OeHI
Office of eHealth Innovation

Meeting Minutes

eHealth Commission

4/16/2025| 12pm| Virtual Meeting

Type of Meeting	Monthly eHealth Commission Meeting
Facilitator	Kaakpema (KP) Yelpaala
Commission Attendees	Toni Baruti, Mona Baset, Amy Bhikha, Sophia Gin, Patrick Gordon, Micah Jones, Krystal Morwood, Jackie Sievers, Kevin Stansbury, Parrish Steinbrecher, Misgana Tesfaye, Kaakpema (KP) Yelpaala Absent: Michael Feldmiller (prior notice), Alex Reed (prior notice), Ellen Sarcone (prior notice),

Minutes

Call to Order

KP Yelpaala

- Quorum Met: No
- Voting of Meeting Minutes: Meeting minutes for both March and April will be approved in May.

Announcements

Stephanie Pugliese, Director, Office of eHealth Innovation

Lieutenant Governor Dianne Primavera

- Lieutenant Governor Dianne Primavera kicked off the meeting by highlighting the opportunity to present with Stephanie Pugliese at the Business Research Intelligence Conference last month. The conference was focused on social determinants of health and health equity.
- Lieutenant Governor announced that she presented Colorado's bid to host the 2026 Annual National Lieutenant Governor's Association Meeting in Denver. Colorado won the bid and will be hosting this event in 2026.
- Lieutenant Governor Dianne Primavera also highlighted the launch of the 2025 Colorado Health IT Roadmap. This will be released later this month.
- Stephanie Pugliese provided an update regarding eHealth Commissioner bios on the OeHI website. She let commissioners know that they are able to send updates if they would like an updated bio and/or photo.
- Stephanie reiterated the excitement and anticipation of the 2025 Colorado Health IT Roadmap. Communications regarding this and more will be coming out this month.
- Stephanie noted that an implementation plan, which will complement the Roadmap, will be released later in the year. This will be a more detailed version of the roadmap to address some more specific needs around health IT that we heard in listening sessions and feedback in

refreshing the roadmap.

New Business

Current & Emerging Threats in the Health Sector and Staying Safe Online

Errol Weis, Chief Security Officer, Health Information Sharing and Analysis Center

- Presentation Slides: April 2025 eHealth Commission Slides

Detailed Summary: Errol Weis presented on cybersecurity. He explained the types of cybersecurity threats that we should be aware of, common examples, how to prevent cybersecurity attacks, and more.

- **4,670**
  - Errol kicked off the presentation explaining that every hour, 4,670 patient records are breached.
  - He expressed the great need to protect patient information.
- **What is ISAC?**
  - ISAC is short for "Information Sharing and Analysis Center". This concept developed in the mid 1990's when the US federal government recognized that much of critical infrastructure is owned and operated by the private sector.
  - ISACs empower sharing and collaboration in critical infrastructure communities to prevent, detect and respond to cybersecurity and physical security events.
  - ISACs collect, analyze, and disseminate actionable threat information to their members and provide them with tools to mitigate risks and enhance resiliency.
  - Health-ISAC was formed in 2021, and is a community of over 12,000 Global Security Analysts, built on trust and anonymity.
  - Members must be in the health sector and interested in providing value to the overall Health-ISAC eco-system by listening, sharing, and/or contributing.
  - Currently, Health-ISAC is in 140 countries globally.
- **The Cyber Threat System**
  - Errol explained that there are several different types of cyber threats such as
    - Hacktivism
    - Crime
    - Insider
    - Espionage
    - Terrorism
    - Warfare
  - He further explained that all threats are being targeted towards healthcare sectors.
  - Per Errol's presentation, Hacktivists use computer network exploitation to advance their

political or social causes.
    - Sometimes hacktivism can be done legally. Other times it is done illegally.
    - Errol provided modern-day examples of hacktivism such as:
        - Anonymous support for Occupy Wall Street (2011)
        - Panama Papers – 11 million financial and legal records exposed corruption and secretive offshore companies (2016)
        - Revealed offshore holdings of 140 politicians and public officials around the world
        - More than 214,000 offshore entities connected to people in more than 200 countries
        - Hacktivist collective Anonymous took actions to support Black Lives Matter (BlueLeaks 2020)
    - Hacktivism is affecting health care due to the following matters:
        - Gender reassignment surgery
        - Family planning and reproductive health / Abortions
        - COVID Vaccines
    - Hacktivism is not only affecting health care providers and the systems they use, but also healthcare insurers and payers. This can pose extreme threats beyond cybersecurity (exposure of protected health information (PHI), physical attacks, misinformation, etc.)
- **Cybercriminal Activity**
    - Errol explained that the motive for cybersecurity attacks are often money. These attacks are highly unfortunate, largely because cybersecurity criminals often lack consideration of the impacts these attacks can make.
    - Ransomware (holding data for ransome) is a common tactic.
    - Health-ISAC tracks ransomware cases across all sectors, and has tracked over 21,000 since 2021, with 2023 being the highest number of cases.
    - Ransomware impacts on hospitals alone include:
        - Ambulances forced to divert
        - Disrupted delivery of treatments
        - Canceled elective procedures
        - Delayed laboratory results
        - Delays in scheduling appointments
        - Downtime for Electronic Health Records management systems
        - Patient records unavailable
        - Leaked sensitive patient data
        - Surrounding area hospitals overwhelmed
    - Errol reported that last year, Health-ISAC saw cybercriminals directly targeting patients

via blackmail (many examples of this are provided in the presentation linked above).
    - He further explained that nation-state cybercriminal activity is a common occurrence because of the desire for strategic advancements in healthcare, biotechnology, and national security, as well as generating revenue for state and military objectives.
- **Common Cyber Threats**
    - Errol gave an overview of common cyber threats that many are falling victim to. These include invoices that look like they are being sent from reputable companies such as Norton and McAfee. It's important to note that the threat lies in the fact that these invoices are not actually coming from these companies, but instead, cybercriminals.
    - Errol explained that victims often call the number listed on the "invoice" to dispute the charge. From there, victims are directed to a cybercriminal, performing as an apologetic customer service agent, who ultimately retrieves bank information from the customer/victim.
    - Another threat that is commonly utilized by cybercriminals is multi-factor authentication fatigue-sending repeated messages to a victim, asking them to approve a login request. The repetition of these notifications eventually fatigue victims and cause them to accept/approve that request.
- **Artificial Intelligence (AI)**
    - Errol provided a warning as cybercriminals are beginning to utilize AI to carry out cyber attacks. This is largely done by imitation of another party via AI (ChatGPT, Google Gemini, and other forms of AI), and can be highly deceiving.
- **Staying Safe Online**
    - Errol provided some quick tips on how to stay safe online. These tips include:
        - Use strong passwords (diversify passwords and usernames)
        - Utilize a password manager system (a list of recommended systems was provided by Errol in the presentation slides)
        - Utilizing multi-factor authentication

Open Discussion

- Parrish Steinbrecher asked if there were any cases that Errol has seen where password managers are being hacked by cybercriminals.
    - Errol responded by explaining that there are some security issues that pop up from time-to-time with password managers. However, he has not yet heard of any instances of attacks happening with anyone who has had a reputable password manager. He explained that utilizing password managers is much safer than alternatives. He included that password managers typically have strict protections in place, making it more challenging for cybercriminals to access that data.

- Kaakpema (KP) Yelpaala asked about cyber insurance as many healthcare organizations are required to have cyber insurance and cybercriminals know this.
    - Errol explained that he is a fan of cyber insurance, especially in the health care sector. Furthermore, while there is a potential that cybercriminals may up ransom during ransomware attacks due to awareness of cyber insurance, ultimately, being cyber insured is something that is highly encouraged by Errol.
- KP also asked what the single most important thing is that groups can do to be more prepared for potential cyber attacks.
    - Errol encouraged listeners to review the ways to stay safe online (found in the presentation linked above) and implement those. His top 3 are to:
        - Stay up to date on patches (updating software as needed/prompted)
        - Utilize backup devices
        - Utilize Multi-factor authentication

Public Comment Period

- No new comments

Action Items

- *Next meeting:* May 14, 2025 (HYBRID meeting) at 1575 Sherman Street, Denver, Colorado 80203- 6th Floor Conference Room

Motion to Adjourn

Kaakpema (KP) Yelpaala

- Motion to adjourn this meeting was approved by Commissioner Kevin Stansbury
- Seconded by Commissioner Krystal Morwood