



California
Department of
Health Services

SANDRA SHEWRY
Director

State of California—Health and Human Services Agency
Department of Health Services



ARNOLD SCHWARZENEGGER
Governor

June 9, 2005

AFL 05-25

TO: GENERAL ACUTE CARE HOSPITALS

SUBJECT: SUGGESTED PROTECTIVE MEASURES

The Department of Health Services, Licensing and Certification is sending this important information to hospitals in light of the recent news coverage about hospitals as possible targets for terrorism. We have confirmed that there is no indication of any planned targeting of hospitals; however, given the heightened awareness that the press reports have produced, this is a good opportunity to restate some reasonable protective measures for hospitals to consider and against which to evaluate their current protective measures posture.

Access Control:

- Advise appropriate staff, both medical and non-medical, of the potential for unauthorized personnel to present apparently legitimate credentials and/or to wear recognizable uniforms to gain access to a facility. Ensure they understand the potential threat to a medical facility that houses people, pharmaceuticals, and chemicals as well as equipment, and provide instructions on how to deal with suspicious events. Encourage employees to confront all suspicious individuals or individuals without proper identification, particularly in sensitive areas, such as:

Laboratories

Pharmacies

Physical plant

Shipping and receiving areas

Note: Some hospitals have emergency and intensive and critical care facilities co-located. Two points to consider: These are vulnerable to compromise (i.e., meaning co-location allows all to be simultaneously compromised).

AFL 05-25

Page2

June 9, 2005

- Maintain control over all entry points, and monitor all exit points. Using closed circuit TV (CCTV), record all movements in both areas. Ensure there is adequate lighting to support CCTV and that nothing obstructs CCTV field of view (e.g., overgrown vegetation). If possible, maintain card access to all areas beyond the main entrance.
- Enforce stringent credentialing and badging of all hospital employees. Implement credentialing and badging of contractors, official visitors, inspectors, and others with hospital business.
- Inspect parcels and packages brought into the facility. Conduct random inspections of parcels and packages brought in by visitors.
- Ensure all areas that are closed to the public (e.g., pharmaceutical storage areas, laboratories, Heating Ventilation and Air Conditioning (HVAC) and utility equipment areas, cleaning supply closets) are locked. Inspect locks and other security hardware on doors, windows, and other facilities.

Inspection:

- Increase inspection and inventorying of sensitive materials and equipment (e.g., pharmaceuticals, radiological material). Remove unnecessary sensitive material and equipment. Require rigorous accounting for all sensitive materials and equipment movement.
- At regular intervals during each day, inspect the interior and exterior of buildings, storage areas, waste bins, closets, and other areas for suspicious packages. Report any unusual items to the security office.
- At irregular intervals during each day, inspect HVAC intakes and electric, gas, water, and telecommunications feeds into the facility for signs of tampering.

Communications:

- Test the operation of internal communication systems (e.g., from medical personnel to the security office) and external communication facilities (e.g., to local law enforcement)
- Test alarm systems for proper operation

Security Force

- Ensure the security guard force is fully briefed and trained in handling suspicious persons and/or packages.

AFL 05-25
Page 2
June 9, 2005

- Review points of contact with local law enforcement and the Joint Terrorism Task Force. Establish periodic communication to update the threat situation.
- Contact local police at first contact with any suspicious activity and, if possible, record and document the following information.
 1. A full description of the individual(s), to include clothing worn.
 2. The license plate, including state, make, and model of any vehicle.
- If not in place, add CCTV to all access points, parking areas, the exterior of all access points, and driveways leading to access points.

Cyber Security:

- Review cyber security procedures to prohibit unauthorized access to data and information. Restrict access to computer systems to necessary personnel.
- Review the facility web page and eliminate information that might be sensitive.

Security Plan:

- Review the security plan and procedures for dealing with this type of threat and update plans as necessary.

If you have any questions regarding this information, please contact Jocelyn Montgomery, Disaster Preparedness Coordinator for Department of Health Services, Licensing and Certification at jmontgo2@dhs.ca.gov.

Sincerely,

Original Signed by Brenda G. Klutz

Brenda G. Klutz
Deputy Director

cc: See Next Page
AFL 05-25
Page 4
June 9, 2005

cc: California Hospital Association
2201 K Street
Sacramento, CA 95816-4922

California Emergency Services Authority
1930 Ninth Street
Sacramento, CA 95814

.