Data Management and Information Security

Purpose

Computer databases provide an excellent format with which to manage emergency responders' information. In order to maintain privacy required by law and to facilitate efficient communication between agencies, issues of information security and interoperability must be addressed in the pre-deployment phase to ensure accurate management of responders during deployment and enable reliable, comprehensive monitoring and surveillance post-deployment.

How to Develop a Pre-deployment Information System Security Plan for Field Settings

1. Form information security structure.
2. Assess security needs.
3. Identify laws, regulations, and statutes applicable to agency and information.
4. Outline steps and responsibilities based assessment and regulations.
5. Implement security procedures.
6. Manage risk through incremental changes.

Components of Information Security

There are 12 components of implementing an information management system in the field:

Risk Management	Risk assessment (identify potential threats and their impact) and risk mitigation (prioritize and implement risk controls).
Security Policy	Security systems in place; responsibilities for security systems; address compliance issues.
Organization of Information Security	Structure for the governance of the security program.
Asset Management	Inventory and classify information assets, agree upon its ownership, and protect against its loss to damage and theft.
Human Resources Security	Confidentiality and availability of data through changes in personnel and position responsibilities.
Physical and Environmental Security	Safeguards that consider the physical structures that house and support the information systems.
Communications and Operations Management	Processes to maintaining appropriate level of security, purchase and maintain physical assets, and resolve any issues that arise.
Access Control	Only authorized personnel can access systems.
Information Systems Acquisition, Development, and Maintenance	Secure processes for the entire lifecycle of the information system.
Information Security Incident Management	Steps to identify, respond to, and manage any information security incident.
Continuity Management	System functioning recovery should an incident occur.
Compliance	Compliance with security policies and authority to enforce policies.

Personally Identifiable Information (PII)

Any information that can be used to distinguish or trace a specific individual and any other information that can be directly linked to that individual including name, address, telephone number, social security number, and health records.

Forms with fields for name, address, telephone number, and social security number, and personal health history contain PII

How to Protect PII

- Minimize the collection, use, and retention of PII.
- De-identify the information.
- Generalize the information (group by common values), suppress the information (delete PII), or replace the information with averages.

Interoperable IT Systems: Important Action Items

There will often be a need to communicate and share data across IT systems:

- Agencies need to establish common policies and procedures.
- IT specialists should communicate the differences in format, hardware, and software pre-deployment and ensure mutual levels of security standards.
- Ownership of assets where management will overlap should be discussed.
- Documenting these features can allow the IT specialists to prepare their systems for interoperability during and post-deployment to facilitate a faster response.

Emergency Responder Health Monitoring and Surveillance

The Emergency Responder Health Monitoring and Surveillance (ERHMS) system is a health monitoring and surveillance framework that includes recommendations and tools specific to protect emergency responders during the pre-deployment, deployment, and post-deployment phases of a disaster. The intent of ERHMS is to identify exposures and/or signs and symptoms early in the course of an emergency response in order to prevent or mitigate adverse physical and psychological outcomes and ensure workers maintain their ability to respond effectively and are not harmed in the course of this response work. Data will also help to identify during the post-deployment phase which responders would benefit from medical referral and possible enrollment in a long-term health surveillance program. Please refer to Chapter 4 and section 4T for more information on Data Management and Information Security.

National Institute for Occupational Safety and Health (NIOSH) ERHMS Contact:

- CDR Renée Funk, Coordinator, ERHMS at rfunk@cdc.gov or 404-498-1376

For more information on ERHMS, please visit:
erhms.nrt.org & www.cdc.gov/niosh/topics/erhms