Suspicious Activity Reporting (SAR) for Public Health and Health Care Partners

The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) has developed SAR awareness training for key non-law enforcement constituencies, or "hometown security partners," who are important to the SAR effort. The everyday duties and responsibilities of public health and health care professionals place them in a unique position to observe suspicious activity that, when viewed within the totality of circumstances, may indicate preoperational planning of a terrorist-related incident.

This awareness training is designed to **assist public health and health care professionals in understanding their critical role as homeland security partners**; recognizing what kinds of suspicious behaviors are associated with pre-incident terrorism activities; understanding how and where to report suspicious activity; protecting privacy, civil rights, and civil liberties; and ensuring compliance with applicable patient confidentiality laws.

The integration of public health and health care professionals into the SAR process and the information sharing activities of state and local fusion centers will benefit the collective homeland security effort by enhancing the preparedness of public health and health care organizations across the country, while supporting the prevention, protection, response, and recovery efforts of all homeland security partners.

Access the SAR Training for Public Health and Health Care Partners video at:

http://nsi.ncirc.gov/training_online.aspx

Additional Resources

Nationwide SAR Initiative (NSI) Resources

http://nsi.ncirc.gov/resources.aspx

Provides additional resources and information about the NSI, including fact sheets, policy and privacy documents, technology information, and training resources.

U.S. Department of Health and Human Services Office for Civil Rights

http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/emergency/index.html

Provides guidance for sharing patient information under the HIPAA Privacy Rule, including in emergency situations, such as assisting in disaster relief, public health, and law enforcement efforts.

Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule: A Guide for Law Enforcement

http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/emergency/final_hipaa_guide_law_enforcement.pdf

Explains under what circumstances a HIPAA-covered entity may disclose protected health information to law enforcement.

Issued 06/15

Suspicious Activity Reporting
Indicators and Behaviors

Behaviors	Descriptions
Potential Criminal or Non-Criminal Activities Requiring Additional Information During the Investigation	
Eliciting Information	Questioning individuals or otherwise soliciting information at a level beyond mere curiosity about a public or private event or particular facets of a facility's or building's purpose, operations, security procedures, etc., in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.
Testing or Probing of Security	Deliberate interactions with, or challenges to, installations, personnel, or systems that reveal physical, personnel, or cybersecurity capabilities in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.
Recruiting/Financing	Providing direct financial support to operations teams and contacts or building operations teams and contacts; compiling personnel data, banking data, or travel data in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.
Photography	Taking pictures or video of persons, facilities, buildings, or infrastructure in an unusual or surreptitious manner that would arouse suspicion of terrorism or other criminality in a reasonable person. Examples include taking pictures or video of infrequently used access points, the superstructure of a bridge, personnel performing security functions (e.g., patrols, badge/vehicle checking), security-related equipment (e.g., perimeter fencing, security cameras), etc.
Observation/ Surveillance	Demonstrating unusual or prolonged interest in facilities, buildings, or infrastructure beyond mere casual (e.g., tourists) or professional (e.g., engineers) interest and in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person. Examples include observation through binoculars, taking notes, attempting to mark off or measure distances, etc.
Materials Acquisition/ Storage	Acquisition and/or storage of unusual quantities of materials such as cell phones, pagers, radio control toy servos or controllers; fuel, chemicals, or toxic materials; and timers or other triggering devices, in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.
Acquisition of Expertise	Attempts to obtain or conduct training or otherwise obtain knowledge or skills in security concepts, military weapons or tactics, or other unusual capabilities in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.
Weapons Collection/ Discovery	Collection or discovery of unusual amounts or types of weapons, including explosives, chemicals, and other destructive materials, or evidence, detonations or other residue, wounds, or chemical burns, that would arouse suspicion of terrorism or other criminality in a reasonable person.
Sector-Specific Incident	Actions associated with a characteristic of unique concern to specific sectors (e.g., the public health sector), with regard to their personnel, facilities, systems, or functions in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.
Defined Criminal Activity and Potential Terrorism Nexus Activity	
Breach/Attempted Intrusion	Unauthorized personnel attempting to enter or actually entering a restricted area, secured protected site, or nonpublic area. Impersonation of authorized personnel (e.g., police/security officers, janitor, or other personnel).
Misrepresentation	Presenting false information or misusing insignia, documents, and/or identification to misrepresent one's affiliation as a means of concealing possible illegal activity.
Theft/Loss/Diversion	Stealing or diverting something associated with a facility/infrastructure or secured protected site (e.g., badges, uniforms, identification, emergency vehicles, technology, or documents {classified or unclassified}), which are proprietary to the facility/infrastructure or secured protected site.
Sabotage/Tampering/ Vandalism	Damaging, manipulating, defacing, or destroying part of a facility/infrastructure or secured protected site.
Cyberattack	Compromising or attempting to compromise or disrupt an organization's information technology infrastructure.
Expressed or Implied Threat	Communicating a spoken or written threat to commit a crime that will result in death or bodily injury to another person or persons or to damage or compromise a facility/infrastructure or secured protected site.
Aviation Activity	Learning to operate, or operating an aircraft, or interfering with the operation of an aircraft in a manner that poses a threat of harm to people or property and that would arouse suspicion of terrorism or other criminality in a reasonable person. Such activity may or may not be a violation of Federal Aviation Regulations.