

# Security Risk Analysis

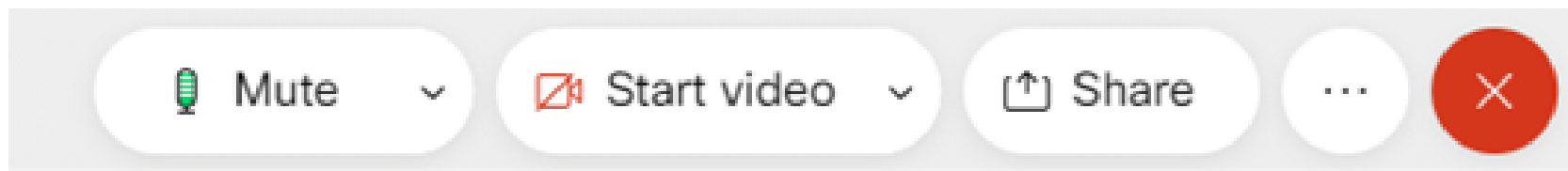
**Why it's more important now than ever!**

# Muting and Unmuting Audio

To mute your audio, click the microphone icon at the bottom of your screen (icon will turn red).

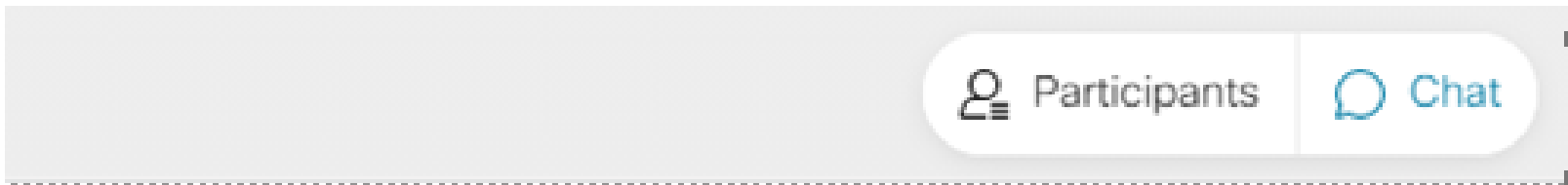
To unmute, click the microphone icon again.

If your icon is green, you are unmuted.



# Chat Panel

Click on the “chat” icon at the bottom right of your screen to open the chat panel



To send a question or comment:

1. Select “Everyone” from the **To:** dropdown list
2. Click in the chat box and type a question or comment
3. Click **Enter**

## Meet our Team



**Gary Carder, BA, CIT, RRT**  
Health IT Consultant



# About KFMC

- KFMC has been supporting practices with the Meaningful Use/Promoting Interoperability programs for over 10 years.
- During this time, KFMC's Health IT consultants helped over 1,600 Kansas providers select, implement, and meaningfully use Health Information Technology.
- This assistance includes Promoting Interoperability attestation, Security Risk Analysis, Policies and Procedures - review, development, and updating, along with process workflow and redesign.





# Why Now?

- Ransomware attacks on healthcare providers rose 350% in 4<sup>th</sup> quarter 2019<sup>1</sup>.
- Providers were the target of 79% of the cybersecurity healthcare breaches in 2020<sup>2</sup>.
- Now is not the time to relax on practice security.
- The Office for Civil Rights (OCR) requires periodic Security Risk Analysis. Recommendation is yearly, and whenever there is a significant change in your infrastructure.

<sup>1</sup><https://healthitsecurity.com/news/ransomware-attacks-on-healthcare-providers-rose-350-in-q4-2019>

<sup>2</sup> <https://fortifiedhealthsecurity.com/pressreleases/fortified-health-security-releases-2021-horizon-report/>



# Current Statistics from HHS.gov

- From April 2003 to June 2020 the most alleged complaints include
  - Impermissible uses and disclosures of protected health information (PHI)
  - Lack of safeguards for PHI
  - Lack of patient access to their PHI
  - Lack of administrative safeguards for PHI
  - Use or disclosure of more than the minimum necessary PHI
- Top two most common covered entities alleged to have committed violations
  - General Hospitals
  - Private Practices and Physicians



# Recent Monetary Penalties

## The practice of Steven A. Porter, M.D., Ogden, Utah

- \$100,000
- OCR Investigation post breach reporting
- OCR found that Dr. Porter had never done a Security Risk Analysis at the time of the report, and failed to do one or implement corrective actions after reporting the breach

## Rural Eastern Kansas hospital

- \$250,000
- Falsely attested to performing a Security Risk Analysis
- Whistleblower earned \$50,000
- ONC assessed the fine even though no breach had occurred





# Office of Civil Rights

“All health care providers, large and small, need to take their HIPAA obligations seriously,” said OCR Director Roger Severino. “The failure to implement basic HIPAA requirements, such as an accurate and thorough risk analysis and risk management plan, continues to be an unacceptable and disturbing trend within the health care industry.”



# Penalties

<b>Violation category— Section 1176(a)(1)</b>	<b>Each violation</b>	<b>All such violations of an identical provision in a calendar year</b>
(A) Did Not Know	\$100-\$50,000	\$1,500,000
(B) Reasonable Cause	1,000-50,000	1,500,000
(C)(i) Willful Neglect- Corrected	10,000- 50,000	1,500,000
(C)(ii) Willful Neglect- Not Corrected	50,000	1,500,000

<https://www.federalregister.gov/documents/2013/01/25/2013-01073/modifications-to-the-hipaa-privacy-security-enforcement-and-breach-notification-rules-under-the#h-95>



# Impact of COVID-19

- Large movement towards remote work/work from home
- New adoption or increased use of telehealth with some relaxed restrictions at this time<sup>1</sup>
- **Both increase your attack surface**
- **Security risk analysis must be updated to reflect these new vulnerabilities.**

<sup>1</sup> <https://www.telehealth.hhs.gov/providers/policy-changes-during-the-covid-19-public-health-emergency/#incorporating-newly-allowed-technology-due-to-hipaa-flexibility>



# Components of Security Risk Analysis

- Identify Risks
  - Security Management Process
  - Workforce Security
  - Information Access Management
  - Encryption
  - Integrity
  - Facility Access Controls
  - Business Associates
  - Contingency Plans
- Risk Scores
  - Likelihood
  - Impact
- Risk Prioritization
- Risk Remediation






# Documentation

- Leadership Approval
- SRA Retention
- Business Associate Agreements
- Asset Inventory
- Risk Remediation







A good Security Risk Analysis is not “one and done.” Risk remediation should be an ongoing activity and documented.



# Questions?



# SRA+

For more information and to see a demo, visit our website at <https://www.sraplus.com/>



# For More Information Contact

**Gary Carder**  
**The Kansas Foundation for Medical Care, Inc.**  
**800 SW Jackson St., Suite 700**  
**Topeka, Kansas 66612**  
**785.271.4175**  
**[gcarder@kfmc.org](mailto:gcarder@kfmc.org)**



***Better health outcomes for everyone.***