

BREAKOUT SESSION



**12TH ANNUAL
TELEHEALTH
SUMMIT
OF SOUTH CAROLINA**

OCTOBER 28-30, 2024

Technology and Innovation Track:

Cybersecurity & Technology: Understanding Threats and Compliance

**Tuesday, October 29
3:30 PM - 4:15 PM**



Thomas Wootton
Iron Bow Technologies



Cybersecurity and Telehealth: Understanding Threats and Compliance

Presented By: Tom Wootton
Cybersecurity Advisory Services Lead, Iron Bow Technologies



Becker's Podcast Daily Briefing
Today's top stories in 5 minutes or less

Listen now



Few rural hospitals are using free cybersecurity help, White House says

Giles Bruce - Wednesday, September 4th, 2024



Less than a quarter of rural hospitals have used a new program that provides free cybersecurity assistance from Microsoft and Google, [Nextgov/FCW](#) reported.

About 350 of 1,800 small and rural U.S. hospitals have accessed the cybersecurity help that [launched](#) in June, according to a Sept. 3 update by White House deputy national cybersecurity advisor Anne Neuberger covered by the news outlet. Those facilities span from Maine to Texas and across the Midwest.

As healthcare cyberattacks proliferate, rural hospitals [have been found](#) to be more vulnerable because of their lack of proximity to other medical facilities and dearth of [cybersecurity funding](#). The White House partnered with the Big Tech companies to boost rural hospital cybersecurity.

Microsoft is offering grants and up to a 75% discount on cybersecurity products for critical access and rural emergency hospitals and a free year of cybersecurity for larger rural hospitals already using its services, as well as no-cost cybersecurity assessments, training for frontline and IT staff, and Windows 10 updates for one year.

Google is extending complimentary endpoint security advice and funding support for software migration, and started a pilot program of cybersecurity products tailored to rural hospitals.



Becker's Podcast Daily Briefing
Today's top stories in 5 minutes or less

Listen now



Russian hackers target healthcare sector

Naomi Diaz - Friday, September 6th, 2024



The FBI is [warning](#) U.S. critical infrastructure industries about hackers associated with the Russian General Staff Main Intelligence Directorate 161st Specialist Training Center.

These hackers, who have been operating since 2020, have been targeting global entities, according to a Sept. 5 advisory from the FBI. The hackers have been engaged in espionage, sabotage and efforts to inflict reputational damage.

The hackers are known for targeting critical infrastructure and key resource sectors across various regions, including government services, financial institutions, transportation systems, energy grids and healthcare systems. Their activities primarily focus on NATO members, the European Union, and countries in Central America and Asia, the advisory said.



Home » Security

Data leak exposes 14,000 US medical professionals: what we know so far

Updated on: September 11, 2024 11:02 AM



The leak was caused by a misconfiguration of the company's systems, which exposed files that were not meant to be publicly accessible. The database backup, dated June 2nd, 2024, contained a vast amount of personal data, putting medical professionals at risk.

The leaked sensitive data included:

- Full names
- Addresses
- Phone numbers
- Email addresses
- Dates of birth
- Work experience
- Jobs assigned by MNA Healthcare
- Communications with MNA Healthcare representatives
- Encrypted Social Security Numbers (SSNs)
- Hashed temporary passwords to access the platform

Cybersecurity IN Healthcare

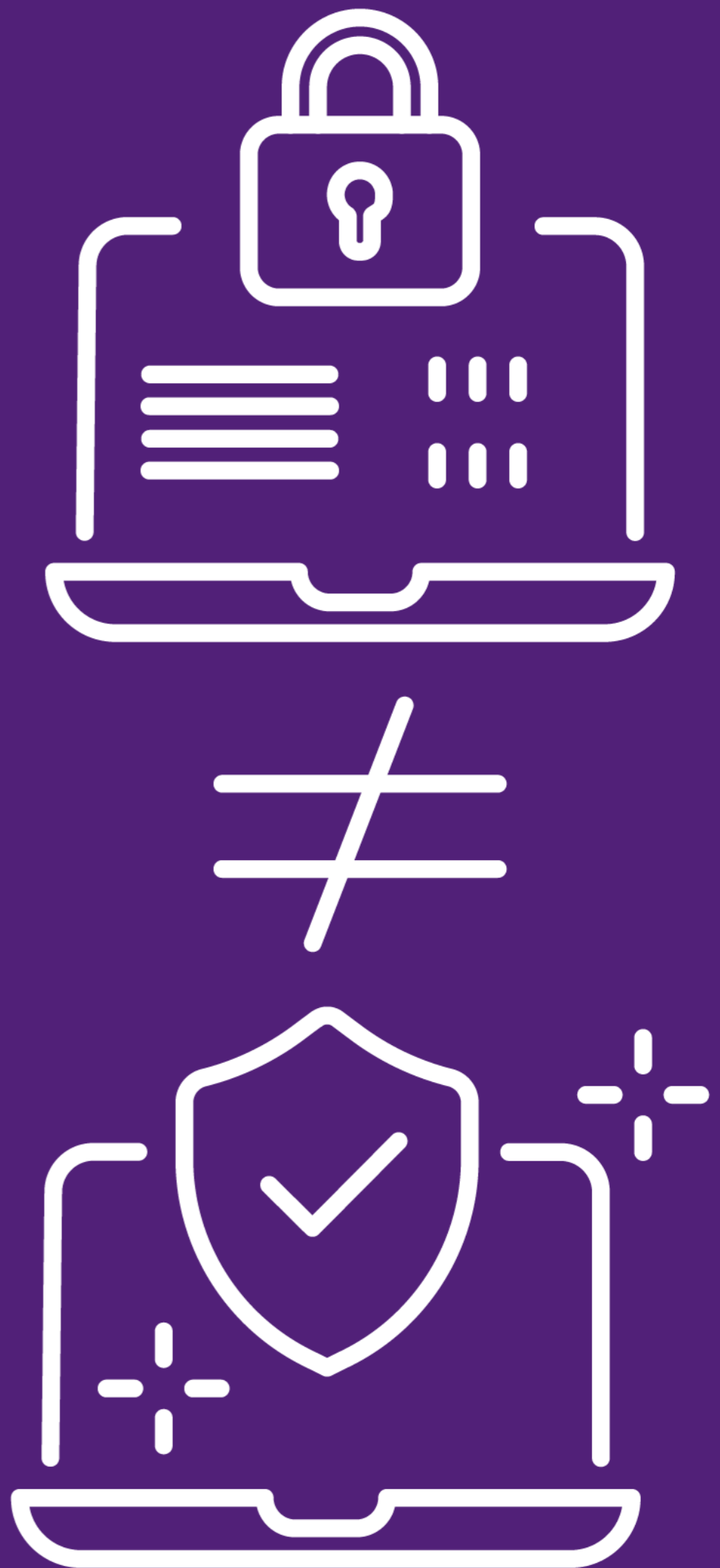
Common Misconceptions

- If there is an accessibility or availability issue, IT will fix it.
- If there is a cyber event that impacts the organization or institution, IT will correct it.
- If a regulatory violation occurs and is discovered in an audit or assessment, IT takes the blame and is responsible for remediation.
- IT and Cyber are the same thing.



To put it another way...

- If there is a patient with a sore joint, who does that patient see? A surgeon? A cardiologist? A pediatrician?
- Thinking the IT department/individual is the same as a Cyber department/individual is akin to saying a patient can see any healthcare professional regardless of ailment for proper treatment.
- IT and Cyber are not the same thing and should not be addressed or treated the same way.



Recent (>1 year) Statistics

Health-ISAC analyzed cybersecurity breach-related data from mid-2023 over the past 13 ½ years posted by the U.S. Government:

5,558

Events

438M

Breached PHI
Records

The above averages to over
**86,000 PHI records being
exposed every day over the
past 13 ½ years.**


2,209

Incidents were
Reported Over Past
3 Years

3,349

Incidents Were
reported Over the
First 10 ½ years of
reporting

What IS Present

- Some compliance with industry regulation (HIPAA)
 - Some cybersecurity management in large conglomerates
 - General understanding that cybersecurity postures can always be improved
- 
- The background of the slide is a dark blue gradient with a complex network of white and light blue icons. These icons include a lightbulb, a person's head profile, a shield with a padlock, a medical cross, a smartphone, and various data flow symbols, representing the intersection of healthcare and cybersecurity.

What IS NOT Present

- Adequate cybersecurity attention and coverage in smaller and more rural healthcare institutions
- Adequate cybersecurity budgets and cybersecurity training for ALL employees/staff
- Attention on and mitigation of the overuse and over-reliance on unstable technologies
- Proper risk management of the healthcare institution versus compliance-focus
- The understanding that cybersecurity can no longer be an afterthought. It **MUST** be part of all decision-making within the institution as human lives are at stake

What Does This Mean for Telehealth?

- Organizational connection security concerns
- Connection security and stability concerns
- Data sharing security concerns
- Understanding threats that affect Telehealth platforms as well as healthcare institutions
- Social-engineering vulnerabilities

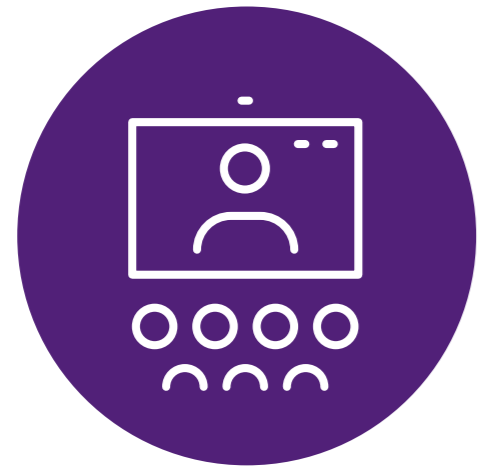


What (Simplified)?

- Does the organization have any security on the devices they use to connect with patients?
- Will the connection be constant without interruption?
- If files are shared during the session, who else has access to them (if anyone)?
- What else is out there that one should be concerned about that could have a negative impact on Telehealth or healthcare in general?
- Is there someone connected that is trying to trick the organization into divulging information?

Cybersecurity AND Healthcare

What Can Be Done?



Training and awareness for employees



Make cybersecurity part of the daily routine



Ask questions, collaborate, and communicate



Be transparent across the organization



Check and double-check security settings/configurations **PRIOR** to connecting with patients

What Can Be Done?

- Look at cybersecurity training and awareness as actual learning exercises, not as a yearly check-the-box compliance item that has the approach of “click, click, next, Finish”.
- The more you apply cybersecurity knowledge to your everyday routines, the more secure the organization will become as a whole.



Questions?



Thank You!

Visit the Iron Bow Booth &
Find us at the Networking Reception!