MICHIGAN MUNICIPAL RISK MANAGEMENT AUTHORITY

THE RISK JOURNAL

A PUBLICATION FOR MMRMA MEMBERS AUGUST 2023

RISKS IN MEDICAL CARE, PART 7

Managing and Minimizing Technology Risks in Health Care

by Cindy King, Director of Membership Services and Human Resources

MMRMA's RAP and CAP grants are valuable tools that help fund member projects to reduce technology risks.

CYBER EXPERTS CAUTION that it is not a matter of *if* any given organization will experience a cyberattack, but instead a matter of *when.* Healthcare providers are no exception, and it is the responsibility of everyone within medical care environments to help mitigate or reduce risk. MMRMA provides both the tools and guidance to assist in members' risk management efforts.

MMRMA grant opportunities

Our Risk Avoidance Program (RAP) and Certification and Accreditation Program (CAP) grants are two such tools to reduce technology risk for healthcare providers (and all members). MMRMA staff and the Membership Committee have identified key areas in which accessing grant funds can be streamlined via our "standard grants." These include several aimed at mitigating cyber or technology risks, such as:

- Cybersecurity training for employees
- Vulnerability assessment/ penetration testing
- Two/multifactor authentication
- Emergency funding to address immediate threats.

The application process is far less complex than federal or other types of grants. When a risk mitigation project falls under the standard grant criteria, the member is assured of receiving funding as long as funds remain in the quarterly funding cycle. Go to **www.mmrma.org** and log in to access RAP/CAP grant guidelines and application forms.

Protecting sensitive data

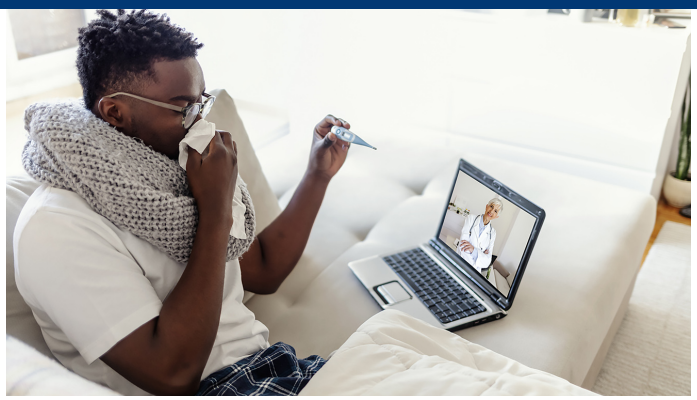
Technology risks include data breaches, compromised email, and ransomware attacks. Potentially, these crimes can significantly impede the delivery of healthcare services, interrupt routine business operations, and prevent staff from accessing systems and patient information. Attacks could also lead to compromised or stolen personal or sensitive patient information.

Resolving cyber incidents once they occur and restoring normal business operations can be extremely costly. Data breaches and other cyber incidents could also expose an organization to litigation. Cybercrime-related attacks can also result in reputational damage, have regulatory ramifications, and result in loss of business if patients choose to seek another healthcare provider.

According to cybersecurity consulting firm Rehmann, "The medical field has the highest cost per breached record at $429 each, due to the records containing personally identifiable information (PII)." Rehmann estimates that "the average U.S. primary care physician has almost $1 million in potential exposure from a security incident." [1]

continued on page 2

1 https://www.rehmann.com/resource/make-cybersecurity-a-priority-in-your-organization/



Technology Risks, continued from page 1

Impacts on care and treatment

Galen Data, a provider for cloud-connected medical devices, lists other technology risks, including altered data that could result in incorrect healthcare decisions, changes in device technology causing adverse results, risk of miscommunication, and poor implementation of technology, noting that "80% of Americans [have had] at least one frustrating experience with technology." [2]

ECRI, a nonprofit healthcare industry advocate, points to other technology risks—supply chain shortfalls, inadequate emergency stockpiles, and wi-fi dead zones—each of which could have a significant impact on patient care that can lead to compromised patient safety, delays in receiving care, injuries, or even death.

Smart medical devices pose additional technological risks. Such devices are used to monitor or measure any number of health criteria, such as blood pressure, glucose levels, and medication dosing.

According to the FDA, "Most [smart devices] contain software and connect to the internet, hospital networks, your mobile phone, or other devices to share information… [including devices] that are implantable or wearable or used at home or in health care settings." [3]

Artificial intelligence in medical settings

An emerging technology risk garnering significant attention is that of artificial intelligence (AI). Good Rx Health cites ways that AI is being used in healthcare settings, including to "assist in cancer detection and analyze medical images for diagnoses" with improved speed and accuracy.

The article also shares some associated pitfalls: "AI models can be biased and lead to incorrect or incomplete diagnoses…Healthcare professionals need to understand the limitations of AI and only use it in combination with their clinical judgment." [4]

Risks related to telehealth

Technology makes possible the use of telemedicine, which can be particularly helpful for those who live in rural or underserved areas where access to physicians and healthcare facilities may be difficult. Patient portals have provided easy and convenient access for interacting with medical professionals. Patients are able to schedule appointments, review test results, refill prescriptions, and track medical history.

However, as noted in *U.S. News & World Report,* "Technology can't replace the warmth of human interaction." The article also notes that "test results can be—at best—difficult to interpret, and at worst, lead to devastating news" that would be better delivered by medical professionals who can "interpret these results into something meaningful" for patients.

Technology can be a useful tool but, as the article cautions, "using it as a total solution will…have consequences that were unanticipated." [5]

2 https://galendata.com/disadvantages-of-technology-in-healthcare/

3 https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity

4 https://www.goodrx.com/healthcare-access/digital-health/ai-and-healthcare

5 https://health.usnews.com/health-care/for-better/articles/pros-and-cons-of-technology-in-health-care

Cybersecurity Best Practices

- **Develop comprehensive cybersecurity policies, train employees on them, and stress their importance in protecting the organization and patients.**
- **Secure computers, services and wireless networks.**
- **Use antivirus and anti-spyware protection.**
- **Update software to the latest versions.**
- **Use data backups and offsite or remote storage.**
- **Implement two/multifactor authentication.**

Medical Device Best Practices

- **Create unique passwords and do not share with others.**
- **Keep devices within your physical control.**
- **Only connect a device to other devices and software if the device manufacturer or healthcare provider indicates it is okay to do so.**
- **Regularly update devices to install patches and fixes for new cybersecurity risks.**
- **Check with the manufacturer about best practices specific to the device.**
- **Call the manufacturer if a device performs strangely or inconsistently.**
- **Follow up on alerts from the device.**
- **Enlist the help of family or caregivers if the patient is not tech savvy.**

More Resources

https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity

Understanding Michigan's New Hands-Free Driving Law

by Cindy King, Director of Membership Services and Human Resources

The new law makes it illegal to talk on the phone, send text messages, take or view videos, or post to social media sites while driving.

EFFECTIVE JUNE 30, 2023, Michigan joined many other states in adopting laws governing the use of cell phones and other devices to discourage distracted driving and help reduce accidents. According to Bridge Michigan, "The law comes amid an increase in traffic deaths that experts blame on distracted and drunk driving. In 2022, fatalities in Michigan rose to 1,133 up from 985 in 2019." [1]

Public Acts 39, 40 and 41 of 2023 prohibit "using a mobile electronic device to do any task, including, but not limited to, any of the following:

> Sending or receiving a telephone call.

> Sending, receiving, or reading a text message.

> Viewing, recording, or transmitting a video.

> Accessing, reading, or posting to a social networking site.

The new law defines operating a motor vehicle as: "To drive or assume physical control of a motor vehicle on a public way, street, road, or highway. This would include times when the vehicle is not moving temporarily because of traffic, road conditions, or a traffic light or stop sign, but would not apply to a vehicle that is legally parked."

Permitted actions

The law permits the following:

Using a device for emergency purposes, including calling, or texting a 9-1-1 system or making an emergency call to a law enforcement agency, healthcare provider, fire department, or other emergency services entity to report any of the following:

> A medical emergency, traffic accident, serious road hazard, fire, or hazardous materials emergency.

> Someone driving in a reckless or unsafe manner or who appears to be under the influence of alcohol or drugs.

> A crime being committed.

Using a global positioning system (GPS) or navigation feature as long as information is not entered by hand.

Using a device in a voice-operated or hands-free mode as long as the driver does not use their hands to operate it beyond:

> Using a single button press, tap, or swipe to activate or deactivate a function of the device or to select a name or phone number.

> Using the permanently installed user interfaces of a device that is integrated into the motor vehicle.

The law does not apply to law enforcement officers, firefighters, paramedics, EMTs, and others who use the device while carrying out official duties.

The State of Michigan website answers some Frequently Asked Questions [2] and has the full text of the law. [3]

Younger people delay driving

The new law comes at a time when teenagers are delaying getting driver's licenses. As reported by the *Washington Post,* "In 1997, 43 percent of 16-year-olds and 62 percent of 17-year-olds had driver's licenses. In 2020, those numbers had fallen to 25 percent and 45 percent."

"Anecdotally, we're hearing that younger people aren't driving or getting their licenses as quickly as in the past," said Mark Friedlander, director of communications at the Insurance Information Institute.

The trend is most pronounced for teens, but even older Gen Z members lag behind their millennial counterparts. In 1997, almost 90 percent of 20- to 25-year-olds had licenses; in 2020, it was only 80 percent." [4]

Updated resource to come

MMRMA insures nearly 18,000 vehicles, and it is every member's responsibility to ensure that policies and employee training align with new legal requirements. To assist members, MMRMA is updating its *Distracted Driving Model Policy and Guidelines* to reflect changes in the law. Once available, we will upload it to the My Documents section of the MMRMA member portal.

1 https://www.bridgemi.com/michigan-government/michigan-police-go-slow-writing-tickets-new-hands-free-driving-law
2 https://www.michigan.gov/msp/divisions/ohsp/safety-programs/distracted-driving
3 http://legislature.mi.gov/doc.aspx?mcl-257-602b
4 https://www.washingtonpost.com/climate-solutions/2023/02/13/gen-z-driving-less-uber/

RISK MICHIGAN MUNICIPAL RISK MANAGEMENT AUTHORITY

Learn Leadership, Empowerment Skills at Annual Meeting

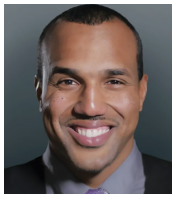
Port Huron's Blue Water Sandfest is Michigan's first sand-sculpting festival and one of the top 10 in the U.S., attracting some of the nation's finest sand artists. The backdrop is Fort Gratiot Light Station, Michigan's oldest, nearing its 200th birthday. Visitors can walk up its 94 steps for spectacular views of Lake Ontario and Lake Huron.

The *Risk Journal* is edited by Tamara Christie, Communications Manager, and published six times a year for members of Michigan Municipal Risk Management Authority. We welcome your feedback. To comment or suggest story ideas, please contact Tamara at 734 513-0300, 800 243-1324, or tchristie@mmrma.org.

by Tamara Christie, Communications Manager

ATTENDEES AT MMRMA'S upcoming 2023 Annual Meeting will gain valuable tools and information from our expert lineup of speakers and presenters. This year's theme is *MMRMA: Agents of Knowledge*, and the event planning team and staff have put together an informative and enjoyable program that will offer networking, training, and more.

Keynoter Arel Moodie



Arel Moodie

Television host and author Arel Moodie will help kick things off Thursday at the Opening Session with a talk showcasing his expertise in Adult Development Theory.

Research shows that human development is not limited to childhood—adults also continue to evolve through various stages. This can mean our values, strengths, fears, and perspectives can shift significantly throughout our lives. Moodie will share how to apply this knowledge to build connections and influence those around us.

Friday training sessions

On Friday, Moodie returns with tips on becoming a better public speaker and trainer. Next, Ben Schierbeek will present a session on empowerment, including a discussion of self-talk soundtracks and the distinction between reputation and character.

Ben Schierbeek

After lunch, leadership development expert Steve Ockerbloom will provide guidance on conflict management. We all encounter conflicts now and then, personally and in business.

Steve Ockerbloom

Ockerbloom applies a studied framework that describes five common conflict management styles, how to identify our own and others' most commonly used styles, and how to apply this knowledge to better resolve situations in our lives.

Speakers will provide insights on how to make connections with others, better resolve conflict, and become more organized.

Annual Board meeting

This is our annual opportunity to share highlights and performance results from the past year at MMRMA. In addition to staff and business partner presentations, returning guest speaker Randall Dean will provide his latest insights on the best ways to get organized at work, including apps, tips, and more.

All attendees are invited to attend the Annual Business meeting of the Board of Directors on Saturday morning, as well as the meeting of MMRMA's captive insurance company, Greenstone, on Thursday at 8:30 am.

We look forward to seeing attendees and sharing these informative and beneficial resources with our membership.