



Kentucky Hospital Research & Education Foundation Emergency Preparedness Update for July 2, 2019

KIPRC Releases New K-SURE Brief on Major Overdose Related Substances in KY

(Lexington) A new report from the Kentucky Substances Use Research and Enforcement (K-SURE) program is attached. This report looks at a combination of law enforcement and public health data for heroin, overall opioids, methamphetamine, cocaine, and fentanyl for the period from January 1, 2017 to December 31, 2018. Data tracked include citations / arrests for possession and trafficking, emergency department visits, hospitalizations, deaths, and tested lab submissions.

You can find the report (item #2), and a variety of other reports, at <http://www.mc.uky.edu/kiprc/pubs/overdose/index.html>.

93 Kentucky Hospitals Now Part of KY SOS!

KHA is excited to salute all 93 hospitals who have joined the Kentucky Statewide Opioid Stewardship (KY SOS) so far. Opioid stewardship involves a coordinated effort to reduce opioid-related harm by developing alternative means to manage pain and, when opioids are used, assuring that opioid prescribing and patient monitoring aligns with evidence-based guidelines. KY SOS will focus on reducing opioid overprescribing and improving safe opioid use by providing hospitals and health systems with education and resources on how to attain the highest level of performance on opioid stewardship.

KHA is proud to lead the KY SOS program as hospitals commit to working together to improve opioid stewardship collectively to combat the opioid epidemic in the commonwealth. To see the list: <http://www.newkyha.com/NewsBlog/tabid/550/EntryId/1573/93-Kentucky-Hospitals-Now-Part-of-KY-SOS.aspx>

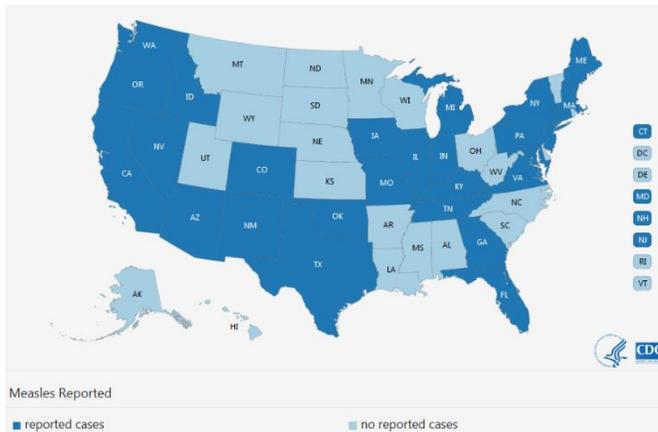
For information about how your hospital can join KY SOS, please contact **Donna Meador** at KHA (dmeador@kyha.com).

CBS: *Opioid lollypop* whistleblower story

See more: https://www.cbs.com/shows/whistleblower/video/0_y7pdBuMJ84nml86IMd7cajmhhvmSwZ/whistleblower-a-new-drug-dubbed-er-on-a-stick-was-100-times-more-powerful-than-morphine/

New cases lift US measles total to 1,095

([CIDRAP News Scan](#)) With 18 more infections recorded in the last week, the United States has seen 1,095 measles cases in 2019—the most cases in the United States since 1992 and since measles was declared eliminated in 2000.



Twenty-eight states have reported cases in 2019, a number unchanged for the past several weeks, according to a Centers for Disease Control and Prevention (CDC) update today. The CDC is tracking four ongoing outbreaks (3 or more related cases) in New York's Rockland County; New York City; Butte County, California; and Washington state.

"These outbreaks are linked to travelers who brought measles back from other countries such as Israel, Ukraine, and the Philippines, where large measles outbreaks are occurring," the CDC said.

As of Jun 24, New York City has noted 609 cases—13 more than the previous week—in a measles

outbreak that began last September in predominantly Orthodox Jewish communities in Brooklyn and Queens. [Jul 1 CDC update](#) & [Jun 24 NYC Health update](#)

CDC announces multistate *Salmonella* outbreak tied to papayas

Late last week the CDC announced a multistate outbreak of *Salmonella* Uganda infections linked to whole papayas imported from Mexico. The fresh fruit was sold in Connecticut, Massachusetts, New Jersey, New York, Pennsylvania, and Rhode Island.

A total of 62 people in eight states have become sickened after eating the fresh fruit. Twenty-three people have been hospitalized, but there have been no deaths. Illnesses began from Jan 14 to Jun 8, with a ramp-up seen since April. Of 21 people who were interviewed, the CDC said, 16 (76%) reported eating papayas before symptom onset.

In 2017, the CDC tracked another *Salmonella* outbreak tied to Mexican papayas, which resulted in at least 251 illnesses in 25 states and 2 deaths. **Jun 28 CDC [announcement](#)** & **Nov 6, 2017, CIDRAP [news scan](#)**

Bill for Safe Food Act seeks to Consolidate Federal Oversight.

Citing fragmented food safety oversight, which is split up between 15 federal agencies, two lawmakers want Congress to scrap the current system and the ineffective laws that regulate it. ([Food Safety News, 6/27/19](#))

**A New Way to Test for Signs of Consciousness
In Unresponsive, Brain-Injured Patients**

(NPR) Scientists are investigating a better test of consciousness in brain-injured patients. If it becomes widely available, it could help with agonizing decisions about withdrawal of life support.

Learn more: <https://www.npr.org/sections/health-shots/2019/06/27/736382903/a-new-way-to-test-for-signs-of-consciousness-in-brain-injured-patients>

----- *A collection of news stories from our vast sources you may find interesting* -----

How 'Human on a Chip' Technology Could Change the Way We Test Drugs

<https://news360.com/article/500170463>

Blood Pressure Medication Recall: How It Happened, What You Should Do

<https://news360.com/article/500510748>

Plants may be transmitting superbugs to people

<https://news360.com/article/500139124>

**Medical experts say it's harmful and full of bacteria,
but this group says when western medicine didn't work, their own urine did**

<https://www.9news.com/article/news/local/group-in-boulder-drinks-their-own-pee-for-health-benefits/73-80277854-becf-4e0e-bade-9b2e2745ed1e>

**Legal Weed Is A Danger To Dogs.
Here's How To Know If Your Pup Got Into the Pot**

<https://www.npr.org/732332846>

If You Can't Upgrade From Windows 7 to Windows 10, What Should You Do?

<https://news360.com/article/500059309>

Alexa Has Been Saving You Time: Now She Can Save Your Life

<https://news360.com/article/499955916>

...and this one freaked the kids out!

We're Growing Little Skull Horns Because of Our Phones

<http://newser.com/s276788>

[Preparing Your Community for the HSIN Technical Refresh](#)

(US DHS) Join DHS on Tuesday, July 16, 1 PM ET, for a special **HSIN Best Practices** Community of Excellence (CoE) session to learn what you need to know and do prior to the HSIN migration from SharePoint 2010 to 2016, which will bring new features and functionality to HSIN.

No registration is required; you may access the meeting room by clicking the HSIN Connect link below at the scheduled time.

Connect Room: <https://share.dhs.gov/hsinbpcoe>

Phone Number: 855-852-7677; 8403609#

What is HSIN? The Homeland Security Information Network (*HSIN*) is the Department of Homeland Security's official system for trusted sharing of Sensitive But Unclassified information between federal, state, local, territorial, tribal, international and private sector partners.

[What is HSIN?](#) · [How to Join HSIN](#) · [HSIN Videos](#) · [Critical Infrastructure](#)

Latest HSIN Advocate newsletter:

https://content.govdelivery.com/attachments/USDHSIN/2019/06/28/file_attachments/1239699/HSIN-Newsletter-July2019.pdf?page=4

New director named for Lexington VA Health Care System

(WTVQ) he Department of Veterans Affairs (VA) announced the appointment of Gregory W. Goins, FACHE, as Director of the Lexington VA Health Care System. Goins will oversee delivery of health care services to more than 38,000 Veterans and an operating budget of more than \$426 million. Most recently, Goins was the Medical Center Associate Director for the Cincinnati VA Medical Center, Cincinnati, OH.

Full story: <https://www.wtvq.com/2019/06/29/new-director-named-lexington-va-health-care-system/>

Hospital & Healthcare Cyber Threats

(R. Bartlett, KHREF) Given the high level of angst that many in healthcare collectively went through last week when we thought one of our own might have been hit again, only to be relieved that it was a false alarm probably triggered by a management team huddle to brief members on the need for things like back-ups, patching systems, email discipline, attachment vigilance, and cyber preparedness over the long holiday week we are in, I thought I would share some of the recent DHS Cybersecurity advisories and recommendations that came out over the last few weeks which likely prompted the personnel briefings. The threat from a cyber attack is real, and the consequences could be both costly and life-threatening, and so there is value in turning this into a "teaching moment".

NSA Releases Advisory on BlueKeep Vulnerability

(US DHS Cyber) -June 5 - The National Security Agency (NSA) has released a cybersecurity advisory for CVE-2019-0708—a vulnerability dubbed *BlueKeep*. Although Microsoft has issued a patch, potentially millions of machines are still unpatched and remain vulnerable.

The Cybersecurity and Infrastructure Security Agency (CISA) encourages users and administrators to review NSA's [news release](#) and [advisory](#), Microsoft Security Response Center's "[A Reminder to Update Your Systems to Prevent a Worm](#)," and [Microsoft Customer Guidance for CVE-2019-0708](#). CISA recommends patching the affected operating systems:

- [Windows 7, Windows Server 2008 R2, and Windows Server 2008](#)
- [Windows 2003 and Windows XP](#)

Link: <https://www.us-cert.gov/ncas/current-activity/2019/06/04/NSA-Releases-Advisory-BlueKeep-Vulnerability>

US DHS CISA Alert (AA19-168A)

Microsoft Operating Systems *BlueKeep* Vulnerability

(June 17) The Cybersecurity and Infrastructure Security Agency (CISA) is issuing this Activity Alert to provide information on a vulnerability, known as "*BlueKeep*," that exists in the following Microsoft Windows Operating Systems (OSs), including both 32- and 64-bit versions, as well as all Service Pack versions.

New *LooCipher* Ransomware Spreads Its Evil Through Spam

A new ransomware called *LooCipher* has been discovered that is actively being used in the wild to infect users. While it is not known exactly how this ransomware is being distributed, based on some of the files that were found, it is believed it is through a spam campaign.

LooCipher was first discovered by security researcher [Petrovic](#) and since then [BleepingComputer](#) and [Michael Gillespie](#) have observed multiple people being infected with this ransomware.

While not sure what kind of phishing campaign is spreading this ransomware, it is pushing a malicious Word document called `Info_BSV_2019.docm`.

When the ransomware is executed, *LooCipher* will create a file called `c2056.ini` on the Windows desktop where it will store the unique ID for the computer, a time limit when the key will allegedly expire, and a bitcoin address. This file states to not remove or alter it as it may interfere with the proper decryption of the ransomware.

Read more: <https://www.bleepingcomputer.com/news/security/new-loocipher-ransomware-spreads-its-evil-through-spam/>

If you wondered where I was last week?

(R. Bartlett, KHREF) I have had a few queries about what I was doing in Washington, DC, last week. I was invited to participate on a panel, representing the nation's hospital sector (which is a little scary in itself), to talk about Societal Resources and Services as part of the international Electric Infrastructure Security (EIS) Summit.

The theme of this tenth annual forum was on Resilience following a major disaster. The most recent disasters in the US, to include the major flooding in Middle America, punctuated the discussions. Compounding the discussion was that in today's society everything comes from everywhere, and that integration of systems is connecting supply chains worldwide. Sixteen nations, and over 200 leaders from major government groups and

businesses, participated in the program. Even has a few Senators and Congress members speak, along with members of the President's National Security Council.

The panels and discussions looked at what critical infrastructures and organizations were doing to prepare for a major "Black Sky" catastrophe, where there are still gaps that need to be addressed, and thoughts about key next steps. While people typically think of "Black Sky" as being a complete, massive power outage, it can be any major disaster that takes out multiple critical lifeline systems typically resulting in a cascading series of failures that compounds the seriousness of the event and threats to life.

The "500 pound gorilla" in the room was clearly cyber terrorism and cyber threats, accentuated by recent news stories about the US planting cyber code to stop the use of certain Iranian weapons, and other stories about how foreign governments (including ours) have crossed-pollinated cyber code in each other's critical control and communication systems.



In the picture: on the right is Lord Toby Harris of the UK House of Lords, Marcus Denison from the UK's largest food supplier, yours truly, David Lusk who is the Senior Manager for FedEx Global Operations, and Brooks Nelson who directs Global Resilience for the US Chamber of Commerce.

Some of my lead talking points about problems faced by hospitals and healthcare in a disaster included lessons learned from EarthEx 2018, which apply to so many major disasters, included: **power** (and the many dependencies); **water** (can't run a HC facility on little bottles of water for long); **fuel** (and the potential need to increase what we keep on-hand); **communications** (to request help and supplies, to access

EHR systems so often now "in the cloud", and to bill for services); **supplies** (medical and sustenance); **support for families and patients** - especially those who could be discharged but may have no place to go; demand for services exceeding capacity; and the inherent challenges around **the question of staying or abandoning the facility** - with all the potential risks and challenges associated. This leads to discussions of potential "**Crisis Standards of Care**", and **people on non-sustainable home health devices that typically overwhelm healthcare facilities** in a modern disaster.

There is an interesting new technology that our government and Israeli partners are working on called [BSX Emergency Communication and Coordination Systems](#). Essentially, it is an emergency communication and coordination system that (as I understood the discussion would be much like a "MESH" network), and can meet the needs of highly disrupted environments must be designed with a resilient, flexible "self-healing" system architecture. And given the many critical stakeholders that will need to be included, the system must be deployed broadly and across multiple sectors (to include healthcare), with hardware elements hardened against the full set of Black Sky hazards, and designed for at least a month of operation with no external power source.

But, in the end, I think the simplest take-away I heard that could have a tremendous impact on survival and sustainability, is a program that FedEx has implemented throughout its global system which involves over 400,000 employees. They have a philosophy that essentially says, "Preparedness begins with Prepared Employees, and Prepared Employees." They are using the [CERT \(Community Emergency Response Team\)](#) program to train all their employees and family members; and to develop CERT teams within their facilities. I challenged Mr. Lusk to use his base of global team members to turn outwards towards their communities, neighborhood associations, state and local emergency managers to help re-invigorate the development of CERT programs in the areas that they operate in.

HHS to Identify Healthcare Infrastructure Critical in Emergencies

Under legislation signed June 24 by President Trump, HHS is directed to work with other public health officials and private sector entities to identify the critical healthcare infrastructure needed to be maintained through an emergency or disaster.

Learn more: <https://hitinfrastructure.com/news/hhs-to-identify-healthcare-infrastructure-critical-in-emergencies>

Fisher-Price Recalls Infant Inclined Sleepers

Please be advised the Infant Inclined Sleeper has been recalled by Fisher-Price according to the Consumer Products Safety website at

https://www.cpsc.gov/Recalls?combine=INFANT+INCLINED+SLEEPER&field_rc_date%5Bdate%5D=&field_rc_date_1%5Bdate%5D=

Name of product: Inclined sleeper accessory included with all models of Fisher-Price Ultra-Lite Day & Night Play Yards

Hazard: Infant fatalities have been reported while using other inclined sleep products, after the infants rolled from their back to their stomach or side while unrestrained, or under other circumstances.

Remedy: Refund

Recall date: June 27, 2019

Units: About 71,000

News about this recall can be viewed at <https://www.wkyt.com/content/news/Fisher-Price-recalls-71000-inclined-infant-sleepers-511898131.html>

Hospitals can apply for ASPR funding to create pediatric disaster care centers

(AHA Today for July 1) Hospitals and health systems may apply through Aug. 27 for a portion of \$3 million in funding to create Pediatric Disaster Care Centers of Excellence to enhance pediatric care during public health crises, the Department of Health and Human Services' Office of the Assistant Secretary for Preparedness and Response [announced](#) last week. Applicants should have existing pediatric preparedness capabilities and the capacity to manage pediatric patients within their state and a self-defined multi-state region during a public health emergency, the agency said. [Proposed](#) in April, the centers will serve as pilot sites for the creation of a Regional Pediatric Disaster Care Network and identify issues, develop best practices, and demonstrate potential effectiveness and viability that could apply nationwide during public health emergencies and disasters, ASPR said.

Quarter of hospitals fail to comply with Leapfrog's never-event policy

(Modern Healthcare) About a quarter of hospitals fail to meet the Leapfrog Group's standards in addressing serious patient harm events should they occur, according to a new report. The analysis, [published](#) Thursday, found 74.5% of the more than 2,000 hospitals that participated in the 2018 Leapfrog Hospital Survey complied with all nine aspects of the group's never-event policy. Hospital compliance with the standard has hovered at or slightly below 80% since 2014.

Full story: <https://www.modernhealthcare.com/safety-quality/quarter-hospitals-fail-comply-leapfrogs-never-event-policy>

Johns Hopkins: Health Security Headlines

Extracts from [June 28, 2019](#) & [July 1, 2019](#)

[FDA Warns of Dangerous Cyber Vulnerabilities on Medtronic Insulin Pumps](#) (*The Hill*) The Food and Drug Administration warned patients and health care providers using certain types of insulin pumps of cyber threats involving the devices, with the pumps recalled due to vulnerabilities that could lead to negative health consequences for users.

[Experts Warn of Antimicrobial Resistance, Additional Threats to National Biosecurity](#) (*Homeland Preparedness News*) The Blue Ribbon Study Panel on Biodefense issued its bipartisan report, Biodefense, which assessed the state of biodefense in the country looking at strengths, weaknesses and vulnerabilities. The experts agreed that a range of factors affect our country's ability to fight these threats, including weakened or fragmented federal oversight, limited incentives for research and development, and a lack of preparedness at the local level to protect vulnerable populations.

[Flu Vaccine No Match Against Bug That Popped up Near End](#) (*STAT*) The flu vaccine turned out to be a big disappointment again. The vaccine didn't work against a flu bug that popped up halfway through the past flu season, dragging down overall effectiveness to 29%, the Centers for Disease Control and Prevention reported Thursday.

[Cryptosporidiosis Outbreaks — United States, 2009-2017](#) (*MMWR*) During 2009–2017, 444 cryptosporidiosis outbreaks, resulting in 7,465 cases were reported by 40 states and Puerto Rico. The number of reported outbreaks has increased an average of approximately 13% per year. Leading causes include swallowing contaminated water in pools or water playgrounds, contact with infected cattle, and contact with infected persons in child care settings.

[Ebola Cases Near 2,300 as Virus Returns to Earlier Hot Spots](#) (*CIDRAP*) The World Health Organization yesterday in its weekly profile of Ebola activity aired growing concern about case spikes in two Democratic Republic of the Congo areas—Mabalako and Mandima—that were hit hard when the outbreak began last August.

[Swine Fever Toll in China May Be Twice as High as Reported, Industry Insiders Say](#) (*Reuters*) As many as half of China's breeding pigs have either died from African swine fever or been slaughtered because of the spreading disease, twice as many as officially acknowledged, according to the estimates of four people who supply large farms. While other estimates are more conservative, the plunge in the number of sows is poised to

leave a large hole in the supply of the country's favorite meat, pushing up food prices and devastating livelihoods in a rural economy that includes 40 million pig farmers.

Supporting Heroes Educational Opportunities

Developed from our staff's unique experience with line-of-duty deaths (LODDs) in all three service fields (police, fire and EMS) across three states over many years, as well as studying LODD practices and traditions beyond our service area, Supporting Heroes now presents two classes to help leaders prepare for the unthinkable. Essentially, the classes are an effort to help survivors of future fallen heroes by helping public safety leaders prepare themselves and their agencies before tragedy strikes for the difficult tasks and decisions that will naturally follow.

While geared toward leaders, the classes are open to all who serve or would have a role in an agency's response to a line-of-duty death (such as chaplains, honor guard personnel, and more). The classes are also important for all who strongly believe in rendering 'ultimate honor for ultimate sacrifice.' Future classes are planned for funeral directors and news media personnel.

INTRODUCTION TO LINE-OF-DUTY DEATH (LODD) AND PUBLIC SAFETY OFFICERS' BENEFITS (PSOB)

is a four-hour class that clears up common misunderstandings about the differences between 'line-of-duty' and 'active-duty' death and provides a comprehensive overview of the federal LODD benefits (PSOB). This class was updated from a previous version to reflect recent changes to PSOB law and regulations and to complement ULTIMATE HONOR class content. *This class is now typically presented from 1:00 P.M. to 5:00 P.M. the day before ULTIMATE HONOR.*

ULTIMATE HONOR is an eight-hour class that examines the many ways honor can and should be rendered from the time of a hero's death going forward as well as common challenges. It is about much more than the high-profile ceremonial honors and emphasizes how honors are to be rendered, not because of who (if anyone) is watching, but because of what someone deserves. The most common response from participants is: *"You caused me to think about things I had never even dreamed of before!"*

More information and a schedule of upcoming classes is available at www.SupportingHeroes.org/Classes

Both classes are supported by a grant from Air Evac LifeTeam Foundation (see article below) and, since 9/20/2018, have been presented in 17 cities (across our three states and one in Maryland) to participants from 15 states.

Register Now for KHA's Conditions of Participation Seminars

If a CMS surveyor showed up at your hospital tomorrow, would you know what to do? Two upcoming KHA seminars will cover the 2019 changes in the CMS Hospital Conditions of Participation (CoPs). Hospitals have seen a significant increase in survey activity by CMS, so this is a great way to educate everyone in your hospital on all the sections in the CMS hospital manual especially ones that apply to their department.

CMS Hospital Conditions of Participation Made Easy 2019 - July 17-18

[Brochure & Online Registration](#)

Revised CMS CAH Conditions of Participation 2019: Ensuring Compliance - July 18-19

[Brochure & Online Registration](#)

If you have any questions, please contact **Sharon Perkins** at KHA (sperkins@kyha.com).

Save the Date
KSHE-IAHSS-KHA

2019 Healthcare Coalition Conference

September 17-19, 2019 | Kentucky International Convention Center | Louisville KY

Conference Hotel: Hyatt Regency Louisville

320 W Jefferson Street | Louisville, KY 40202

Hotel Room Rate \$209 - Reservations: call 502-581-1234

Group Name: Healthcare Coalition 2019

[Book Hotel Online](#)

[Sponsorship Levels & Benefits](#) [Available Sponsorships](#)

The KHREF Emergency Preparedness Update is assembled several times a week. When events make it necessary, the Update may be sent out several times a day to keep our hospital and the healthcare community advised on preparedness news and information. Most of this information is compiled from open sources, and where possible reference links will be provided. There is an archive of [Emergency Preparedness Updates available here](#). If you would like to added or deleted, or have something you would like to contribute to a future edition of the Emergency Preparedness Update, please contact rbartlett@kyha.com (include your current email address). The preparedness program for the Kentucky Hospital Association (KHA) and KHREF are supported by US DHHS ASPR HPP funds through a contract with Kentucky Public Health.