

North Carolina Society of Gastroenterology 2024 Annual Meeting



Preventing Legal Related Abdominal Pain- Severity, State Lines, Cyber and AI

Jason D. Newton
General Counsel
Curi



Joint Providership



American Society for
Gastrointestinal Endoscopy

Disclaimers

No conflicts, but I do work for my employer.

Hopefully helpful, but...

Not legal advice.

No endorsements.

No guarantees.

2023:

\$15m Bibb Co., GA

\$20.9m Essex Co., NJ

\$20m Middlesex Co., MA

\$40m Coles Co., IL

\$34m Baltimore Co., MD

\$9m Fulton Co., GA

\$19m Cook Co., IL

\$183m Phila., PA

2023:

\$10m Detroit, MI

\$26m Phila., PA

\$31.6m Michigan

\$13m King Co., WA

\$9m Baltimore, MD

\$20.2m West Palm Beach, FL

\$30m Dekalb Co., GA

\$32.7m Cook Co., IL

\$55.5m Cook Co., IL

\$220m Sarasota Co., FL

\$14m Phila, PA

Asset Protection Before It's Too Late

Get help on Asset Protection Strategies:

- Personal liability insurance aka “umbrella”
- Prenuptial and postnuptial agreements
- Joint tenants by entirety home ownership
- 401K and rollover IRAs
- Contributor IRAs (limitations apply)
- NOT necessarily inherited IRAs
- 529 plans (limitations apply)
- Asset protection trusts (varies by state)
- LLCs and corporations for business assets
- Life insurance & annuities (varies by state)



“Because that’s where the money is”

- + High-Risk Profession
- + High Income Profession
- + High Perception of Wealth
- = Need For Asset Protection

Online “Curbsides” (and a reminder about state lines)

“That which we call a rose [b]y any other
name would smell as sweet”

(It's telehealth, no matter what they say)

(Carefully) Read the Terms of Service- Liability Shifting

- You agree that any medical or professional services or advice (“Professional Advice”) you receive from any physician, specialist physician or other licensed provider (collectively, “Other Professionals”) through use of the Services is solely and exclusively for your own use in making decisions regarding the treatment and care of your patients...
- **You will use or rely upon any such Professional Advice in your sole and exclusive discretion and professional judgment.**
- You agree that **You have all responsibility and liability for your use or reliance upon any Professional Advice received from Other Professionals through the Services,** and **no such Other Professional bears any part or portion of any responsibility or liability for any Professional Advice rendered to you** or on behalf of any of your patients.

(Carefully) Read the Terms of Service- Disclaimer of Quality

TO THE FULLEST EXTENT PERMITTED BY LAW, THE **SERVICES ARE PROVIDED ON AN “AS IS” BASIS** AND VENDOR AND ITS AFFILIATES, THIRD PARTY LICENSORS, VENDORS, AND AGENTS HEREBY DISCLAIM ALL REPRESENTATIONS OR WARRANTIES, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, TITLE, NON-INFRINGEMENT, AND FITNESS FOR ANY PURPOSE. **VENDOR MAKES NO REPRESENTATION OR WARRANTY RELATED TO THE RELIABILITY, ACCURACY OR COMPLETENESS OF THE SERVICES, NOR DOES IT GUARANTEE THAT THE SERVICES WILL BE SECURE, TIMELY, UNINTERRUPTED, ERROR-FREE OR MEET SUBSCRIBER’S EXPECTATIONS.**

(Carefully) Read the Terms of Service- Unilateral Indemnification

You shall indemnify, defend and hold harmless us and our affiliates, directors, officers, employees, shareholders and agents, from and against any and all liabilities, claims, damages, injuries or losses arising out of or relating to your use of the Services (including any third party claims related to negative patient outcomes or medical malpractice with respect to the Services), the use or storage of the Data, your operations (including without limitation by any patient), your breach of the Agreement or compliance with any applicable law, including privacy, data security or data protection laws and regulations. This section shall survive the completion, expiration, termination or cancellation of this Agreement. Vendor may at its own expense participate in the defense and settlement of any claim with its own counsel, and you may not settle a claim without Vendor's prior written consent (not to be unreasonably withheld).

Due Diligence

- Is this the practice of medicine into the state of the subscriber?
- Is the consultant licensed in the state of the subscriber?
- Could you be subjected to suit in the consultant's state in a medical malpractice action?
- If you are serving as a consultant, does your MPL coverage protect you?
- If you are the subscriber, do you have a coverage gap if you use this service?
- What about documentation of the consult?
- **Practices should and must call their broker and underwriter *before* engaging with a service like this...**

Sept. 1, 2022

- Telemedicine visit
- Doctor in NC, patient in VA
- Bad outcome
- Med mal suit filed in VA Federal Court
- NC doctor is defendant in that case
- Tortious acts "took place" in VA
- Personal jurisdiction exists
- VA court denied motion to transfer to NC court



Med mal suit vs. NC doctor survives dismissal



Resource:

- Virtual Curbside Consult App Considerations Blog Post



What about REALLY Virtual “Consults”? ...Dr. ChatGPT is in



<https://www.thedailybeast.com/chatgpt-passed-the-us-medical-licensing-exam-will-it-be-your-future-doctor>

What about REALLY Virtual “Consults”? ...Dr. ChatGPT is in



<https://www.thedailybeast.com/chatgpt-passed-the-us-medical-licensing-exam-will-it-be-your-future-doctor>

What about REALLY Virtual “Consults”? ...Dr. ChatGPT is in

- Will your clinicians “consult” ChatGPT?
- Are they doing so already?
 - “That is exactly how we treated the patient”*
- Will patients?
- Will jurors?
- Will job candidates?

*<https://www.nytimes.com/2023/03/14/technology/openai-new-gpt4.html>



The screenshot shows a web browser displaying a New York Times article. The URL in the address bar is <https://www.nytimes.com/2023/03/14/technology/openai-new-gpt4.html>. The article title is "10 Ways GPT-4 Is Impressive but Still Flawed". The byline is "By Cade Metz and Keith Collins". The sub-headline reads: "OpenAI has upgraded the technology that powers its online chatbot in notable ways. It's more accurate, but it still makes things up." The date is "March 14, 2023". A chatbot interface is visible, showing a user prompt: "Tell me a novel joke about the singer Madonna." and the AI response: "Why did Madonna study geometry? Because she wanted to learn how to strike a pose in every angle! 📐 🎤 ✍️".

JA

how do you test the function of all cranial nerves?



The cranial nerves are 12 pairs of nerves that emerge directly from the brain and control many functions, including vision, hearing, smell, taste, facial movements, speech, and swallowing. The following is a general overview of how to test the function of all the cranial nerves:



1. Olfactory (smell): Test the patient's ability to identify various scents with one nostril occluded.
2. Optic (vision): Test visual acuity, visual fields, and color vision using various charts and



how do you test the function of all cranial nerves?

and pinprick, and test jaw movements and strength.

6. Abducens (eye movements): Test lateral gaze.
7. Facial (facial expression and taste): Test facial expressions, corneal reflex, and taste sensation.
8. Vestibulocochlear (hearing and balance): Test hearing using various methods, and test balance and coordination.
9. Glossopharyngeal (swallowing and taste): Test the gag reflex and taste sensation.
10. Vagus (voice and swallowing): Test the patient's voice quality and swallowing ability.
11. Accessory (shoulder and neck movements): Test shoulder and neck strength and range of motion.
12. Hypoglossal (tongue movements): Test tongue strength, movement, and deviation.

Testing the function of all cranial nerves requires a comprehensive neurological exam, including a detailed medical history and physical exam. A healthcare provider, such as a neurologist, can perform a thorough cranial nerve exam to assess the function of all 12 cranial nerves.



Is it a violation of the standard of care for an anesthesiologist if there is a tear to the patient's soft palate during intubation?



Is it a violation of the standard of care for an anesthesiologist if there is a tear to the patient's soft palate during intubation?



I am not a medical professional, but I can attempt to provide you with some general information on this topic.





Is it a violation of the standard of care for an anesthesiologist if there is a tear to the patient's soft palate during intubation?



I am not a medical professional, but I can attempt to provide you with some general information on this topic.



A tear to the patient's soft palate during intubation may or may not represent a violation of the standard of care. It depends on several factors, including the patient's unique anatomy, any pre-existing conditions, and the specific circumstances of the intubation.

KE

What if the anesthesiologist used a glidescope and did not directly visualize the endotracheal tube as it was being inserted into the patient's mouth past the soft palate and into the airway?

KE

What if the anesthesiologist used a glidescope and did not directly visualize the endotracheal tube as it was being inserted into the patient's mouth past the soft palate and into the airway?

If the anesthesiologist used a GlideScope and followed appropriate guidelines and protocols, the occurrence of a tear to the patient's soft palate during intubation may still be considered an unfortunate but unavoidable complication. However, if the anesthesiologist failed to take necessary precautions or did not adhere to established standards of care while using the GlideScope, this could potentially represent a violation of the standard of care.



But if the anesthesiologist didn't directly visualize the endotracheal tube as it was being inserted into the mouth past the soft palate and into the airway, isn't that negligence?



But if the anesthesiologist didn't directly visualize the endotracheal tube as it was being inserted into the mouth past the soft palate and into the airway, isn't that negligence?

If the anesthesiologist followed appropriate guidelines and protocols while using the GlideScope, their actions may not be considered negligent, even if they did not directly visualize the endotracheal tube as it was inserted. However, if the anesthesiologist failed to take necessary precautions, did not adhere to established standards of care, or misused the GlideScope, this could potentially represent negligence and a violation of the standard of care.

But if the anesthesiologist didn't directly visualize the endotracheal tube as it was being inserted into the mouth past the soft palate and into the airway, isn't that negligence?

If the anesthesiologist followed appropriate guidelines and protocols while using the GlideScope, their actions may not be considered negligent, even if they did not directly visualize the endotracheal tube as it was inserted. However, if the anesthesiologist failed to take necessary precautions, did not adhere to established standards of care, or misused the GlideScope, this could potentially represent negligence and a violation of the standard of care.

A thorough investigation, potentially including a review by medical experts, would likely be necessary to determine if the anesthesiologist's actions in this specific case were negligent or constituted a violation of the standard of care. This information is not a substitute for professional legal or medical advice. If you have concerns about a specific situation, it is important to consult with a qualified medical professional or an attorney experienced in medical malpractice cases.

JA

If a patient presents for a right knee arthroscopy and the left knee is prepped and draped and operated on, is that a violation of the standard of care applicable to an orthopaedist?

JA

If a patient presents for a right knee arthroscopy and the left knee is prepped and draped and operated on, is that a violation of the standard of care applicable to an orthopaedist?



Yes, operating on the wrong knee during an arthroscopy would generally be considered a violation of the standard of care applicable to an orthopedist. The American Academy of Orthopaedic Surgeons (AAOS) has established guidelines for preventing wrong-site surgery, which includes the use of preoperative verification processes, marking the correct surgical site, and implementing a time-out process immediately prior to the start of the procedure.



Yes, operating on the wrong knee during an arthroscopy would generally be considered a violation of the standard of care applicable to an orthopedist. The American Academy of

If a patient presents for a right knee arthroscopy and the left knee is prepped and operated on, it may be considered a deviation from the standard of care applicable to an orthopedist. The healthcare provider may be liable for any harm caused by the wrong-site surgery, and the patient may be entitled to compensation for damages resulting from the medical error.

It's important for healthcare providers to follow established guidelines and protocols to prevent wrong-site surgery and to communicate clearly with patients about the planned procedure and the risks and benefits associated with it. If a medical error does occur, the healthcare provider should take immediate steps to address the situation and provide appropriate follow-up care to the patient.

JA

If a patient is diagnosed with cholecystitis and the plan of care is to perform a laparoscopic cholecystectomy would a ductal injury be considered a violation of the standard of care even if all the ductal structures were identified through the critical view of safety?

If a patient is diagnosed with cholecystitis and the plan of care is to perform a laparoscopic cholecystectomy would a ductal injury be considered a violation of the standard of care even if all the ductal structures were identified through the critical view of safety?



If a patient is diagnosed with cholecystitis and a laparoscopic cholecystectomy is planned, a



If a patient is diagnosed with cholecystitis and a laparoscopic cholecystectomy is planned, a ductal injury during the procedure would generally be considered a deviation from the standard of care, even if all the ductal structures were identified through the critical view of safety.

Therefore, it is important for healthcare providers to follow established guidelines and protocols for laparoscopic cholecystectomy, including the use of the critical view of safety, to reduce the risk of bile duct injury. In the event of a ductal injury, the healthcare provider should take immediate steps to address the situation, provide appropriate follow-up care to the patient, and communicate effectively with the patient and their family about the nature and implications of the injury.

JA

If a male patient over the age of 65 presents with an elevated PSA, is it a violation of the standard of care to prescribe a prolonged (greater than 4 weeks) course of antibiotic therapy before proceeding with biopsy or referral to a urologist for possible work up of prostate cancer?

JA

If a male patient over the age of 65 presents with an elevated PSA, is it a violation of the standard of care to prescribe a prolonged (greater than 4 weeks) course of antibiotic therapy before proceeding with biopsy or referral to a urologist for possible work up of prostate cancer?



Prescribing a prolonged course of antibiotics for a male patient over the age of 65 with an



Prescribing a prolonged course of antibiotics for a male patient over the age of 65 with an elevated PSA before proceeding with biopsy or referral to a urologist for possible workup of prostate cancer would generally be considered a deviation from the standard of care.

The American Urological Association (AUA) recommends that men with an elevated PSA level should undergo further evaluation, such as a prostate biopsy or referral to a urologist, to determine the cause of the elevation. Delaying the workup for prostate cancer with prolonged antibiotic therapy could potentially delay diagnosis and treatment of the cancer, which could have serious implications for the patient's prognosis and outcome.

In general, healthcare providers should follow established guidelines and protocols for the evaluation and management of elevated PSA levels, including timely referral to a urologist for further evaluation and treatment. If there are concerns about the patient's ability to undergo prostate biopsy or other diagnostic tests, the healthcare provider should work with the patient to address these concerns and develop an appropriate plan of care.

A.I. in Your Practices

- Should I do a demo?
- Do you advertise it?
- Do you disclose it?
- Do you document it?
- Does rollout do a retrospective review?
- Do you blame it?
- Will it blame you?
- What do your contracts say?

Software as a (Co-Defendant)

- Skounakis v. Dr. Sotillo and Dr. G's Franchising Companies, LLC (A-2403-15T2 (NJ Super. Ct. App. Div. March 19, 2018)
 - **Plaintiff's Expert Cardiologist: Dr. G's program deviated from the standard of care by including a combination of phendimetrazine and liothyronine**

Software as a (Co-Defendant)

- Skounakis v. Dr. Sotillo and Dr. G's Franchising Companies, LLC (A-2403-15T2 (NJ Super. Ct. App. Div. March 19, 2018)
 - Plaintiff's Expert Cardiologist: Dr. G's program deviated from the standard of care by including a combination of phendimetrazine and liothyronine
 - **Appellate Court: Plaintiff's expert 1) does not have to be a computer software expert, and 2) may testify about the propriety of the medications Dr. G's program prescribed**

The World “Before” Ransomware*

CYBER THREATS CONTINUE TO ESCALATE

Advisen's Cyber Data Exposes Cyber Trends

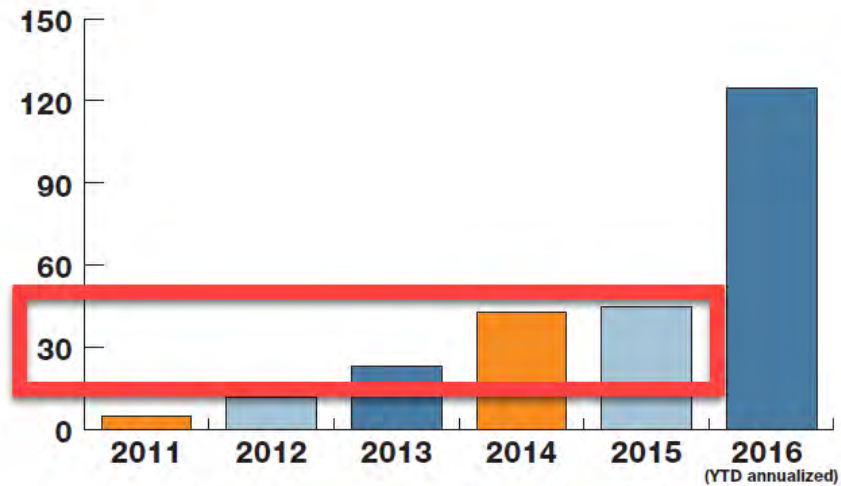
RANSOMWARE CASES PROJECTED
TO DOUBLE IN 2016

Ransomware cases have steadily increased over the past 5 years. With 2016 half over, the number of cases is expected to double from 2015 to 2016, reaching an all-time high.

**2016 data is as of July 15, 2016.*

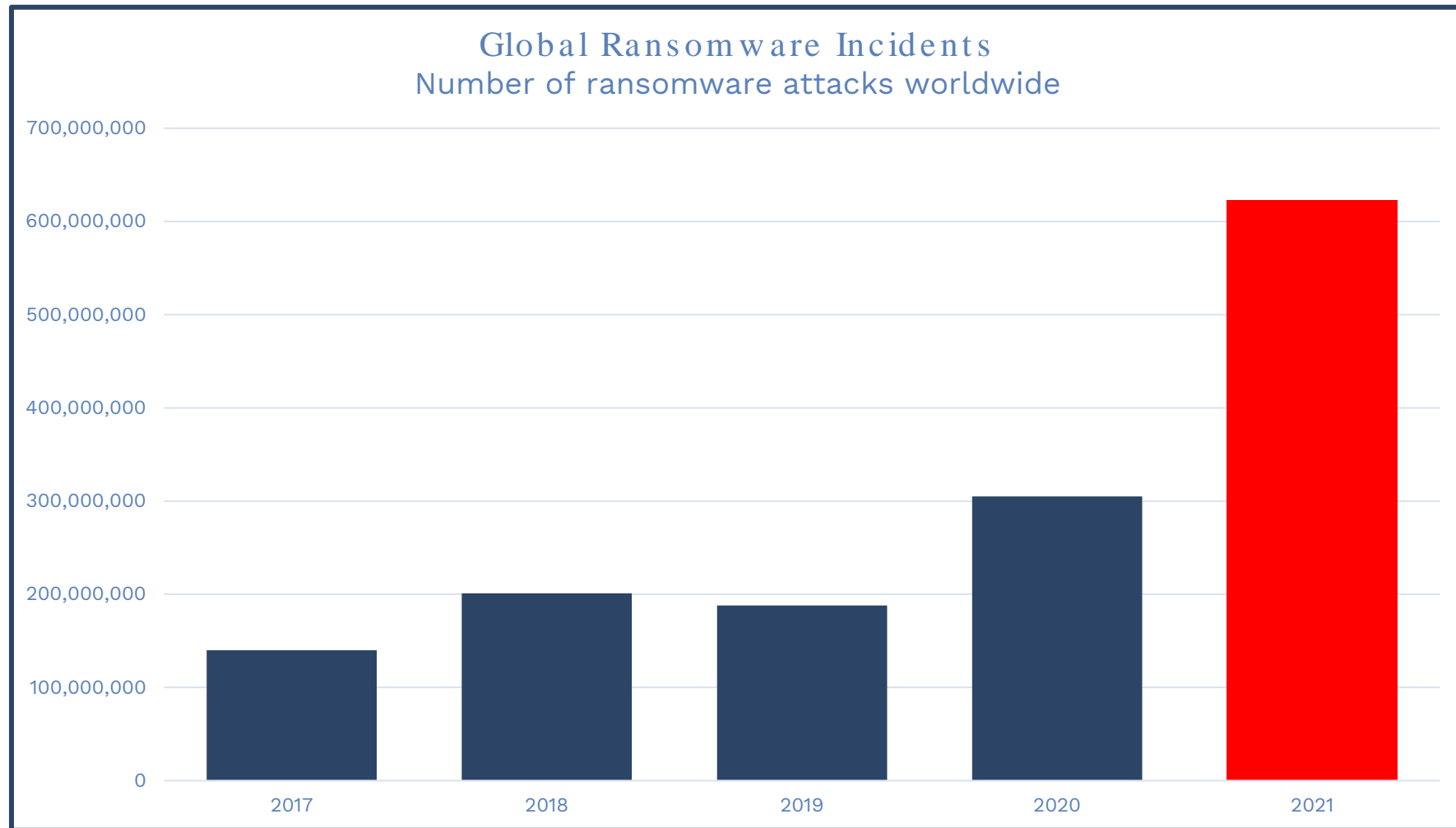
Network Security Disruptions grew

5X from 2010 to 2015



Ransomware Attacks Trend 2011-2016*

The World Today



Source: 2022 SonicWall Cyber Threat Report

The World “Before” Ransomware*

DAILY REPORT ONLINE

How a Fax Cost a Savannah Hospital \$500K

JULY 31, 2019

When asked for school records, an employee in a hospital office inadvertently sent private medical records with therapy notes for a former patient. The jury deliberated a little less than an hour before awarding \$500,000, plus court costs.



It WAS about “compliance.”

It IS about “data as an asset and a risk.”

The World Today



Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Hackers Have Ability To Control Key Infrastructure, U.S. Says

By **Dave Simpson**

Law360 (April 13, 2022, 10:50 PM EDT) -- Skilled hackers have shown the capability of taking full control of numerous key U.S. infrastructure systems, including those in the energy and manufacturing sector, according to a Wednesday cybersecurity alert from several federal agencies.

The report from the Department of Energy, the Cybersecurity and Infrastructure Security Agency, the National Security Agency, and the Federal Bureau of Investigation claims that these advanced hackers have created custom tools for targeting such systems.

<https://www.law360.com/articles/1484014/print?section=aerospace>

The World Today

Critical Infrastructure Security , Fraud Management & Cybercrime , Healthcare

Healthcare Most Hit by Ransomware Last Year, FBI Finds

Bureau Warns Underreporting Remains Rife, Including by Critical Infrastructure

Mathew J. Schwartz (euroinfosec) • February 27, 2023

Healthcare and public health bore the brunt of ransomware attacks on critical infrastructure sectors launched during the last year, says the FBI.

See Also: OnDemand | Navigating the Difficulties of Patching OT

The FBI's Internet Complaint Center last year received 870 complaints that "indicated organizations belonging to a critical infrastructure sector were victims of a ransomware attack," said David Scott, deputy assistant director of the FBI's Cyber Division, speaking at the Futurescot conference Monday in Glasgow, Scotland.

Critical manufacturing and the government, including schools, followed healthcare as the most-attacked sectors, IC3 data shows.

The World Today



NEWS (/TOPIC/NEWS) | HEALTH CARE (/TOPIC/HEALTH-CARE)

How the war in Ukraine threatens hospital cybersecurity — and what to do about it

Stacy Weiner, Senior Staff Writer

May 24, 2022

Though far away, the war in Ukraine endangers the security of crucial digital health tools in the U.S., from electronic health records to life-saving medical devices. An

“Health care has data that could be invaluable to adversaries seeking information about U.S. military and government leaders,” says Riggi, who spent nearly three decades at the FBI.

<https://www.aamc.org/news-insights/how-war-ukraine-threatens-hospital-cybersecurity-and-what-do-about-it?>

The World Today



Portfolio Media, Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Sensitive Data Of Congress Members, Staff Leaked In Hack

By Ben Kochman

Law360 (March 9, 2023, 8:10 PM EST) -- Social Security numbers, home addresses and other personal data belonging to Congress members and employees were stolen in a cyberattack on a Washington, D.C., health care platform, U.S. House of Representatives leaders say.

The U.S. Capitol Police and FBI have told House Speaker Kevin McCarthy, R-Calif., and House Minority Leader Hakeem Jeffries, D-N.Y., that health insurance marketplace DC Health Link appears to have had a "significant data breach" that led to stolen data being offered for sale on an online hacking forum, the lawmakers said in an open letter late Wednesday.

The FBI was able to purchase a set of the data, which includes names of spouses, dependent children, Social Security numbers and home addresses, the letter said.

"This breach increases the risk that members, their staff and their families will experience identity theft, financial crimes and physical threats — already an ongoing concern," McCarthy and Jeffries said.

A DC Health Link spokesperson, Adam Hudson, confirmed the breach in a statement on Thursday. Hudson did not say how many people's data is believed to have been exposed, but someone on an online hacking forum claimed this week to have stolen a database containing information belonging to 170,000 people, according to a screenshot viewed by Law360.

The World Today

<https://www.wsj.com/articles/chatgpt-helped-win-a-hackathon-96332de4>

WSJ PRO

ChatGPT Helped Win a Hackathon

A team from cybersecurity firm Claroty used the AI bot to write code to exploit vulnerabilities in industrial systems



Today's ChatGPT is too unpredictable to be a reliable weapon on its own, but that won't always be the case, a cybersecurity expert said.

PHOTO: DADO RUVIC/REUTERS

By Kim S. Nash

March 20, 2023 5:30 am ET | WSJ PRO

The ChatGPT AI bot has spurred speculation about how hackers might use it and similar tools to attack faster and more effectively, though the more damaging exploits so far have been in laboratories.

In its current form, the ChatGPT bot from OpenAI, an artificial-intelligence startup backed by billions of dollars from Microsoft Corp., is mainly trained to digest and generate text. For security chiefs, that means bot-written phishing emails might be more convincing than, for example, messages from a hacker whose first language isn't English.

Industries Affected



23%

Healthcare
(including Biotech & Pharma)

15%

Finance & Insurance

6%

Government

12%

Education

4%

Nonprofit

17%

Business & Professional Services
(including Engineering & Transportation)

10%

Manufacturing

2%

Technology

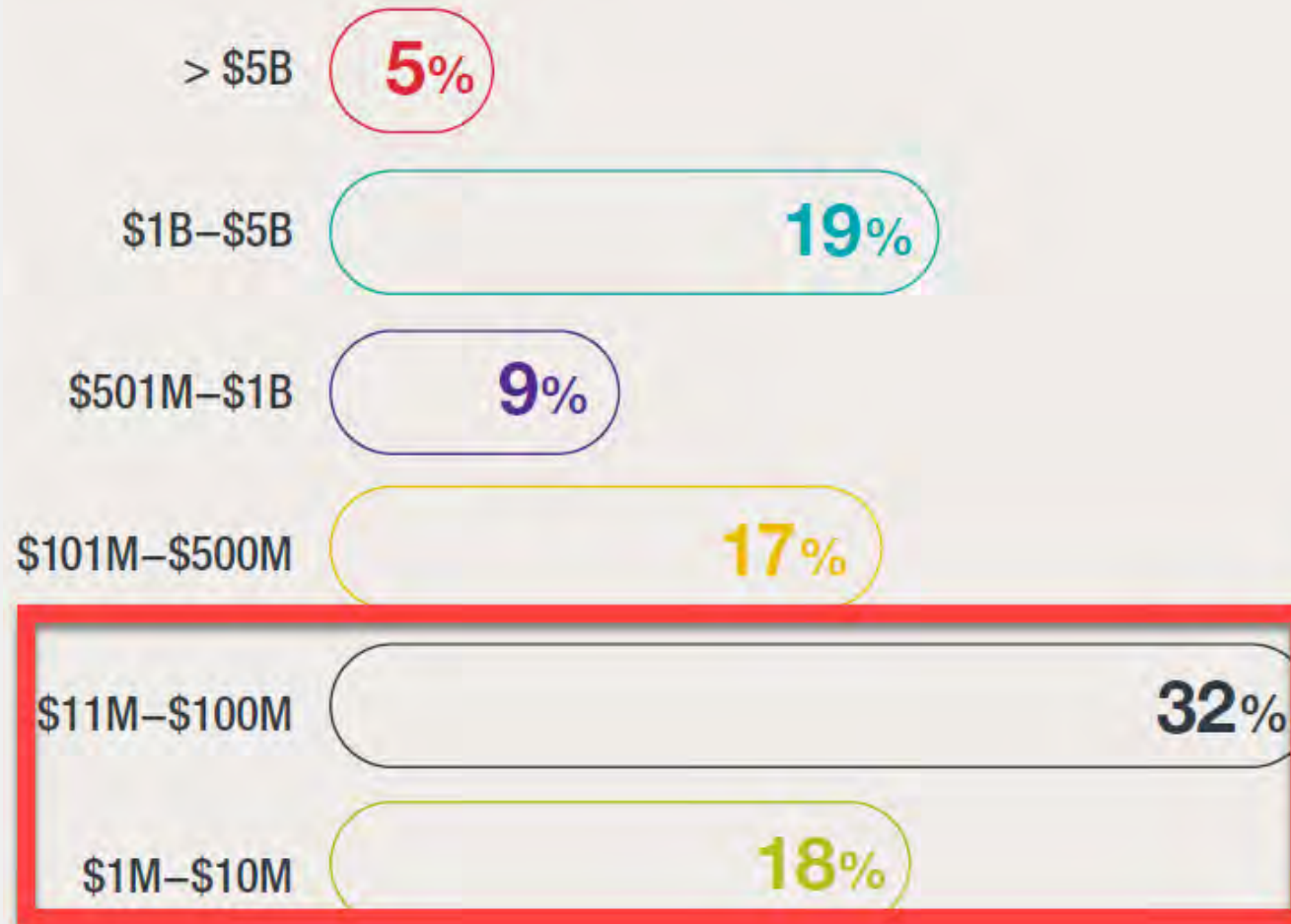
9%

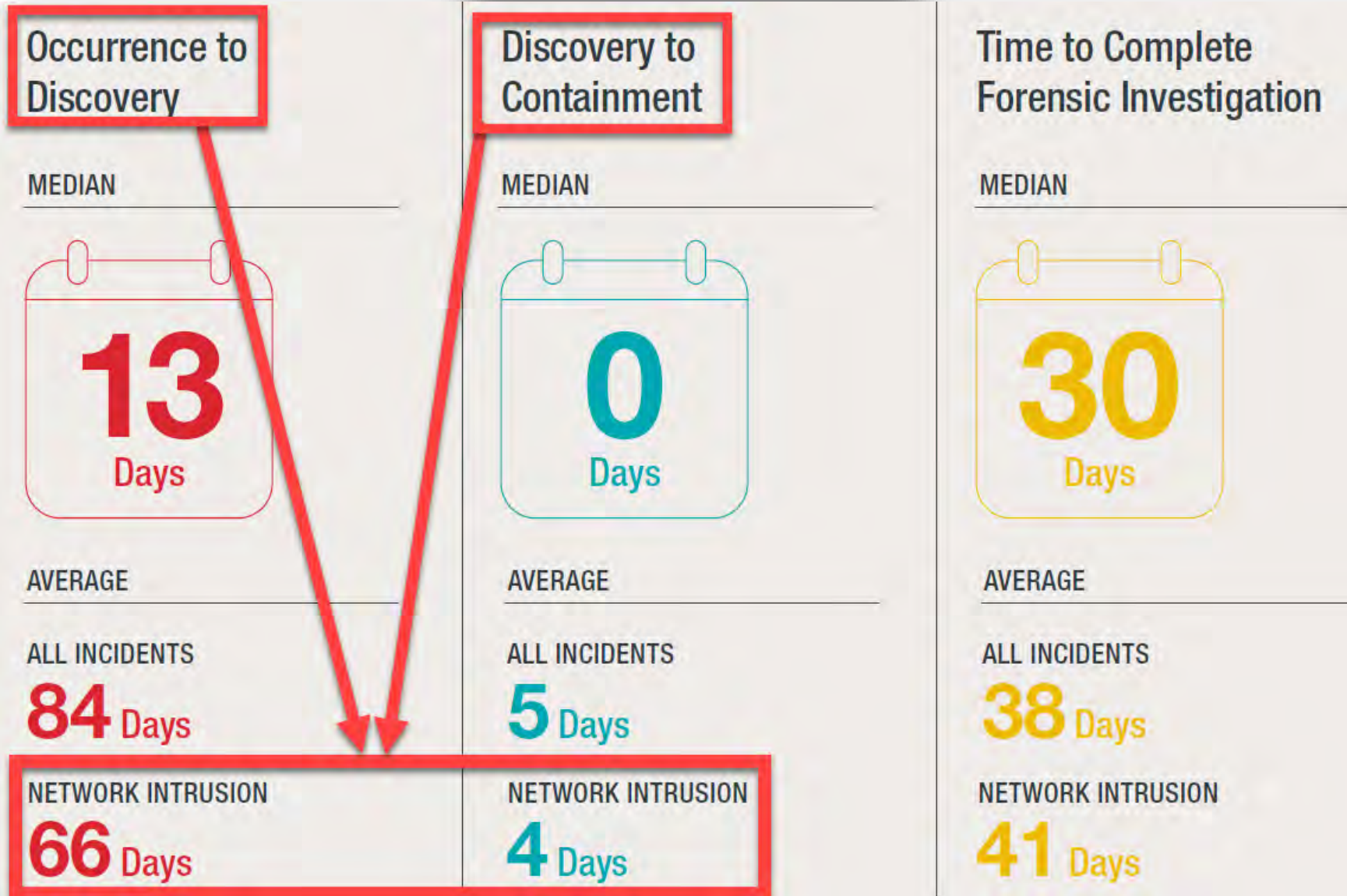
Retail, Restaurant & Hospitality

2%

Energy

Entity Size by Revenue





OCR Enforcement Actions - \$1.3m



U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Office for Civil Rights

September 11, 2023

**HHS Office for Civil Rights Settles with L.A. Care Health Plan Over Potential
HIPAA Security Rule Violations**

LA Care, the largest publicly operated health plan in the country paid \$1,300,000 to
settle

OCR Enforcement Actions - \$100,000



U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office for Civil Rights

October 31, 2023

HHS' Office for Civil Rights Settles Ransomware Cyber-Attack Investigation

OCR Settles with Business Associate in attack affecting over 200,000 individuals

OCR Enforcement Actions - \$80,000



**U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Office for Civil Rights**

November 20, 2023

**HHS' Office for Civil Rights Settles HIPAA Investigation of St. Joseph's
Medical Center for Disclosure of Patients' Protected Health Information to a
News Reporter**

*St. Joseph's Medical Center provided a national media outlet access to COVID-19 patients'
protected health information*

OCR Enforcement Actions - \$480,000



U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES Office for Civil Rights

December 7, 2023

HHS' Office for Civil Rights Settles Landmark Phishing Cyber-Attack Investigation

*Louisiana Medical Group settles after investigation reveals large cybersecurity breach affecting
nearly 35,000 patients*

What is MFA?

Multi-factor Authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN. MFA is a core component of a strong identity and access management (IAM) policy. Rather than just asking for a username and password, MFA requires one or more additional verification factors, which decreases the likelihood of a successful cyber attack.



What is MFA?

Multi-factor Authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or component of an access management system. Rather than just a username and password, MFA requires more additional factors, which decrease the risk of a successful compromise.

If you do ONE thing...

The image shows a screenshot of the Wells Fargo website's login page. The page features a red header with the Wells Fargo logo and navigation links for 'Enroll', 'Customer Service', 'ATMs/Locations', and 'Español'. A search bar is also present. The main content area displays a greeting 'Good afternoon' and the instruction 'Sign on to manage your accounts'. Below this, there is a form with a 'Username' field. A yellow banner with the text 'If you do ONE thing...' is overlaid on the page. To the right, a 'Multi-Factor Authentication' overlay shows a fingerprint being scanned, with the text 'Step 3: Fingerprint verified'.

<https://www.onelogin.com/learn/what-is-mfa>

OCR Quarter 1 2022 Cybersecurity Newsletter

Defending Against Common Cyber-Attacks

- CEs should:
 - 1) Subscribe to Cybersecurity and Infrastructure Security Agency (CISA) alerts and bulletins
 - Complete form at: <https://public.govdelivery.com/accounts/USDHSCISA/subscriber/new>
 - 2) Subscribe to alerts from the HHS Health Sector Cybersecurity Coordination Center (HC3)
 - Email: HC3@HHS.GOV to subscribe

<https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-first-quarter-2022/index.html>

From: [REDACTED]@gmail.com

Sent: Wednesday, June 8, 2022 1:08 PM

To: Jason Newton <jason.newton@curi.com>

Subject: Re: [REDACTED] 2022- Jason Newton's Slide Deck Attached

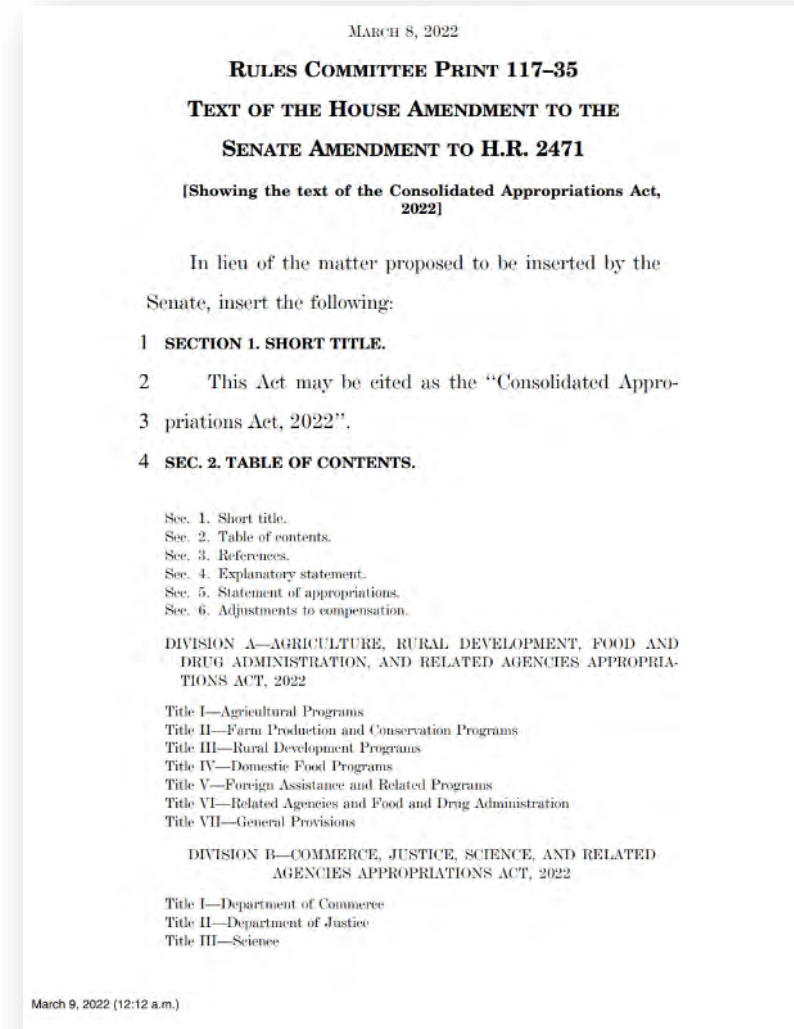
NOTICE: EXTERNAL EMAIL. Do not click links or open attachments unless verified. Report all suspicious emails using the "Report Phishing" button in Outlook.



****Regularly test employees and target training to those who fail***

The World Tomorrow

- CIRCIA—The Cyber Incident Reporting for Critical Infrastructure Act
- 2,741 pages
- Signed by President Biden **March 15, 2022**
- **“Covered Entities” include “Healthcare”**
- **72 hours to report cyber incidents** to CISA (US Dept. of Homeland Security Cybersecurity and Infrastructure Agency)
- **24 hours to report ransomware payments**
- A lot to be determined—could be 18-24 months before more is clear due to rule-making process





TLP: CLEAR

Ransomware Vulnerability Warning Pilot (RVWP)

March 2023

OVERVIEW

Organizations across all sectors and of all sizes are too frequently impacted by damaging ransomware incidents. Many of these incidents are perpetrated by ransomware threat actors using known vulnerabilities. By urgently fixing these vulnerabilities, organizations can significantly reduce their likelihood of experiencing a ransomware event. In addition, organizations should implement other security controls as described on stopransomware.gov.

The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCA), which President Biden signed into law in March 2022, required CISA to establish the RVWP (see Section 105 [6 U.S.C. 652]).

However, most organizations may be unaware that a vulnerability used by ransomware threat actors is present on their network. Through the Ransomware Vulnerability Warning Pilot (RVWP), which started on January 30, 2023, CISA is making a new effort to warn critical infrastructure entities that their systems have exposed vulnerabilities that may be exploited by ransomware threat actors.

<https://www.cisa.gov/stopransomware/Ransomware-Vulnerability-Warning-Pilot>



TLP:CLEAR

Ransomware Vulnerability Warning Pilot (RVWP)

March 2023

Q: Who will notify me if I have a vulnerability?

A: [CISA Regional staff members](#), located throughout the country, make notifications and may provide assistance and resources to mitigate the vulnerability.

Q: What can I expect in the notification?

A: Notifications will contain key information regarding the vulnerable system, such as the manufacturer and model of the device, the IP address in use, how CISA detected the vulnerability, and guidance on how the vulnerability should be mitigated.

Q: How should I expect to receive a notification?

A: CISA regional staff members will make notifications by phone call or email.



TLP:CLEAR

Ransomware Vulnerability Warning Pilot (RVWP)

March 2023

Q: How do I verify it is CISA notifying me?

A: If you receive a notification, you can verify the identity of the CISA personnel through [CISA Central: Central@cisa.gov](mailto:Central@cisa.gov) or (888) 282-0870.

Q: If I received a notification, does that mean I was compromised?

A: Receiving a notification through CISA RVWP is not indicative of a compromise. However, it does indicate you are at risk and the information system requires immediate remediation.

Q: Am I required to comply with CISA's recommended actions?

A: No. Receiving a notification does not require you to comply with or institute any of CISA's recommendations.



TLP: CLEAR

Ransomware Vulnerability Warning Pilot (RVWP)

March 2023

OVERVIEW

Q: How did CISA determine I was vulnerable?

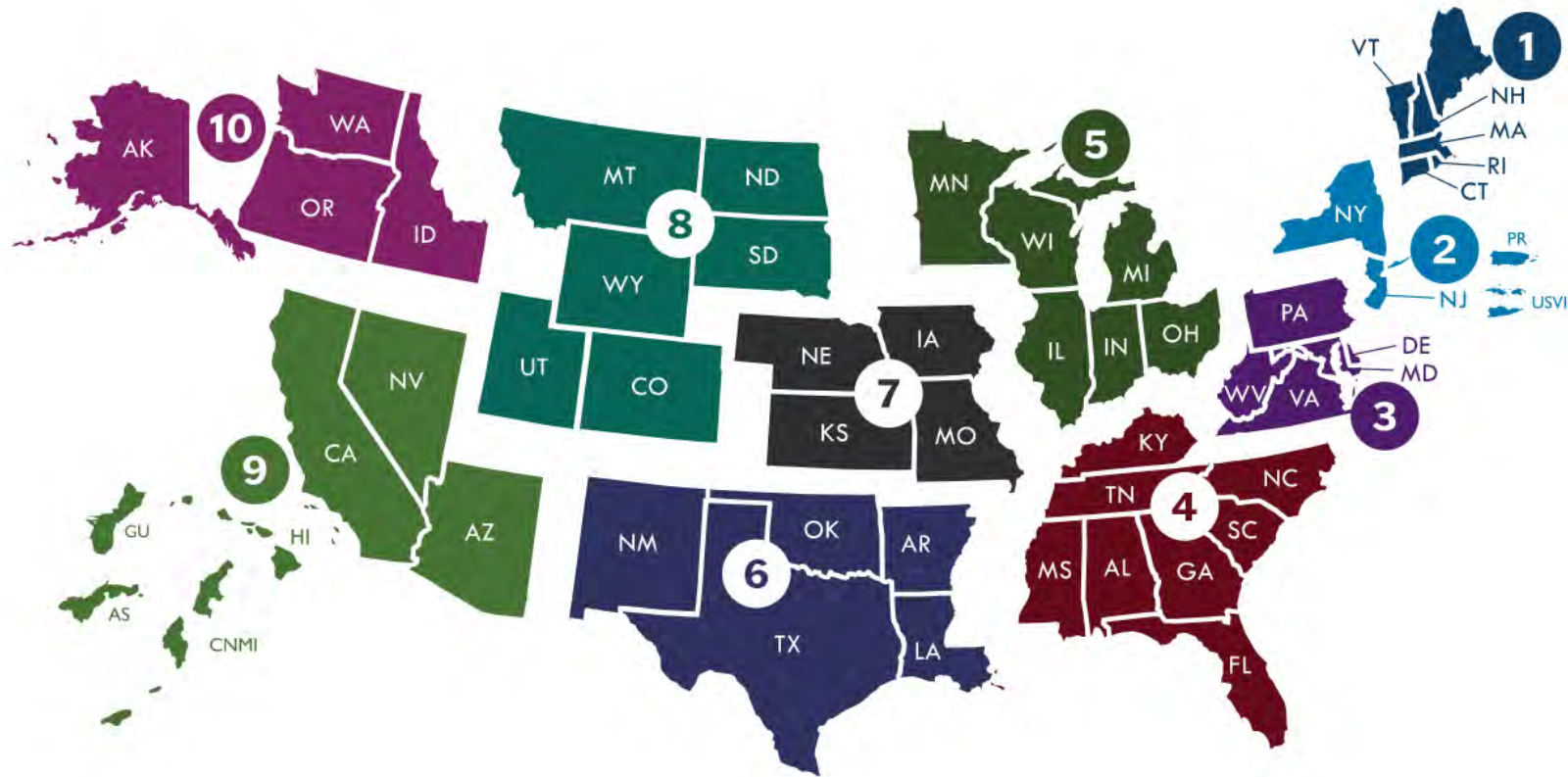
A: CISA leverages multiple open-source and internal tools to research and detect vulnerabilities within U.S. critical infrastructure.

Q: Can I receive other CISA services?

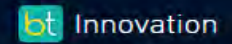
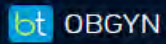
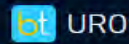
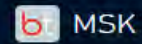
A: Absolutely! CISA offers multiple no-cost resources and tools. As a starting point, organizations should sign up for [CISA's Cyber Hygiene Vulnerability Scanning](#), undertake a self-assessment to determine progress in implementing the [Cybersecurity Performance Goals](#), and **build a relationship with a [regional CISA cybersecurity advisor](#)** to participate in additional applicable services or capabilities.

Contact Your Regional Office

CISA's program of work is carried out across the nation by personnel assigned to its 10 regional offices. To contact your region's office, click on the appropriate Region below based on your state.



backtable



BackTable / VI / Podcast / Episode #349

EPISODE #349
CYBER SECURITY FOR PHYSICIANS

bt With Jason Newton, Esq

▶ 1683

Ep 349 Cybersecurity for Physicians with Jason Newton, Esq



BackTable, LLC (Producer). (2023, July 28). Ep. 349 – Cybersecurity for Physicians [Audio podcast]. Retrieved from <https://www.backtable.com>



North Carolina Society of Gastroenterology 2024 Annual Meeting

Multiple Choice Question

To treat my patients via telehealth when they are temporarily physically located in other states:

- a) I only need to have a medical license in the state in which I'm located at the time of the encounter.
- b) If the state is adjacent to my home state, I only need to have a medical license in the state in which I'm located at the time of the encounter.
- c) If the patient consents, I only need to have a medical license in the state in which I'm located at the time of the encounter.
- d) I need to have a medical license in the state in which the patient is physically located.

Multiple Choice Question

To treat my patients via telehealth when they are temporarily physically located in other states:

- a) I only need to have a medical license in the state in which I'm located at the time of the encounter.
- b) If the state is adjacent to my home state, I only need to have a medical license in the state in which I'm located at the time of the encounter.
- c) If the patient consents, I only need to have a medical license in the state in which I'm located at the time of the encounter.
- d) I need to have a medical license in the state in which the patient is physically located.**

Thank you!

