NAEMT Position Statement
EMS Agency Adoption of Cyber Readiness Plans

Statement:
NAEMT believes all EMS agencies should invest in creating a cyber readiness plan to protect its operations from a cyber-attack. The plan should focus on the "Cybersecurity Triad": keeping confidential data private, ensuring data is protected from unauthorized access or changes, and protecting and ensuring system availability. The plan must address three (3) functional areas: policy, compliance, and architecture incident response; operational security; and identity and access management. In addition, all EMS agencies should consider the purchase of cyber insurance. In order to properly execute the plan and protect communities from a cyber incident initiated directly or indirectly through an EMS agency, appropriate funding needs to be made available by federal, state, and local governments to build the necessary cyber secure infrastructures.

Background:
At this time, healthcare remains a prime target of financially-motivated and state-sponsored attacks with 157 breaches as of August 8, 2023. According to IBM's Cost of a Data Breach Report 2023, healthcare data breaches are the most expensive for thirteen (13) consecutive years, averaging $10.93 million.

The cultivation of cyber readiness within EMS stands as an absolute imperative. The necessity arises from the integration of technology into the EMS operational landscape and underpins the effectiveness of EMS and the integrity of collaborations across local, state, and federal levels. The reliance on technology, while undoubtedly enhancing EMS capabilities, concurrently exposes EMS to an unprecedented level of vulnerabilities that have the potential to disrupt the delivery of patient care and the transfer of critical medical data to hospital systems.

The interconnectedness of systems and data repositories, while fostering efficiency, simultaneously invites malicious actors to exploit vulnerabilities that can cripple operations, compromise sensitive patient information, and potentially disrupt the flow of care from the field to the hospital. EMS needs to bolster its collective defenses against cyber threats. By adopting robust cybersecurity measures, EMS not only safeguards patient data but also fortifies the infrastructure that supports the delivery of services. The secure exchange of information, both clinical and logistical, forms the backbone of effective healthcare delivery and patient outcomes.

References:

Careless, J. (2020). *Protecting EMS From Cyberthreats*. Hmpgloballearningnetwork.com. https://www.hmpgloballearningnetwork.com/site/emsworld/article/1223681/protecting-ems-cyberthreats

Dameff, C., Farah, J., Dotson, M., Killeen, J., & Chan, T. (2021, September 15). Cybersecurity. Annals of Emergency Medicine. Retrieved March 21, 2022, from https://www.annemergmed.com/article/S0196-0644(21)00856-8/fulltext

Friese, G. (2021, June 14). Cyberattackers are coming for Public Safety; prepare now. EMS1. Retrieved January 13, 2022, from https://www.ems1.com/cybersecurity/articles/cyberattackers-are-comingfor-public-safety-prepare-now-75YuF5gNYhEYqBME/

[NAEMT YouTube]. (2023, June 14). *What EMS Needs to Know About Cybersecurity Readiness and Response* [Video]. NAEMT. https://www.youtube.com/watch?v=dQjqhLtbrqA

Zavadsky, M. (n.d.). High-Performance EMS: Cybersecurity. https://www.hmpgloballearningnetwork.com/site/emsworld/article/217946/high-performance-ems-cybersecurity

Adopted: October 13, 2023