review the alerts and bulletins for guidance on risk mitigation procedures, including increased network monitoring for unusual network traffic or activity, especially around active directory. Additionally, it is important to heighten staffs' awareness of increased risk of receiving malware-laden phishing emails.

Geo-fencing for all inbound and outbound traffic originating from, and related to, Ukraine and its surrounding region may help mitigate direct cyber risks presented by this threat; however, it will have limited impact in reducing indirect risk, in which malware transits through other nations, proxies and third parties.

AHA also recommends that organizations identify all internal and third-party mission-critical clinical and operational services and technology; in doing so they should put into place four-to-six week business continuity plans and well-practiced downtime procedures in the event those services or technologies are disrupted by a cyberattack.

It is essential at this time to check the redundancy, resiliency and security of your organization's network and data backups, and ensure that multiple copies exist: off-line, network segmented, on premises and in the cloud, with at least one immutable copy.

It is also critical that a cross-function, leadership-level cyber incident response plan be fully documented, updated and practiced. This should include emergency communications plans and systems.

More information can be found at cisa.gov

2022 PAC Contributions

Barry Burkart
Tim Thornell

Critical Assess Hospital (CAH) Telehealth Guide

The Technical Assistance and Service Center (TASC) has partnered with the Northwest Regional Telehealth Resource Center (NRTRC) to produce an update to the Critical Access Hospital (CAH) Telehealth Guide. Recent federal guidance has been included in this edition. The updated guide provides information and guidance for assessing and implementing telehealth services for CAHs, including purchasing, staffing, maintenance, reimbursement, and reporting for outpatient services.

Additionally, the guide includes best practices and resources developed by subject matter experts (SME), technical consultants, and telehealth resource centers (TRCs). The objective is to provide Flex Programs and CAHs with a comprehensive guide that will allow them a singular point of reference for CAH telehealth standards with direct content and links to appropriate public and federal resources.

The guide can be found at the| National Rural Health Resource Center at https://www.ruralcenter.org/resource-library/cah-telehealth-guide.

Further questions and concerns can be directed to tasc@ruralcenter.org.

Well Advised March Webinars

Below are the webinars being presented in March by our endorsed vendor, Well Advised. These online sessions are designed to help you learn about important issues related to Medicare. The Well Advised presenters will answer your questions during these events. You may also submit questions in advance to info@well-advised.com.

1) Medicare Drug Plans: What You Need to Know, hosted by Dr. Robert Morris will be presented March 1, 2022 at 11:00 a.m. MT.
If you're eligible for Medicare or close to eligibility, it's time to start thinking about securing your prescription drug coverage. You'll also learn how to avoid late enrollment penalties, and how to get extra help with paying for your prescription medications.

2) Medicare and Mental Health Benefits, hosted by Dr. Robert Morris will be presented March 2, 2022 at 11:00 a.m. MT
Mental health conditions can be stressful on those who suffer with them. They may also be stressful on their family members. In this brief Well Advised live event presented by Dr. Robert Morris, we'll look at important issues related to mental health conditions and Medicare.

3) Medicare and Nutrition Therapy, hosted by Dr. Robert Morris will be presented March 15, 2022 at 11:00 a.m. MT
As we age, our risk for malnutrition rises. During this live online event hosted by Well Advised, Dr. Robert Morris will explore Why good nutrition is important for older adults; Tips for improving your nutrition; Who qualifies for medical nutrition therapy services that are covered by Medicare

4) How Medicare Special Needs Plans Work, hosted by Dr. Robert Morris will be presented March 22, 2022 at 11:00 a.m. MT
Medicare Special Needs Plans (SNPs) are types of Medicare Advantage plans that are designed for people with specific types of medical conditions. In this half-hour live event presented by Well Advised, we'll look at the issues that affect you, including:

5) First Time Enrollment in Medicare will be presented on March 29, 2022 at 11 a.m. MT

To register for any of these webinars, go to https://well-advised.com/medicarewebinars

For more information on WHA Resources, contact Josh Hannes at josh@wyohospitals.com or 307-632-9344