HIMSS®18
The leading health information and technology conference
WHERE THE WORLD CONNECTS FOR HEALTH

Conference & Exhibition | March 5–9, 2018
Las Vegas | Venetian – Palazzo – Sands Expo Center

Physician Awareness, Preparedness, and Perception of HIPAA and Cybersecurity

Session #255, March 8, 2018

Laura G. Hoffman, Assistant Director, Federal Affairs
Maithili Jha, Manager, Environmental Intelligence and Strategic Analysis
American Medical Association

DISCLAIMER: The views and opinions expressed in this presentation are those of the author and do not necessarily represent official policy or position of HIMSS.

Conflict of Interest

Neither Laura Hoffman, JD, nor Maithili Jha, MPH have any real or apparent conflicts of interest to report.

Agenda

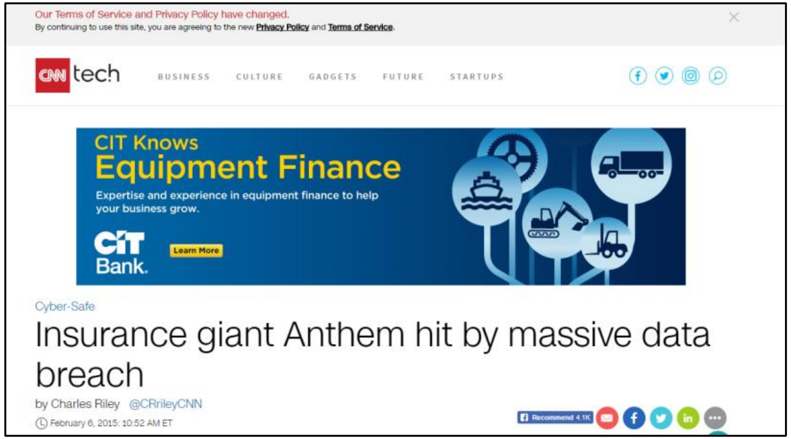
- Overview of AMA cybersecurity study
- Impact of findings
- Takeaways for the health IT industry

Learning Objectives

- Identify physicians’ desire to be empowered advocates for their patients
- Understand small and medium-sized medical practices require additional—and often unique—resources, tools, and support to bolster their cyber hygiene
- Recognize an increasingly interconnected heath system requires the entire medical community to be resilient
- Learn how stakeholders share a responsibility to secure electronic patient information
- Demonstrate the AMA’s role in shaping the national cybersecurity conversation to focus on patient safety

News

2015



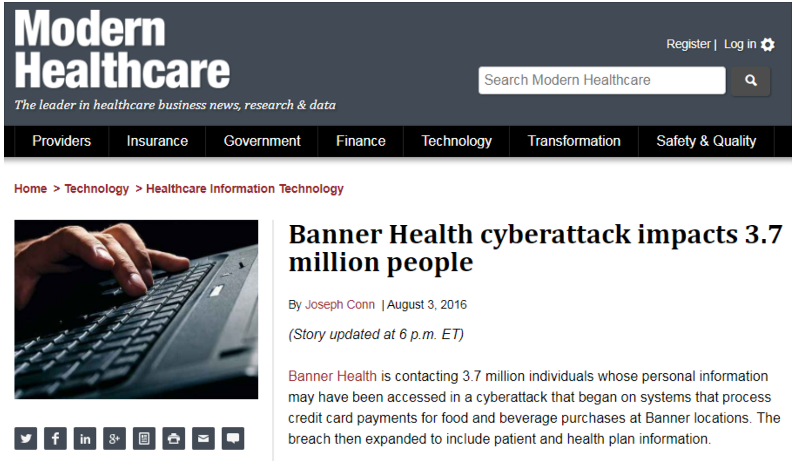
Our Terms of Service and Privacy Policy have changed.
By continuing to use this site, you are agreeing to the new **Privacy Policy** and **Terms of Service**.

Cyber-Safe

Insurance giant Anthem hit by massive data breach

by Charles Riley @CRrileyCNN
February 6, 2015: 10:52 AM ET

2016



Home > Technology > Healthcare Information Technology

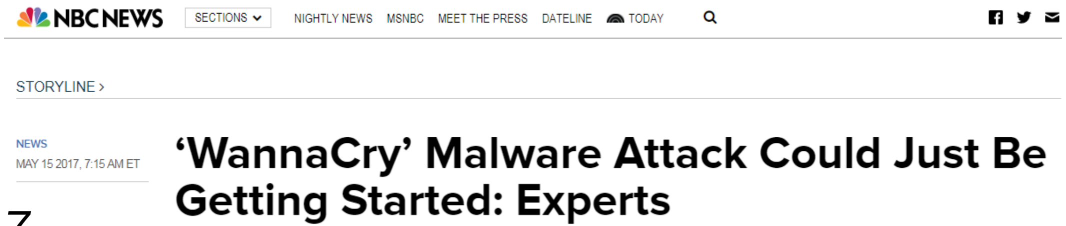
Banner Health cyberattack impacts 3.7 million people

By Joseph Conn | August 3, 2016

(Story updated at 6 p.m. ET)

Banner Health is contacting 3.7 million individuals whose personal information may have been accessed in a cyberattack that began on systems that process credit card payments for food and beverage purchases at Banner locations. The breach then expanded to include patient and health plan information.

2017



STORYLINE >

NEWS
MAY 15 2017, 7:15 AM ET

‘WannaCry’ Malware Attack Could Just Be Getting Started: Experts

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.

Key themes of research

- Physician awareness and understanding of HIPAA and the cyber threat element
- Physician preparedness for cyber threats
- Physician response to cyber threats
- Policy and regulatory activity related to privacy and security that impacts physicians
- Vendor response with specific emphasis on offerings for various sized medical practices

Literature search conclusions

- The physicians' voice is underrepresented in the current universe of health cybersecurity research.
- Anecdotal evidence of physicians'
  - awareness of risk
  - recognition of the importance of ePHI security
  - basic actions to protect ePHI
  - desire for further education and toolkits
  - familiarity with HIPAA regulations and requirements
  - need for and lack of focused resources from outside vendors

Screeners and quotas

- Hospital Affiliation
- Size of Practice
- Practice Area/Specialty
- Age
- Practice Ownership
- Physician Ownership
- Years Practicing Medicine
- Hours Per Week of Patient Care
- Gender
- Practice Physician Count
- Hospital Employed
- Practice Type

Findings

Qualitative Themes	Supported by Quantitative Results
Most physicians interviewed experienced some type of cyber attack.	83% of physician practices report they have experienced some form of cybersecurity attack.
Physicians are very concerned about future cyber attacks and expect them to get worse, not better.	The majority of physicians surveyed (55%) are very or extremely concerned about future cyber attacks in their practice.
Physicians believe they follow HIPAA. They trust that their security experts are doing the right thing.	87% are confident that their practice is HIPAA compliant.

Qualitative Themes	Supported by Quantitative Results
Physicians obtain training from various sources. Hours spent on training vary widely.	37% obtain training from their health IT vendor, 18% from another third-party. Most spend 2 hours in HIPAA training.
Physicians generally realize the value of EHRs and the need for HIPAA compliance, but struggle with the processes.	85% believe it is very or extremely important to share ePHI outside of their health system to provide quality care.
Physicians struggle with obtaining and sending patient data among siloed systems.	Two-thirds say greater access to ePHI would help provide quality patient care more efficiently.

Practice Size	Characteristics	Cybersecurity Highlights
Small (1-25 physicians)	• 46% primary care • 100% wholly owned by practice physicians • 63% practicing more than 15 years	• 32% say they have not experienced a cyber attack that they know of. • 56% extremely/very concerned about future cyber attacks. • Cost is reason for not having cyber insurance (37% vs. 21% large). • 52% conduct an SRA once per year or more.
Medium (26-50 physicians)	• 66% specialty care • 76% wholly owned by a hospital • 58% age 36-50 • 74% practicing 15 years or less	• 89% have experienced a cyber attack. • Medium practices are 2X more likely to experience insider attacks compared to small practices (43% vs. 20%). • 63% extremely/very concerned about future cyber attacks. • Most likely to have cyber insurance (42% vs. 22% small and 25% large). • 53% conduct an SRA once per year or more.
Large (50+ physicians)	• 60%/40% specialty/primary care • 59% wholly owned by a hospital • 52% over 50 years of age	• 90% have experienced a cyber attack. • Large practices are 2X more likely to experience an insider attack compared to small practices (47% vs. 20%). • 48% extremely/very concerned about future cyber attacks. • 48% conduct an SRA once per year or more.

Takeaways

CYBERSECURITY IS A PATIENT SAFETY ISSUE

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

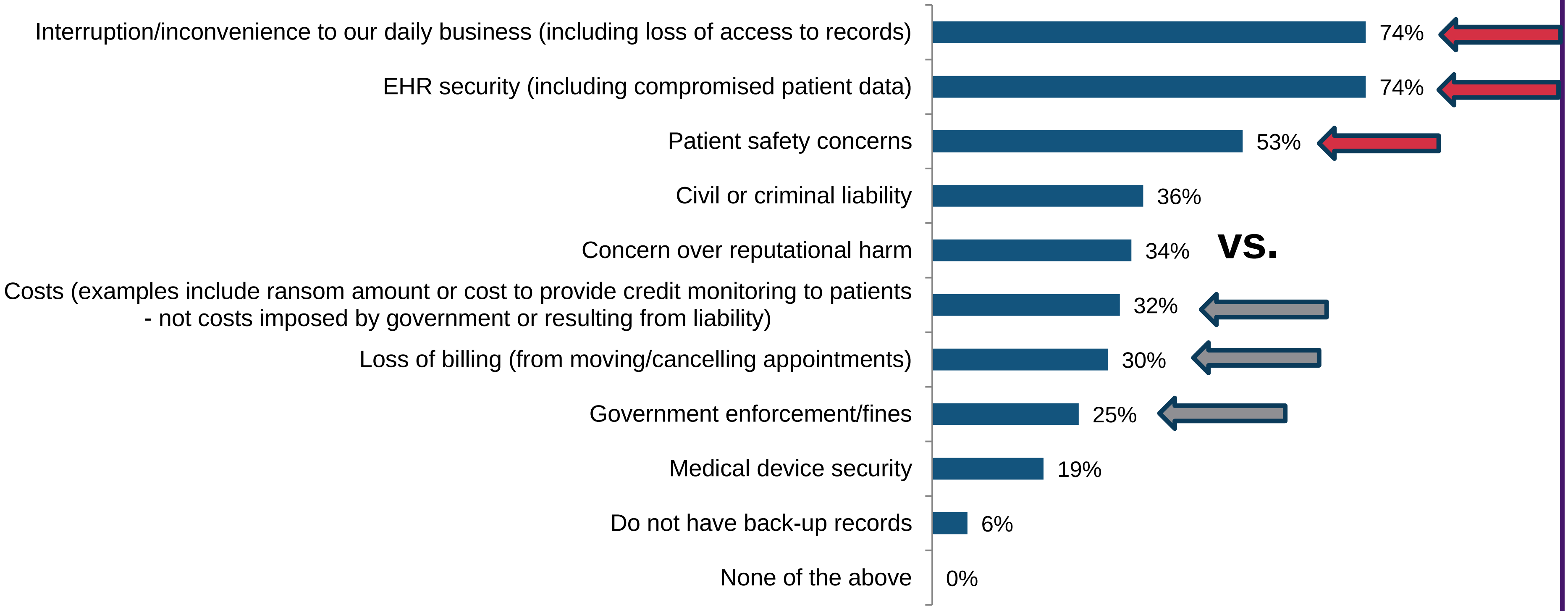
Understand and act

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, but also 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

What percentage of physicians have experienced a cyber attack?

1. 40%
2. 83%
3. 68%
4. 74%

https://live.eventbase.com/polls?event=himss2018&polls=4283

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

A wide array of efforts…

- NIST
- OCR
- ONC
- DHS
- FDA
- FBI

- HITRUST
- HCCIC
- NCCIC
- NH-ISAC
- HHS CISO
- Consultants
- State laws

- HiMSS
- Health IT vendors

Understand the physician perspective and act to help protect patient safety

- Industry and government must 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.
- Framing the issue as one of patient safety helps to translate the complexity of cybersecurity to real-world needs and actions for physicians.

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.

What’s the most important security tool for a physician?

1. A security risk analysis
2. A cybersecurity framework
3. Ongoing security training
4. Two-factor authentication

https://live.eventbase.com/polls?event=himss2018&polls=4284

CYBERSECURITY IS A PATIENT SAFETY ISSUE

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

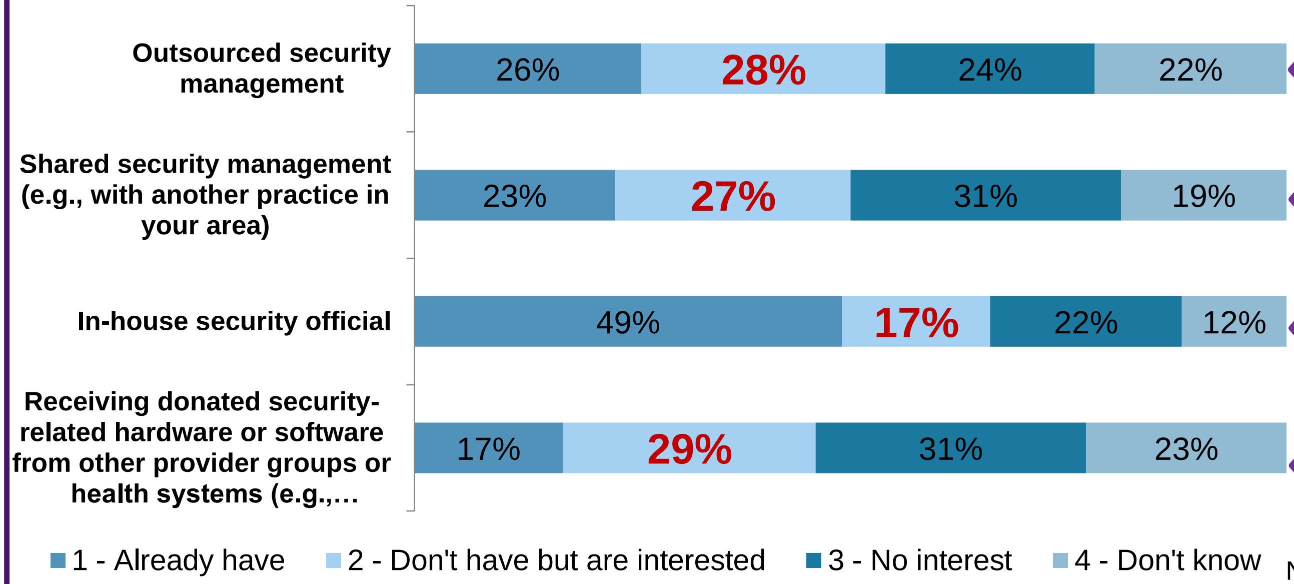
Understand and act

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.

Which of the following does your practice have or would your practice be interested in?



40% of small practices don’t have but are interested.

34% of small practices don’t have but are interested.

More than 60% of medium and large practices have; 20% small practices have.

46% of small practices don’t have but are interested.

Note: Small=1-25, medium = 26-50, large = 51+

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.

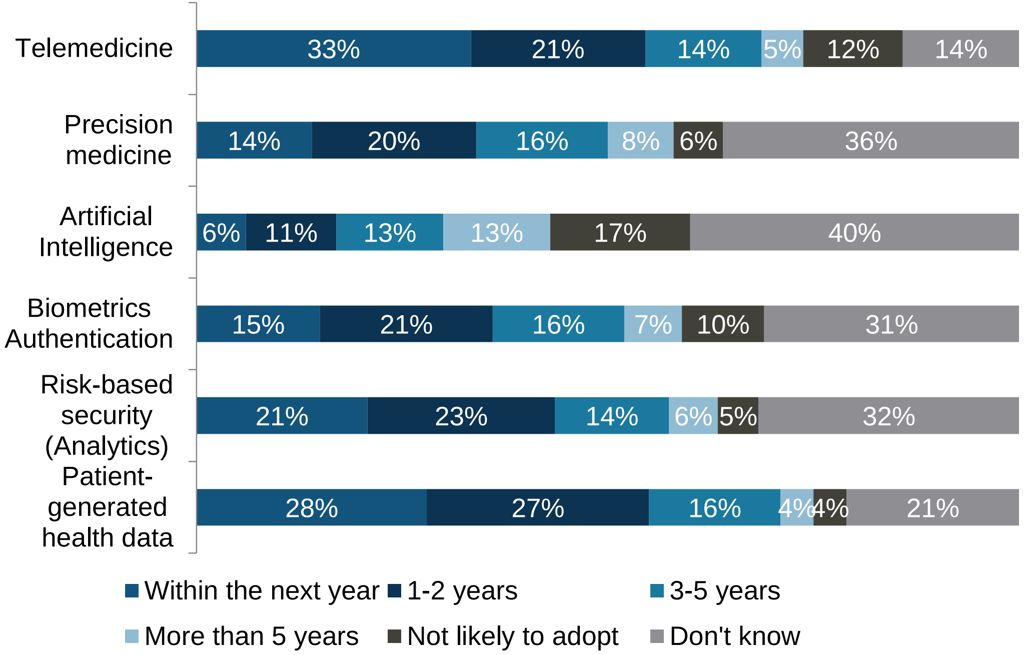
Looking forward

What technologies need more privacy and security attention?

1. APIs and connecting apps
2. HIEs
3. Telemedicine
4. Remote patient monitoring

https://live.eventbase.com/polls?event=himss2018&polls=4285

Please indicate when you are likely to adopt each of the following into your practice.



Likely to adopt within the next year

	Small	Med	Large
Telemedicine	15%	36%	46%
Precision med	9%	22%	13%
AI	2%	11%	5%
Biometrics	8%	22%	15%
Risk-based security	13%	27%	21%
Patient-gen health data	23%	30%	30%

33% indicate a likelihood of adopting telemedicine within the next year.

Likelihood of adopting telemedicine within the next year, by practice size:

Small	Medium	Large
15%	36%	46%

Likelihood of adopting telemedicine within the next year, by specialty:

Family/GP	Pediatrics	Internal Medicine
21%	16%	15%

28% of practices are likely to adopt patient-generated health data within the next year, by practice size.

Percentage that plan to use **patient-generated health data** by practice size:

Small	Medium	Large
23%	30%	30%

33% of practices are talking to health IT vendors to prepare for telemedicine and patient generated health data.

	Small	Medium	Large
Telemedicine	36%	33%	32%
Patient-generated health data	41%	26%	32%

Current AMA advocacy efforts

AMA cybersecurity advocacy activities

- Developed resources to help physicians understand cybersecurity, including how to conduct a checkup of their systems and secure their office networks and computers.
- Proposed an improvement activity under the Merit-based Incentive Payment System (MIPS) to give credit to physicians who voluntarily adopt a cybersecurity framework.
- Drafted comments urging NIST to develop tools to help small practices implement the NIST cybersecurity framework.
- 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.

AMA cybersecurity advocacy activities

- 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 other cyberattacks.
- 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 advocacy efforts with health professional organizations.

Questions?

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

- Maithili Jha
  - Manager, Environmental Intelligence and Strategic Analysis
  - American Medical Association
  - Maithili.Jha@ama-assn.org

- Reminder: Please complete online session evaluation!