



Healthcare

CAREFULLY SPEAKING®

A Risk Management Resource for Aging Services | 2025 Issue 1

Workplace Security: Common Measures to Safeguard Residential Environments

Workplace security rests upon a foundation of physical safeguards and procedural controls designed to minimize risk and enhance organizational response to violent or abusive incidents. This edition of *CareFully Speaking*® offers recommendations that are intended to help aging services organizations evaluate and upgrade their degree of security preparedness.

Policy statement

A zero-tolerance organizational policy regarding violence is the first line of defense in safeguarding staff and residents from threats and abuse. Written policy should prohibit specified behaviors – e.g., physical, verbal and psychological forms of aggression and harassment – and state expressly that all forms of violence are unacceptable. (See “[Addressing the Challenge: Workplace Violence in LTC Setting](#),” issued by the American Health Care Association and the National Center for Assisted Living, March 20, 2024.)

In this issue...

- Security Concerns Related to Terminated Employees... [page 2](#).
- Environmental Safeguards for a More Secure Workplace... [page 4](#).
- Quick Links... [page 5](#).

Security needs assessment

All aging services settings must find the right balance between security, resident autonomy and operational flexibility. Different facilities require different types of controls, based on such factors as size, resident population, location and staffing numbers. As needs evolve over time, security measures must be regularly reviewed by leadership. (The sidebar “Environmental Safeguards for a More Secure Workplace,” on [page 4](#), lists some of the basic security concerns that are typically faced by aging services organizations.)

A **zero-tolerance** organizational **policy regarding violence** is the first line of defense in **safeguarding staff and residents** from threats and abuse.

Violence prevention training

Such training should be provided upon hire and at least annually thereafter for all administrators and staff, as well as volunteers and temporary employees. Training should be scenario-based, with an emphasis on intervening effectively in conflict situations without undue use of force. Training sessions should include general threat management techniques, such as the following, which may help to defuse a volatile situation:

- **Establish rapport** by addressing the individual in a calm and respectful manner.
- **Use a neutral tone of voice**, keeping volume down.
- **Be aware of body language**, avoiding sudden movements and maintaining a relaxed posture.
- **Keep a proper distance** while gently steering the individual toward a quiet, non-public space.
- **Have an escape route in mind** should the situation get out of control.
- **Be firm and direct in manner**, but not angry or irritated.
- **Acknowledge the individual's feelings**, and listen carefully and sympathetically.
- **Summon a supervisor or administrator** if a situation rapidly escalates.

Security Concerns Related to Terminated Employees

A hostile termination can potentially jeopardize workplace security. In addition to consulting legal counsel prior to terminating an employee who may be hostile or violent, ask security personnel and/or law enforcement agencies whether a [behavioral threat assessment](#) is warranted. (For a checklist of criteria to consider and actions to take when terminating volatile employees, click [here](#).)

The following post-termination actions, among others, may help to minimize threats to a facility's integrity and safety:

- **Promptly disable the terminated employee's email account**, computer access, phone extension and voicemail.
- **Remove the employee from email group distribution lists**, internal office phone lists, and website and building directories.
- **Request the employee's ID badge and keys** (if applicable) and disable IT security codes and building access cards.
- **Collect company-issued cell phones**, laptops and other mobile devices.

Response measures

Aging services organizations that fail to address threatening or abusive behaviors when they first appear create significant liability exposure should the behaviors recur. In particular, they expose themselves to potential claims of vicarious liability for condoning a hostile or dangerous work environment. The following measures can help strengthen an organization's ability to respond to real or potential violence:

- **Review the facility's emergency action plan** and ensure that it covers such critical areas as responding to firearm, bomb and hostage threats; handling both family and media inquiries; and debriefing staff members afterward.
- **Develop emergency communication procedures**, involving utilization of alarms, public address systems, staff cell phones, designated websites and other media.
- **Consider forming a threat management team** to respond to potentially violent situations.
- **Establish a dedicated hotline** for reporting incidents.
- **Explain to staff members how and when they should call for assistance** during dangerous situations.
- **Include scenarios of threats and/or escalating behaviors** – such as active shooter situations or the detection of intruders – in annual emergency preparedness drills.
- **Promptly contact police when there is an imminent risk of violence**, e.g., verbal threats, physical aggression, the presence of weapons, or any other behavior that places residents or staff in danger.
- **Institute a formal post-incident response protocol**, including prompt and thorough investigation, documentation and reporting of events to law enforcement and regulatory agencies, as required by law.
- **Collect data on reported threats and violence** via established performance improvement channels, and perform root cause analysis to determine key factors contributing to the incidents.

Facility access controls

Every aging services setting should have video surveillance and access controls at points of ingress and egress. The following additional security measures, among others, can help prevent unauthorized entry:

- **Staff ID badges**, which are programmed to permit varying levels of access, as assigned.
- **Centralized access control units**, which monitor staff movement via badges, and which allow for regular security audits of entries and exits.
- **A visitor management system**, which may range from basic visitor registration and sign-out procedures to assigning escorts to visitors, if necessary, for safety and privacy reasons.
- **Designated access zones**, such as memory care and psychiatric units, which have their own access requirements for staff and visitors.
- **Pedestrian pathways**, which guide visitors and other third parties within the facility.

Security personnel

At moments of crisis, swift and decisive action by well-trained security staff can mean the difference between life and death. At the same time, security personnel who lack basic competence can do more harm than good. For this reason, organizations that utilize security staff should have the following risk control strategies in place, among others:

- **Delineate in writing security staff duties and responsibilities**, including, but not limited to, managing visitor check-in, monitoring access to sensitive areas, ensuring adherence to safety protocols, and responding to both natural and man-made emergencies.
- **Train all hires in the basics of emergency response**, including conflict resolution, active shooter protocols and first aid. Document training sessions in personnel files.
- **Complete a security needs assessment** focusing on, among other factors, past and emerging threats, resident vulnerabilities, local crime statistics, and any laws or regulations relating to armed security, if applicable.

- **Consult with local law enforcement agencies** to confirm that policies governing use of both firearms and non-lethal weaponry (e.g., pepper spray, stun guns, tasers, batons) are legally compliant.
- **Ensure that security personnel are covered by insurance**, checking for possible exclusions relating to firearms.
- **Carefully document weaponry qualifications**, including training, licensure and certification for all security staff authorized to carry a firearm. If security personnel are contracted rather than employed directly, verify that the staffing agency keeps thorough records.

When security personnel deploy a weapon, it is essential to scrupulously document the circumstances, including the nature of the threat, the rationale for deployment and the outcome of the confrontation. It is also necessary to record basic information about the threatening individual, including name, age, demographics, and physical and mental condition. Reports should be forwarded to the appropriate authorities, as well as to the internal oversight committee for resident/staff/visitor safety.

Sound workplace security measures can help facilities minimize the likelihood and severity of violent or abusive incidents, thus enhancing overall safety while reducing potential liability. The strategies presented in this publication can serve as a starting point for discussions about workplace security and the need to safeguard aging services environments.

At moments of crisis, **swift and decisive action** by well-trained **security staff** can mean the difference between **life and death**.

Environmental Safeguards for a More Secure Workplace



Secure Entry and Exit Points

- **Place barriers at the facility's perimeter**, such as walls, parking gates and security checkpoints.
 - **Implement controlled access systems** – such as automatic locks, key cards, entry codes or biometric scanners – at points of ingress/egress.
 - **Limit the number of unsecured ingress points after hours**, using programmed locking schedules.
 - **Mount motion sensors at restricted access or hazardous areas**, such as rooms containing combustible items or gas-fired water heaters, in order to monitor unauthorized entry.
 - **Install effective locking devices** at stairwell doors and loading dock garages.
 - **Implement two-factor authentication** in areas requiring heightened security, such as the pharmacy, secured residential units and staff lounges.
 - **Enclose residential courtyards or gardens**, and limit unsecured access points.
 - **Assess the effectiveness of security barriers** on a regular basis and preserve maintenance records.
 - **Promptly investigate any security breach** or unauthorized access attempt, in accordance with formal response protocols, and document all actions taken.
-



Video Surveillance

- **Place surveillance cameras at entry points** and around the perimeter, as well as in hallways and common areas.
 - **Notify residents, staff and visitors of the presence of video cameras** by posting conspicuous notices throughout the facility.
 - **Ensure that the closed camera network operates independently** of the facility's main IT system.
 - **Obtain written approval from residents** before monitoring private residential spaces, if state law permits.
 - **Retain security camera footage for a set period**. While a week is typical, some cloud-based systems allow images to be stored for several months.
 - **Draft a separate policy for preserving video footage relating to security incidents** and protecting it against erasing or tampering for an indefinite period.
-



Lighting

- **Illuminate interior spaces clearly and evenly**, as well as exterior areas, such as sidewalks, driveways, walkways and parking lots.
 - **Ensure that stairways are well-lighted** and included in video surveillance activities.
 - **Consider installing motion-triggered low-level lighting** at facility gates and doorways.
-

Implement controlled access systems – such as automatic locks, key cards, entry codes or biometric scanners – at points of ingress/egress.



Duress Alarms

- **Integrate duress alarms into employee badges and mobile phones**, and also install them at appropriate locations within the facility.
- **Route all alerts to security personnel** or other designated crisis responders.
- **Provide personal alarms to all staff who work with violence-prone residents**, and train them in proper use.
- **Connect alarms to the video surveillance system** and nurse call network.
- **Test communication protocols regularly** to ensure that activated alarms trigger an appropriate response.



Signage

- **Announce the organization's zero-tolerance policy toward violence**, using posters placed near entrances and in common areas.
- **Prominently display the facility's no-weapons policy**, in accordance with state regulations.
- **Post "Authorized Personnel Only" signage** in restricted or hazardous areas.
- **Indicate parking rules and hours** in designated parking areas.
- **Put up signs asking visitors to report suspicious activity** – such as trespassing, loitering, and odd or aggressive behavior – to security.

Quick Links to CNA Resources

- *AlertBulletin*® 2024-Issue 4, "[Serious Adverse Events: Creating a Sound Crisis Response Plan.](#)"
- *AlertBulletin*® 2022-Issue 2, "[Crisis Decision-making: Early Planning Helps Promote Better Outcomes.](#)"
- *AlertBulletin*® 2022-Issue 1, "[Adverse Event Review: Enhancing Analysis, Safeguarding Data.](#)"
- *AlertBulletin*® Republished 2020, "[Active Shooter Response: Precautionary Measures Can Save Lives.](#)"
- *CareFully Speaking*® 2024-Issue 2, "[Residents with Serious Mental Illness: Addressing Common Risks.](#)"
- *CareFully Speaking*® 2021-Issue 2, "[Resident-on-resident Sexual Abuse: Taking Aim at a Growing Risk.](#)"
- *CNA Special Resource* 2022, "[Emergency Planning: A Risk Management Guide for Healthcare Facilities and Providers.](#)"

Editorial Board Members

Kelly J. Taylor, RN, JD, *Chair*
 Janna Bennett, CPHRM
 Elisa Brown, FCAS
 Emma Landry
 Michelle O'Neill, MN, MBA, PhD,
 CPHRM, CPPS
 Mary Porter
 Katie L. Templeton, JD, CPCU
 Blaine Thomas
 Natalie Wynegar, MBA, LNHA

Publisher

Mitchell Neal RN, MBA, CPHRM

Editor

Hugh Iglarsh, MA

Did someone forward this newsletter to you? If you would like to receive future issues of *CareFully Speaking*® by email, please register for a complimentary subscription at go.cna.com/HCSubscribe.

For more information, please visit www.cna.com/healthcare.

The information, examples and suggestions presented in this material have been developed from sources believed to be reliable, but they should not be construed as legal or other professional advice. CNA accepts no responsibility for the accuracy or completeness of this material and recommends the consultation with competent legal counsel and/or other professional advisors before applying this material in any particular factual situation. Please note that Internet links cited herein are active as of the date of publication, but may be subject to change or discontinuation and are provided solely for convenience. CNA does not make any representations, endorsements, or assurances about content contained on any website referred to herein or on the accuracy of any of the content contained on third party websites. The views, statements, and materials contained on the website are those of the owner of the site. This material is for illustrative purposes and is not intended to constitute a contract. Please remember that only the relevant insurance policy can provide the actual terms, coverages, amounts, conditions and exclusions for an insured. All products and services may not be available in all states and may be subject to change without notice. Certain CNA Financial Corporation subsidiaries use the "CNA" service mark in connection with insurance underwriting and claims activities. Copyright © 2025 CNA. All rights reserved. Published 4/25. CNA CS25-1.

