Arizona Telemedicine Program

Arizona Department of Health Services

Southwest Telehealth TRC Resource · Center™

maricopa county medical society

Improving Access to Quality Medical Care Webinar Series

Presented by

The Southwest Telehealth Resource Center, Arizona Telemedicine Program, and the Arizona Department of Health Services

Welcome

- Arizona Healthcare Professionals
- Fellow HRSA Grantees
- All other participants

The **Arizona Department of Health Services, the Arizona Telemedicine Program, the Southwest Telehealth Resource Center and Maricopa County Medical Society** welcome you to this free webinar series.

The practice & deliver of healthcare is changing, with an emphasis on **improving quality, safety, efficiency, & access to care**.

Telemedicine can help you achieve these goals!

Webinar Tips & Notes

- When you joined the webinar your phone &/or computer microphone was muted
- Time is reserved at the end for Q&A, please use the **Chat function** to ask questions
- Please fill out the post-webinar survey
- Webinar is being recorded
- Recordings will be posted on the ATP website
    - http://telemedicine.arizona.edu/webinars/previous

Continuing Medical Education Information

“How to Counteract Ransomware Attacks on Healthcare”

Outcome Objectives

1) Describe the basics of ransomware and why it poses cybersecurity and other risks.
2) Determine weaknesses in healthcare systems.
3) Identify methods to counteract ransomware in medical settings.

Accreditation / Credit Designation Statement

This activity has been planned and implemented in accordance with the accreditation requirements and polices of the Accreditation Council for Continuing Medical Education (ACCME) through the joint providership of The University of Arizona College of Medicine - Tucson and Maricopa County Medical Society. The University of Arizona College of Medicine - Tucson is accredited by the ACCME to provide continuing medical education for physicians.

The University of Arizona College of Medicine - Tucson designates this live activity for a maximum of 1 *AMA PRA Category 1 Credit(s)*™. Physicians should claim only the credit commensurate with the extent of their participation in the activity.

Conflict of Interest Disclosure Statement

All Faculty, CME Planning Committee Members, and the CME Office Reviewers have disclosed that they do not have any relevant financial relationships with commercial interests that could constitute a conflict of interest concerning this CME activity.

Disclaimer

- The opinions expressed in this presentation and on the following slides are solely those of the presenter and not necessarily those of the organizations sponsoring this webinar. The organizations do not guarantee the accuracy or reliability of the information provided herein.

Requesting your Certificate

“How to Counteract Ransomware Attacks on Healthcare”

Please complete the Evaluation via the SurveyMonkey link that has opened in a separate browser window.

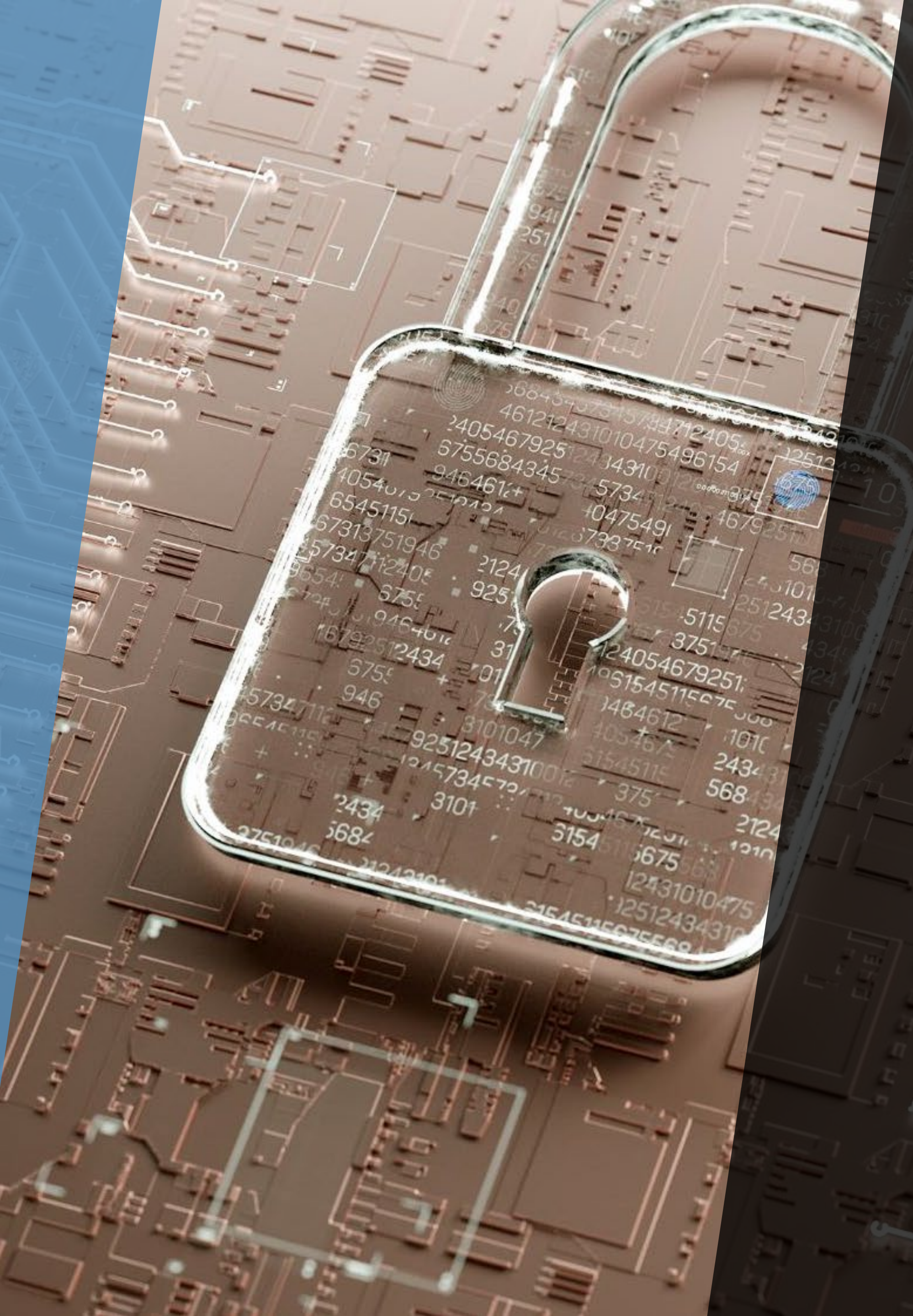
Evaluation can also be found at:
https://www.surveymonkey.com/r/RansomSept22SWTRC

This will be posted in the chat at the end of today’s program.

Jeanne E. Varner Powell, JD

Jeanne E. Varner Powell, JD
Senior Legal Risk Management Consultant, MICA

As a medical malpractice defense attorney, Jeanne represented hospitals and health care professionals for nearly 20 years. In 2020, she left litigation to join MICA as the Senior Legal Risk Management Consultant. In this position, she writes and speaks on medical professional liability topics and consults directly with insured physicians and practices.



MICA®

Ransomware in Health Care

Jeanne E. Varner Powell, JD, Senior Legal Risk Management Consultant

Cyberthieves Target Health Care

Health care is an easy target

- Higher stakes
- More vulnerable
  - Pre-pandemic vulnerabilities
  - Pandemic-related vulnerabilities

Ramifications of Ransomware in Health Care

- Access to necessary patient care records
- Disruption of workflows and processes
- Impaired function of medical devices
- Data breaches
- Government investigations
- Lawsuits
- High recovery costs
- Loss of good will, damage to reputation, and erosion of patient trust

Reducing Ransomware Risks with HIPAA Compliance

- Compliance with HIPAA Security Rule required since 2005
- Security Rule limits access to electronic protected health information (ePHI)
- Security Rule requires implementation of safeguards to protect confidentiality and integrity of all ePHI, not just information in the electronic health record

Security Rule Requirements

Risk Analysis

- Initial, accurate, thorough assessment of potential risks to/vulnerabilities of ePHI
  - Identify all ePHI created, maintained, received, or transmitted
  - Determine and document risks to ePHI
  - Evaluate and document likelihood and impact of risks to ePHI
- Regularly review and periodically update risk analysis – it's an ongoing process

Risk Management

- Implement security measures intended to reduce each risk to a reasonable and appropriate level
- Adopt reasonable appropriate policies and procedures related to Security Rule and risks

Security Rule Penalties

Office of Civil Rights (OCR) can impose fines, penalties, and corrective action plans for non-compliance with Security Rule

OCR audits, compliance reviews, or investigations after a data breach may uncover noncompliance

Under HITECH Act, adoption of "recognized security practices" may mitigate penalties for Security Rule violations

After an Attack: What the Security Rule Requires

- Presence of ransomware or other malware is a “security incident”
- Requires ransomware victim to initiate its security incident procedures and response
- Determine incident scope, origination, cause and contributing factors, and if it is ongoing or finished
- Response activities and documentation
  - Impact
  - Vulnerabilities permitting attack
  - Restoration of data
  - Return to normal business operations
  - Other post-incident activities

Required Reporting of Data Breaches

- Breach= acquisition, access, use, or disclosure of PHI in a manner not permitted under HIPAA Privacy Rule which compromises security or privacy of PHI
- Presumption of "breach" in a ransomware attack
- Breach triggers reporting obligations
  - All individual breach victims no later than 60 days after discovery
  - Office of Civil Rights and media as soon as possible but no later than 60 days after discovery if it involves ≥500 individuals
  - Office of Civil Rights no later than 60 days after the calendar year of the breach if it affect ≤ 500 individuals

Arizona Data Breach Laws

- State law may require health care organizations to report data breaches
- Arizona data breach statutes
  - Definitions for breach, individual, personal information, and more
  - Notification of breach requirements

Breach Notification Content Requirements

- Written notice to affected individuals
- 1st class U.S. Mail
- Plain language
- Brief description including dates of breach and discovery if known
- Description of type of information involved
- Actions for affected individuals to protect from potential harm
- Brief description of what health care organization is doing to investigate breach, mitigate harm, and prevent future breaches
- Contact information such as toll-free number, email address, website, and U.S. postal address

Rebutting the Breach Presumption

- If unsecured, must demonstrate low probability PHI compromised, including documented risk analysis considering at least the following
  - Nature and extent of PHI (identifiers, likelihood of reidentification)
  - Unauthorized person who used or received PHI
  - Whether PHI was acquired or viewed
  - Extent to which risk has been mitigated
- If encryption protections in place, and investigation confirms data remained encrypted during attack, do not have to conduct risk assessment or notify affected individuals

Preserving Forensic Evidence

- Check cyber liability insurance policy for instructions on reporting ransomware and other malware attacks; cyber insurance carrier may assist with selecting attorney experienced in HIPAA investigations and an information technology company specializing in ransomware remediation and forensic analysis

- Consider reporting ransomware and other malware attacks to your medical professional liability insurance carrier

- Possible to gather forensic evidence to rebut breach presumption and avoid breach notifications - saves time, money, goodwill

Forensic Evidence Dos and Don'ts

- Consult information technology (IT) forensic team (FT) before shutting down network devices or running an anti-virus scans; either may delete valuable forensic information
- Identify viable backups but do not begin system or data restoration until experts start investigation; restoration efforts may destroy valuable forensic information
- Give FT inventory of network devices, and firewall, network, and system logs
- Preserve ransom notes, messages, or communications
- Consult cyber liability insurance carrier and IT team before communicating with attackers or paying a ransom

Lawsuits

- Large data breaches may lead to class action lawsuits
- Lawsuits may allege various state law claims
- Some courts dismissing lawsuits

Risk Reduction Strategies

- Consider cyber liability insurance
  - Contact your broker or medical professional liability insurance carrier customer service representative for more information
- Use HIPAA Security Rule compliance to manage cyber liability risk
  - Medical professional liability insurance and cyber liability insurance carriers may be resources
- Consider ransomware, malware, and post-incident forensics when selecting information technology vendor
- Periodically ask information technology and forensics teams for documentation or other evidence of their work
- Arrange for cybersecurity awareness and response training for all physicians and practice staff
  - Cyber liability insurance carrier risk management departments are a resource

HHS Reference Links

U.S. Department of Health & Human Services

- 2016-2017 HIPAA Audits Industry Report
- 2021 Forecast: The Next Year of Healthcare Cybersecurity
- Basics of Risk Analysis and Risk Management
- Cyberattack Quick-Response Checklist and Infographic
- Cybersecurity Challenges to the Healthcare Sector
- Fact Sheet: Ransomware and HIPAA
- Ransomware Trends 2021

Other Reference Links

- https://healthitsecurity.com/news/hhs-warnshealthpacspatient-datavulnerableto-cyber-exploitation
- https://healthitsecurity.com/news/3-key-entry-points-for-leading-ransomware-hacking-groups
- https://www.himss.org/resources/himss-healthcare-cybersecurity-survey
- https://lewisbrisbois.com/blog/category/data-privacy-cyber-security/ransomware-and-the-paramount-importance-of-evidence-preservation-for-health
- https://www.natlawreview.com/article/hitech-act-amendment-incentivizes-adoption-nist-and-other-recognized-cybersecurity
- https://www.securitymagazine.com/articles/95381-clinical-treatment-of-ransomware-in-healthcare
- https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-in-healthcare-2021-wp.pdf

Resource Links

- HHS website: Information for Professionals on the Security Rule
- HHS Security Risk Assessment Tool
- NIST Introductory Resource Guide for Implementing the HIPAA Security Rule
- HHS: Security 101 for Covered Entities
- HHS: Security Standards: Implementation for the Small Provider
- HHS: Basics of Risk Analysis and Risk Management
- HHS: Health Industry Cybersecurity Practices (Managing Threats and Protecting Patients)
- HHS: Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals
- HHS: Breach Notification Rule Requirements

David Shelley

David Shelley
President, BVA Inc.
David grew up in Washington DC, and has been living in AZ since 2004. He loves helping organizations stay current on cutting edge technology that is reliable, secure, and current. A very transparent individual, fair but stern. Because of his talented staff, it allows him to be a very talented, driven, and competent technology advocate and leader. David has a strong background in project management, technical delivery, and customer relations.

bva technology services

Security is Built in Layers

David Shelley – President and Chief Information Officer for over 50 Organizations

Security Actions To Counteract Ransomware Attacks – Directory and Passwords

- No peer-to-peer network configuration
- Installation of a supportable directory structure for user/device authentication
- All devices need to authenticate to a single directory structure
- Changing passwords frequently - Ensure your organization has a 90-day password policy for all devices and applications
- Passwords needs to be at least 12 character
    - Create a phrase for easy recall
- Passwords need to have the following criteria:
    - At least one upper case letter
    - Number
    - Symbol
    - 10 to 12 characters
    - No passwords reused for three years
- Lock down the users so that they cannot install executables files (.exe)
- Clean up all user accounts, disable or delete old users

Security Actions To Counteract Ransomware Attacks – Two Factor Authentication

- Configure all email platforms for Two Factor Authentication (2FA)
- All production website applications that are leveraged needs to be configured with 2FA
- All production devices that touch production or patient data needs to configured with 2FA, such as:
  - Laptops
  - Desktop towers
  - Tablets
- All Remote Desktop Sessions (RDS) or Citrix connections
  - NEED a VPN in front, no servers open to the web
  - Requires 2FA as well
- VPN connections
- SharePoint, EMR, Box, Dropbox, any file collaboration tool

NOTE: The secondary code can be sent to a mobile device, an external token, or leveraging an authenticator application such as Google Authenticator.

Security Actions To Counteract Ransomware Attacks – Next-Gen Anti-Virus/MTR

- Next-Gen antivirus- takes traditional antivirus software to a new, advanced level of endpoint security protection. It goes beyond known file-based malware signatures and heuristics because it's a system-centric, cloud-based approach. ... Detect and prevent malware and fileless non-malware attacks.
- MTR- Managed Threat Response – this terms refers to a services that provides 24/7 threat hunting, detection, and response capabilities delivered by an expert team as a fully-managed service.
- Popular products that fall within this category:
  - Sophos Intercept X with MTR
  - SentinelOne w/Active EDR/MTR
  - TrendMicro Managed XDR
- These products are constantly scanning for odd behavior and code changes to devices
- Catch and stop keyloggers, mimkatz, and other malicious hacking tools

Security Actions To Counteract Ransomware Attacks – Commercial Grade Firewall

- Your organization needs a commercial grade firewall that has less than 10 vulnerabilities
- **IPS** – Intrusion Protection Service - is a form of network security that works to detect and prevent identified threats. ... The IPS reports these events to system administrators and takes preventative action, such as closing access points and configuring firewalls to prevent future attacks.
- **Geofencing** – a firewall feature that identifies the geographic region where traffic originates. It does this by looking at the IP address of incoming traffic or network requests, each of which is tied to a physical location.
- **Deep Packet Inspection** - addresses the latest ransomware and breaches with high-performance streaming deep packet inspection, including next-gen IPS, web protection, and app control, as well as deep learning and sandboxing.
- **Web Filtering** – lock down what your users can browse to on the web as well as block all designated known malicious content.
- Some great commercial firewalls to consider:
  - Sophos XGS series
  - Cisco ASA series
  - Fortinet Fortigate series
  - Palo Alto

Security Actions To Counteract Ransomware Attacks – Correct Spam Protection Service

- Put a system in place that addresses spam, impersonation protection, threat protection regarding links within emails.
- Ensure this service also backs up all email correspondence
- Make sure that this service is cloud based
- Target Threat Protection – opens links that are in emails sent to you in a "sandbox" framework first to ensure validity before it gets opened on your local browser.
- Impersonation Protection – deals with emails where individuals are impersonating someone else. Typically performed for passwords resets, wire transfers, etc…
- Some great services:
  - Mimecast
  - Sophos
  - Barracuda Networks
  - Proofpoint
  - Cisco

Security Actions To Counteract Ransomware Attacks – Point in Time Back Up Solution

- Ensure that your company has a true commercial grade back up solution that is Point-in-Time.
- Configure the back up to also replicate offsite to a third-party facility.
    - Architect this third-party location so that it can be brought up in less than 6 hours in the event of disaster or local corruption/hack.
- Segregate your local back up solution from your production servers/data.
- Some of the popular solution that work well:
    - Quest Rapid Recovery
    - Veeam Recovery
    - Commvault Back Up and Recovery
    - Newer – Veritas Back Up Exec 21
    - Veritas Netbackup 9

Security Actions To Counteract Ransomware Attacks – Vulnerability Scans & User Training

- Work with a strong security firm and contract a quarterly vulnerability scan for your environment.
  - This will allow your organization to constantly know where open holes are and patch them on a continuous basis.
- *Or* purchase your own vulnerability software like Rapid Fire, etc…and perform your own internal scan.
- Leverage a service to train your staff on what to open and what not to open via email. There are several services out there that will send emails that are Phishing-like communications that ask users for passwords posing as internal personnel/management or internal IT.
  - A report gets sent to management of how many opened and whom.
  - Also sends virtual training to users that opened these email so they can learn from their mistakes.

Security Actions To Counteract Ransomware Attacks – Conclusion and Q&A

- There are a lot of good solutions out there that can address all the points outlined in this presentation, not just what I have recommended via products.
- An organization can install all the best solutions in all facets of their environment, and still be breached and get Ransomware. The most important thing is having a good back up solution that you can recover from quickly, within an establish timeline.
- Ransomware is constantly evolving (monthly)
- Q&A

QUESTIONS

Requesting your Certificate

"How to Counteract Ransomware Attacks on Healthcare"

Please complete the Evaluation via the SurveyMonkey link that has opened in a separate browser window.

Evaluation can also be found at:
https://www.surveymonkey.com/r/RansomSept22SWTRC

This will be posted in the chat at the end of today's program.

Improving Access to Quality Medical Care Webinar Series

Please check our websites for upcoming webinars and events

http://www.telemedicine.arizona

Arizona Telemedicine Program

Arizona Department of Health Services

Southwest Telehealth TRC Resource · Center™

maricopa county medical society

Your opinion is valuable to us.
Please participate in this brief survey:

https://www.surveymonkey.com/r/RansomSept22SWTRC

This webinar series is made possible through funding provided by Health Resources and Services Administration, Office for the Advancement of Telehealth and the Arizona Department of Health Services