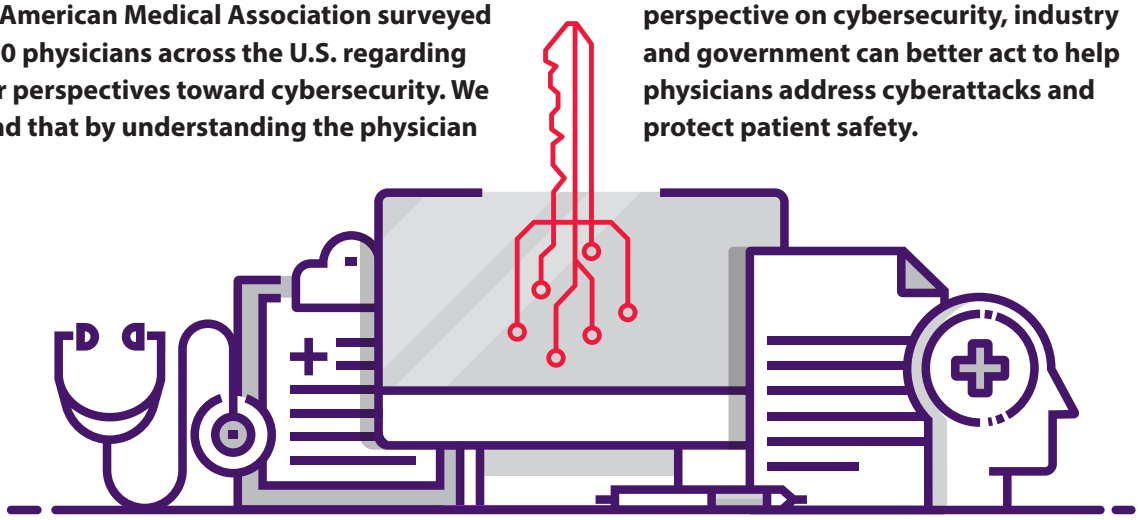
AMA
AMERICAN MEDICAL ASSOCIATION

PATIENT SAFETY: THE IMPORTANCE OF

CYBERSECURITY IN HEALTH CARE

The American Medical Association surveyed 1,300 physicians across the U.S. regarding their perspectives toward cybersecurity. We found that by understanding the physician perspective on cybersecurity, industry and government can better act to help physicians address cyberattacks and protect patient safety.



CYBERSECURITY IS NOT JUST A TECHNICAL ISSUE, IT'S A PATIENT SAFETY ISSUE.

Physicians' top three concerns about cyberattacks are:

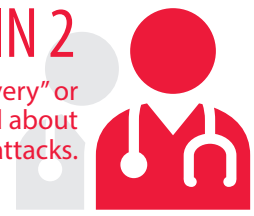
1. **74%** Interruptions in practice operations
2. **74%** Compromised EHR security
3. **53%** Threats to patient safety

CYBERATTACKS ARE INEVITABLE.

Physicians recognize that *it's not a matter of if*, but *when* they will experience a cyberattack.

83% Have experienced some form of cyberattack.

1 IN 2 Physicians is "very" or "extremely" concerned about future cyberattacks.



83% Physicians see the value of a security risk assessment and recognize that HIPAA isn't enough to truly address cyber threats.

PHYSICIANS ARE NOT SECURITY EXPERTS.

The industry needs to understand the physician perspective on security.

ONLY
20%
Of small practices have internal security officers, so they typically rely on—and trust—third-parties like health IT vendors for security support.

OVER
1/3
Of physicians are interested in shared security management solutions.

NEARLY
1 IN 2
Physicians wish they could receive donated security-related hardware or software from other provider groups.

TO SECURELY SHARE DATA, WE NEED TO WORK TOGETHER.

Integrated, value-based care models are only as strong as their weakest link—ensuring the health care community speaks a common language and physician practices exercise good cyber hygiene are important to the entire health ecosystem.

Of physicians believe it is "very" or "extremely" important to share electronic protected health information (ePHI) to provide quality care—they just want to do it safely and within their means.

The federal government should reframe a physician's approach to security by using positive incentives—not just penalties—to encourage physicians to bolster their security practices.

- Create improvement activities within the Merit-based Incentive Payment System that provide physicians with credit for implementing good cyber hygiene.
- Accept a cybersecurity framework as a "reasonable and appropriate" way to meet HIPAA's security risk analysis requirement and be exempt from random HIPAA security audits.
- Create Stark exception and AKS safe harbor to permit sharing services and technology to facilitate secure information sharing among health care providers.