Draft Position Paper 2023-03

EMS Workforce Privacy Protection

Introduction

The Interstate Commission for EMS Personnel Practice recognizes the importance of balancing public access to EMS personnel licensure data while concurrently protecting the privacy and security of the workforce. Considering increasing threats of doxxing, especially targeting public health, healthcare, and government employees following the COVID-19 pandemic, and heightened concerns about terrorism threats (domestic and global), cybersecurity, and national security, there is a pressing need to ensure reasonable safeguards are in place to protect EMS personnel's personal information. This position paper aims to address these concerns by proposing guidelines for states to protect bulk access to EMS personnel data, ensuring primary source validation of EMS practitioners' licenses while safeguarding their individual privacy and security.

Background:

EMS personnel play a crucial role in public health and safety, and their license credentials must be verifiable. However, the exposure of personal information poses a significant risk to their safety, especially in the current environment of increased doxxing and security threats. Balancing the need for public and employer access to EMS personnel data with privacy and security concerns is essential.

Public Access to Licensing Systems:

The public should have access to perform queries of licensing systems to verify EMS practitioners' credentials. This access can be facilitated by providing options to validate an EMS practitioner's license status by using the practitioner's name, National EMS ID number, or state issued license number. The information displayed to the public should include:

1. Provider's name
2. License level
3. National EMS ID number
4. Expiration date of the license
5. License status (active, inactive, restricted, expired, etc.)

Protection of Personal Identifiable Information (PII):

To safeguard EMS personnel's Personal Identifying Information (PII), privacy and security, certain information should be restricted. Restricted information should include: residential addresses, phone numbers, email addresses, and other PII. The exposure of this information is not necessary to validate a license and poses a direct risk to the safety and well-being of EMS responders, especially in cases of doxxing or harassment.

Bulk Release of Records:

The bulk release of EMS personnel records, including the release of all EMS practitioners licensed in a particular state or region, should be restricted and limited to cases where it is absolutely necessary for the public's health, safety and welfare. When such releases are determined to be justified, minimum data sets necessary to fulfill the justified purpose are encouraged. For example, a minimum data set may include:

1. EMS Practitioner's First Initial and Last Name
2. License level
3. License status
4. Expiration date of the license

This minimal data set is sufficient for most verification and reporting needs, while minimizing the risk associated with the exposure of additional personal information.

National Security Implications:

Exposing full datasets that include home addresses of EMS personnel and other PII presents a significant security risk. In an era of increasing cyber threats and the potential for hostile actors to exploit large datasets, the protection of this sensitive information is paramount. Ensuring that EMS personnel's personal data is secure is not only in the interest of individual responders but also critical for national security.

Conclusion:

The Interstate Commission for EMS Personnel Practice urges all states (Compact and Non-Compact) to take immediate action by reevaluating and strengthening their data security policies. This initiative is crucial to ensure the comprehensive protection of Personal Identifiable Information (PII) and sensitive data related to EMS Practitioners. Striking a balance between public and employer access to EMS personnel data is paramount, especially in light of the growing threats of doxxing and the escalating concerns surrounding cyber and national security.

States must act swiftly to implement these measures. By doing so, they not only uphold the integrity of EMS personnel licensing systems but also safeguard the privacy and security of those who tirelessly serve on the frontlines of public health and safety. Join us in this vital mission to secure the data of EMS personnel and fortify our nation's defenses.