
AMA
AMERICAN MEDICAL ASSOCIATION
Cybersecurity:
A Patient Safety Issue
Your MISSION is Our MISSION

# Cybersecurity research project scope



- **Exhaustive literature search** to understand physician perspectives and awareness on issues of security or lack thereof.
- **Physician and industry thought leader interviews** to establish key themes, concerns, and levels of awareness.
- **Quantitative survey,** supplemented and informed by literature search and qualitative interviews, to validate understanding and confirm themes.
- **Synthesis of results** and collaboration on recommendations to inform AMA strategy and advocacy efforts.

# CYBERSECURITY IS A PATIENT SAFETY ISSUE

Not a matter of if, but when, an attack happens

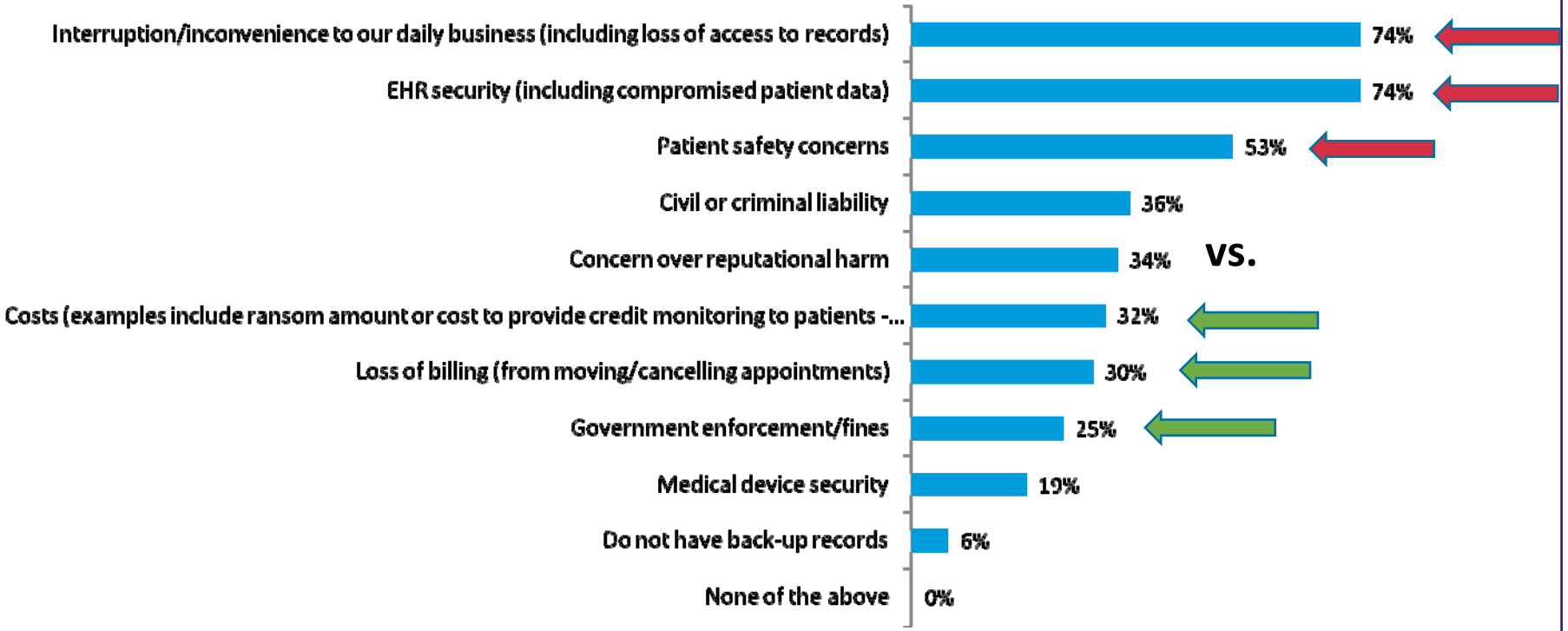
Understand and act

If we want to share data, we have to work together

# How does cybersecurity impact  patient safety?

- Ransomware
  - Limited access to critical care information
- Stolen patient identities
  - Difficult to amend health records
  - Downstream effects impact patient care
- Compromised medical device software
  - Device malfunction

# What concerns you most about future attacks?
## *Select up to five.*



## ECRI's top 10 tech hazards for 2018, security gaps, dirty scopes make the list

ECRI Institute weighed factors like severity, likelihood that the hazard could cause serious injury or death, frequency, overall likelihood and preventability.

## 1. Cybersecurity threats in healthcare delivery and patient endangerment

In the healthcare environment, ransomware and other types of malware attacks constitute potential patient safety crises that can put patients' lives in jeopardy by stalling or halting operations and care delivery. Disruptions can include compromising patient care with canceled procedures, workflow changes, closure of care units or information data breaches.

HEALTH CARE INDUSTRY CYBERSECURITY TASK FORCE

**REPORT ON IMPROVING CYBERSECURITY IN THE HEALTH CARE INDUSTRY**

"The [recommendations] reflect a shared understanding that for the health care industry cybersecurity issues are, at their heart, patient safety issues."

# Changing the national conversation

- Historical approach: cybersecurity is a technical issue focused on compliance.
  - Health IT developers focus on technical issues.
  - Health systems focus on internal security measures.
  - The federal government focuses on regulatory compliance.
- The health care community must “speak a common language” to underscore that cybersecurity is not just a technical issue, it’s a patient safety issue.

# CYBERSECURITY IS A PATIENT SAFETY ISSUE

**Not a matter of if, but when, an attack happens**

Understand and act

If we want to share data, we have to work together

# Cyber attacks are inevitable

- 83% of physician practices report they have experienced some form of cybersecurity attack.
    - Inappropriate employee use and disclosure are more of a concern among larger health systems (e.g., inappropriate use of patient records, sharing/selling patient information).*
    - Phishing and viruses are the most common cyber attacks in small practices.
- One out of two physicians surveyed are “very” or “extremely” concerned about future cyber attacks in their practice.

*source: qualitative interviews

# Positive incentive opportunity: cyber frameworks

- 83% of physicians see the value of a security risk assessment but say HIPAA isn't enough to truly address cyber threats.
- Physicians have historically struggled to meet security risk analysis requirements.
- 70% of physicians would be willing to pay for someone to implement a robust security framework if adoption meant that they would not be randomly audited under HIPAA.
  - Security frameworks help to identify what risk management mechanisms are reasonable and appropriate.

# Positive incentive opportunity: cyber frameworks

- Most of HIPAA utilizes a “reasonable and appropriate” standard for privacy and security controls.
- OCR should accept as “reasonable and appropriate” a physician’s use of a cybersecurity framework to:
  - meet the physician’s obligation under HIPAA and ACI to conduct a security risk analysis; and/or
  - be exempt from random HIPAA security audits.

# CYBERSECURITY IS A PATIENT SAFETY ISSUE

Not a matter of if, but when, an attack happens

**Understand and act**

If we want to share data, we have to work together

# Understand the physician perspective and act to help protect patient safety

- Industry and government should understand the physician perspective and why physicians struggle with security.
  - Only 20% of small practices have internal security officers, leading to heavy reliance on health IT vendors for security support.
  - More than one in three physicians of all practice sizes obtain training from their health IT vendor.

# Physicians need tools, not just trust

- What could help?

✓Tips for good cyber hygiene

✓Simplify language and complex rules

✓HIPAA summaries

✓“How to” guide for Security Risk Assessments

- Physicians prefer to learn through Continuing Medical Education (CME), online tools, and websites.

# CYBERSECURITY IS A PATIENT SAFETY ISSUE

Not a matter of if, but when, an attack happens

Understand and act

**If we want to share data, we have to work together**

# Information sharing is key to value-based care

- Recall: 85% of physicians believe it is “very” or “extremely” important to share ePHI to provide quality care–they just want to do it safely.

- Two-thirds believe greater access to patient data would help provide quality patient care more efficiently.
- Weak cyber hygiene could limit the ability of physician practices to participate in integrated, value-based care models.

# Positive incentive opportunity: resource sharing

- Over one-third of physicians in small practices are interested in shared security management solutions.
- Almost 1 in 2 physicians in small practices wish they could receive donated security-related hardware or software from other provider groups.
- The Federal government should create a Stark exception and an Anti-Kickback Statute (AKS) safe harbor to permit sharing services and technology to facilitate secure information sharing among healthcare providers.

# Other AMA cybersecurity activities

- Developed resources to help physicians conduct a checkup of their systems, and to secure their networks and office computers
- Proposed to the Centers for Medicare & Medicaid Services improvement activities under the Merit-based Incentive Payment System (MIPS) to give credit to physicians who voluntarily adopt a cybersecurity framework and/or perform other cyber hygiene activities Drafted comments urging NIST to develop tools to help small practices implement the NIST cybersecurity framework
- Encouraged the Office of Civil Rights to provide protections to physicians who voluntarily adopt cybersecurity frameworks
- Urged stakeholders to develop tools to help small practices implement best practices and adopt cybersecurity frameworks
- Raised concerns to the U.S. Food and Drug Administration about device cybersecurity and the need to maintain security of data sent to electronic health records
- Engaged with the HHS Office of the Secretary on the importance of educating physicians on cybersecurity
- Highlighted importance of cybersecurity across modalities of care (e.g., telemedicine) to specialties
- Engaged with the administration to monitor and disseminate information to physicians about ransomware and the recent “WannaCry” and “Petya/Non-Petya” cyberattacks
- Joined an Advisory Committee for the Health Information Trust (HITRUST) Alliance’s Common Security Framework to provide the physician perspective, including small and mid-sized practices
- Partnered with HITRUST to provide cybersecurity education and practical advice to small and mid-sized practices across the country
- Providing ongoing feedback to Congress on proposed cybersecurity legislation
- Coordinating ongoing advocacy efforts with health professional organizations

# Contact Information


- Laura G. Hoffman
  - Assistant Director, Federal Affairs
  - American Medical Association
  - Laura.Hoffman@ama-assn.org