

Risk Reporter

Fall/Winter
2015

Vol. 16
issue 3

Special Edition
for Senior Living Communities

A quarterly publication by Church Mutual Insurance Company

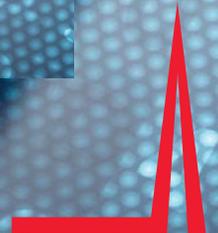
Be aware

October is National Cyber Security
Awareness Month

Protect your records from the rise
in cyber theft

Make active assailant emergency
planning a top priority

Take action to prevent elderly abuse



Be prepared

Active assailant emergency planning for assisted living facilities

“Active shooter is a term used by law enforcement to describe a situation in which a shooting is in progress, and both law enforcement personnel and citizens have the potential to affect the outcome of the event.”

— FBI 2014 Report

While the risk of a violent attack at your long-term care or assisted living facility might seem remote, it is not an impossibility. The FBI advises healthcare facilities to incorporate active assailant preparedness into their emergency plans, and entities as diverse as the Stanford Geriatric Education Center and the American Assisted Living Nurses Association have hosted educational webinars and seminars on the topic. Many state health agencies are also urging long-term care and assisted living facilities to prepare for the grave eventuality of an armed attack.



There are specific actions your organization can take now to enhance security while continuing its larger mission of service to individuals, families and the greater community.

First, ensure emergency readiness

Put the right people and systems in place

Security and insurance professionals can work with you to assess key systems — lighting, backup power, alarms, fire suppression, security cameras, fencing and gates, doors, locking systems, etc. — as well as emergency policies and procedures. They can also work with you to ensure that employees and volunteers are properly screened before being hired.

Consider adding armed security

It's best to contact local law enforcement and seek out legal counsel before hiring armed security. In general, current or former law enforcement officers offer better training, skills and experience than private security company employees — but background checks should be used to screen and select specific individuals.

Then, focus on active assailant situations

Plan in advance

- Plans should incorporate facility lockdown and evacuation procedures, shelter-in-place locations, methods of communication during an incident and when buildings and grounds are safe.
- Address access and communications for the disabled or other special populations.
- Share your organization's plans with law enforcement and first responders prior to an emergency.

Train people to respond appropriately

There are three basic responses to an attack: RUN, HIDE or FIGHT. People can run away from the attacker, find a secure place to hide where the attacker cannot reach them, or overcome and incapacitate the attacker in order to survive and protect others from harm. As an event continues, those under attack could use more than one option.

It's natural for people under attack to be startled and to hesitate out of disbelief or denial. Use drills and training to teach people to respond immediately to an attack. The faster people respond, the faster they can get to safety.

Special considerations

In an active assailant incident, health care staff might run toward a disturbance, rather than away from it, and might not easily leave vulnerable patients and residents. Educational sessions produced by Stanford Geriatric Education Center and other resources frequently highlight the need for health care workers to learn to save themselves first in order to save others.

Prepare for post-event management and intervention

Once a scene is secured, first responders will work with your staff members to transport the injured, interview witnesses and initiate an investigation. Your organization should have an emergency response team in place to help law enforcement, rescue workers, victims, family members and staff members. Post-event planning should also address communications with the media and the public.

Make sure you're covered

Your Church Mutual insurance agent can help you plan for the worst while hoping for the best. If you have questions about liability or coverage related to active shootings or other emergencies, contact your agent directly. For assistance with safety planning, contact our Risk Control Consulting and Research Center at (800) 554-2642, ext. 5213, or riskconsulting@churchmutual.com.

For help screening job applicants and volunteers, we recommend our corporate partner Trusted Employees. Contact the company at trustedemployees.com or (877) 389-4024.

BEHAVIOR WARNING SIGNS

Per the FBI, these behavioral indicators might signal that a person is at risk of acting violently.

- Development of a personal grievance
- Escalation in target practice and weapons training
- Recent acquisitions of multiple weapons
- A significant personal loss including death, breakup, divorce or job loss
- Fascination with previous shootings or mass attacks



Be aware

Assisted living or other residential care facilities should be aware that there has been a significant rise in cyber theft of medical records.

As your organization becomes more dependent on the Internet as a primary channel for doing business, storing resident and employee information and conducting both personal and business interaction, your risks of becoming a primary target for a cyber attack increase.



MEDICAL
RECORDS

Medical records, which often contain Social Security numbers, insurance IDs, addresses and medical details, sell for as much as 20 times the price of a stolen credit card number.

For the past three years, the health/medical sector has accounted for the highest percent of total hackings of any industry, according to the Identity Theft Resource Center.

“We now live in a world that is more connected than ever before. The Internet touches almost all aspects of everyone’s daily life, whether we realize it or not. Recognizing the importance of cyber security to our nation, October has been designated as *National Cyber Security Awareness Month*.”

— U.S. Department of Homeland Security

Understanding the real costs of a cyber attack

It is almost impossible to predict the probability of a cyber attack and the costs associated with the loss and mitigation of it, but understanding the overall real cost of an attack can help inform your security strategies, investment decisions and insurance protection.

Direct costs resulting from cyber crime

In considering the consequences of cyber crime, you must take into account direct losses to individuals as well as your organization. The costs of responding to cyber crime include compensation, regulatory fines, costs associated with legal or forensic issues, and possible payments to victims of information/identity theft.

Indirect costs associated with cyber crime

Indirect costs include such factors as reputational damage to your facilities, loss of confidence in your ability to conduct cyber transactions and reduced revenues because of decreases in residency.

The costs of preventing cyber crime

There are very real costs associated with cyber security, which could require implementation of protection and detection methods, heightened physical and technological security, cyber crime insurance, changes to ensure compliance with regulatory and/or industry standards and employee training. These costs, however, are both foreseeable and far more controllable than the costs of suffering a cyber attack.

Special considerations

Part of your responsibilities in providing care, supervision and assistance to your residents is the coordination of services with health care providers. This often requires maintaining records of medication, medical information and personal data. Cyber criminals are actively trying to gain access to this valuable information by finding weaknesses in the network systems of health care providers and their partners.

Protecting your organization against cyber attacks requires continued investment in technology, education and training of employees and contractors. You will need to maintain an ongoing focus on data management policies and processes to stay ahead of cyber criminals — and protect both your residents’ information and your company’s reputation.

We’re here for you

Our cyber crime liability insurance and protection services focus on your protection and include prevention education, coverage for both electronic and paper data loss or theft, identity theft and post-loss data recovery.

For assistance, contact your agent directly, visit churchmutual.com or contact our Risk Control Consulting and Research Center at (800) 554-2642, ext. 5213, or riskconsulting@churchmutual.com.

For help screening job applicants and volunteers in order to reduce the possibility of internal threats, we recommend our corporate partner Trusted Employees. Contact the company at trustedemployees.com or (877) 389-4024.

Follow industry best practices – create a culture of security

- Monitor applications with access to data
- Establish role-based access controls
- Collect detailed logs and report data
- Use only strong passwords and change default passwords
- Maintain security patches and updates
- Utilize user activity monitoring
- Develop and enforce policies on mobile devices and remote access
- Implement an employee cyber security training program
- Enhance background screening of all staff and volunteers
- Implement measures for detecting compromises
- Develop a cyber security incident response plan



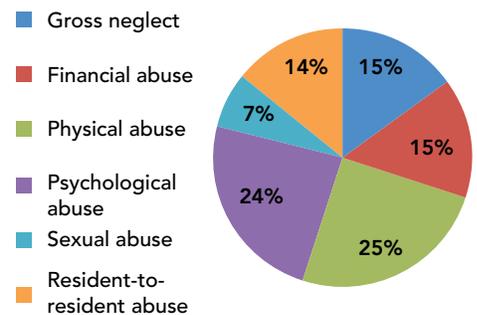


Be alert

Preventing elder abuse in assisted living facilities

Across the U.S., more than 900,000 people reside in assisted living facilities and another 3.2 million in nursing homes. While organizations that operate care facilities are typically committed to providing safe accommodations and excellent medical care, elder abuse — which includes financial, physical, psychological, or sexual abuse, as well as gross neglect — does occur.

Types of Abuse – Assisted Living Facilities



Source: Research Brief: Abuse of Residents of Long Term Care Facilities, 2011, National Center on Elder Abuse (NCEA)

Failure to act hurts organizations that operate care facilities

While elder abuse might be an uncomfortable topic, it is important for management to tackle this problem head-on. An abuse scandal connected to an assisted living center or other residential care facility can have devastating effects:

- Damaged reputation
- Loss of public trust
- Loss of government and/or private funding
- Unexpected legal expenses and/or fines
- Criminal charges and/or civil lawsuits

Taking steps to prevent elder sexual abuse can help protect your organization as well as the residents in your care.

Preventive measures can protect you

Management and employees might hesitate to discuss elder abuse in the mistaken belief that the prevention will be difficult or costly, or from a concern that raising the issue will lead the public to believe a problem already exists, or because of unspoken fears that abuse will be discovered.

A prevention plan offers distinct benefits:

- Clear, well-defined elder-protection policies might reduce liability.
- Uncovering problems sooner rather than later might limit negative impacts.
- Identifying underlying causes of abuse can lead to additional improvements in care.

Preventive measures can support an organization's efforts to ensure the safety and health of all residents.



WARNING SIGNS OF ABUSE

Gross neglect

- Unusual weight loss, malnutrition, dehydration
- Untreated bed sores, poor hygiene, being left dirty

Physical abuse

- Unexplained bruises, welts, broken bones, sprains, dislocations
- Broken eyeglasses or frames

Sexual abuse

- Bruises around breasts, genitals or anus
- Unexplained venereal disease, infections, bleeding

Use a collaborative approach to prevention

The NCEA, working in partnership with experts in the field, has developed a seven-step collaborative approach to elder abuse prevention planning.

Step 1 Assemble a team of advocates, including administration, staff and ombudsmen, adult protective services, licensing and Medicaid fraud experts, to work together on risk prevention.

Step 2 Negotiate a team agreement that clearly defines roles and responsibilities and states explicit goals and objectives.

Step 3 Bring team members together for brainstorming sessions, and keep communications open.

Step 4 Share information and learn about abuse risks in the nursing home.

Step 5 Come up with creative ideas to help reduce risks and prevent abuse.

Step 6 Reach a consensus on action steps and create a clear plan for follow-up.

Step 7 Combine knowledge, perspectives and skills to reduce risks.

This overview is available for download from ncea.aoa.gov.

Make sure you're covered

Please reach out to Church Mutual with any questions about liability or insurance coverage related to elder abuse at residential care facilities. For assistance, contact your agent directly, visit churchmutual.com or contact our Risk Control Consulting and Research Center at (800) 554-2642, ext. 5213, or riskconsulting@churchmutual.com.

If your organization needs help screening job applicants and volunteers, please contact our corporate partner Trusted Employees at trustedemployees.com or (877) 389-4024.

Financial abuse

- Significant withdrawals from accounts, items or cash missing
- Suspicious changes in wills, power of attorney, policies, etc.

Psychological abuse

- Trembling, clinging, cowering, lack of eye contact, agitation
- Shame, depression, anxiety, confusion, disorientation

Relevant Data

Better Decisions

The Right People

Looking to hire trustworthy people? Turn to the trusted resource that Church Mutual recommends

As a leader in the applicant screening industry, Trusted Employees has helped organizations find trustworthy people for more than 20 years — and we prove our worth regularly to corporate partners such as Church Mutual Insurance Company and more than 5,000 active clients. You can rely on our expertise for criminal background checks, drug tests, identity checks, education verifications, and more. We make it easy for you to monitor and compare candidates as they move through the screening process. And our turnkey services are scalable, compliant, customizable — and affordable.

Let us know you're a Church Mutual customer, and you'll enjoy special discount pricing!

For screening of new hires, employees or volunteers, let us provide the customized solution you need to make the best hiring decision. Contact Trusted Employees today at trustedemployees.com or call (877) 389-4024.



Listening. Learning. Leading.®

Church Mutual Insurance Company | churchmutual.com

3000 Schuster Lane | P.O. Box 357 | Merrill, WI 54452-0357

Editor: Amy M. Kimmes | (800) 554-2642, Ext. 4529 | akimmes@churchmutual.com

Risk Control Advisor: Edward A. Steele, CSP, ARM | (800) 554-2642, Ext. 4403 | esteele@churchmutual.com

Risk

Fall/Winter
2015

Vol. 16
issue 3

Reporter

A quarterly publication by Church Mutual Insurance Company

Church Mutual Insurance Company
3000 Schuster Lane
P.O. Box 357
Merrill, WI 54452-0357