IMPORTANCE OF TIMELY CLAIM REPORTING

Quarterly Issue: December 2019

POMS & ASSOCIATES RISK SERVICES

Timely reporting of claims is a crucial element of the claims process and should be well supported by the policies and procedures of your institution. Failure to report a claim in accordance with the policy's requirements can result in a claim being denied, or worse, having the entire policy voided. Furthermore, promptly reporting claims enables you to take full advantage of the resources and expertise provided by your carriers.

To illustrate, it's easy to see why reporting a burst pipe immediately is critical. Until the pipe is repaired, water will continue to cause further damage to the property. The more damage water causes, the more it costs to repair the damage. In 2014, the University of California Los Angeles suffered a water main break, releasing 75,000 gallons of water per minute– ultimately more than 20 million gallons–causing severe water damage by flooding subterranean parking structures and the Pauley Pavilion sports arena, as well as damaging other structures and causing business interruption losses.

Fortunately, campus risk management immediately informed their excess carriers of the circumstances, who were then able to provide consultative expertise as well as send local and excess carrier adjusters onsite with resources to assist in the remediation process. The prompt reporting by campus risk management was essential in preventing further damage caused by delays.

With general liability, the need to even report a claim or incident is not always as obvious as a burst pipe in a building. However, it is still critical that you report instances of even possible claims to CCMSI "as soon as possible" or "as soon as practicable." After all, an

Important Contact Information

NMPSIA	1-800-548-3724
Poms & Associates	505-797-1354
CCMSI	1-800-635-0679
Myers, Stevens, Toohey - Student Accident Insurance	1-800-827-4695 ext. 616

Richard Valerio
NMPSIA Interim Executive Director
Richard.Valerio@state.nm.us

insurance policy is a binding contract between two parties that often includes strict reporting requirements for claims. While there are many reasons organizations would delay or exercise a reluctance to report claims–such as fear of an increase in premiums or not realizing a claim is reportable until sometime later–to delay beyond what a "reasonable person" would do in submitting notice could compromise the insurance agency's ability to settle the matter expeditiously and thus forestall your case.

For example, in the case of cyber liability claims, the [carrier for NMPSIA](#) requires that any claims be filed within the policy year or they will be automatically denied.

Avoiding prompt reporting can result in your insurer deciding the following:

1. the claim being denied for missing a reporting deadline as outlined in the insurance policy,

2. the claim being denied for not fulfilling the reporting requirements which typically involves a list of information that must be included with the claim submission to establish a sufficient notice of the claim or loss, or

3. the undue lag-time between the first notice of loss sent from your institution to the insurer causing a costlier discovery process from resources of investigators, claim adjusters and/or attorney fees.

The sooner a claim is reported, the sooner it can begin to be managed and the less it will ultimately cost.

Workers' Compensation and Property & Liability claims should be reported to CCMSI to the following individuals:

CCMSI Claims Contact Information

Worker's Compensation	Jerry Mayo	jmayo@ccmsi.com	505-837-8730
Property & Liability	Greg Ramirez	gramirez@ccmsi.com	505-837-8722

CCMSI General Inquiries

State Director	Louis Carpenter	lcarpenter@ccmsi.com	505-837-8766
Claims Manager - P&L	Kevin Sovereign	ksovereign@ccmsi.com	505-837-8752
Regional Vice President	Rich Cangiolosi	rcangiolosi@ccmsi.com	505-837-8750

For claims regarding Student Accident Insurance, contact **Myers-Stevens & Toohey & Co., Inc.** at **1-800-827-4695**.

PROTECTING YOUR SCHOOL FROM RANSOMWARE

A [recent ransomware attack](#) prompted the shutdown of all computers and internet servers across the Las Cruces Public Schools. The IT department discovered that some of the District's servers were compromised and they quickly shut down the district's entire computer network in order to contain the virus. Even if a ransomware attack is caught early, recovering from the attack can take significant time and effort.

Ransomware is a type of malicious software, or "malware," through which cyber criminals take remote control of computer systems and threaten to destroy, share, or retain information and data unless the owner of the system pays a ransom. As the [Federal Trade Commission explains](#), attackers can employ a ransomware attack in several different ways, including through phishing emails, exploiting server vulnerabilities, infected websites that download malware onto a system, or online ads—even on trusted websites.

There are several steps schools can take to protect against and limit the impact of such attacks.

How Do I Protect My School Against Ransomware?

US-CERT recommends that users and administrators take the following preventive measures to protect their computer networks from ransomware infection:

- **Employ a data backup and recovery plan** for all critical information. Perform and test regular backups to limit the impact of data or system loss and to expedite the recovery process. Note that network-connected backups can also be affected by ransomware; critical backups should be isolated from the network for optimum protection.

- **Keep your operating system and software up-to-date** with the latest patches. Vulnerable applications and operating systems are the targets of most attacks. Ensuring these are patched with the latest updates greatly reduces the number of exploitable entry points available to an attacker.

- **Maintain up-to-date anti-virus software**, and scan all software downloaded from the internet prior to executing. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic.

- **Restrict users' ability (permissions) to install and run unwanted software applications** and apply the principle of "Least Privilege" to all systems and services. Restricting these privileges may prevent malware from running or limit its capability to spread through the network.

- **Avoid enabling macros from email attachments.** If a user opens the attachment and enables macros, embedded code will execute the malware on the machine.

- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net).

- **Open email attachments and links with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it.

- **Verify email senders.** If you are unsure whether an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Train your organization.** Organizations should ensure that they provide cybersecurity awareness training to their personnel. Ideally, organizations will have regular, mandatory cybersecurity

awareness training sessions to ensure their personnel are informed about current cybersecurity threats and threat actor techniques. To improve workforce awareness, organizations can test their personnel with phishing assessments that simulate real-world phishing emails.

How Do I Respond to a Ransomware Infection?

- **Isolate the infected system.** Remove the infected system from all networks, and disable the computer's wireless, Bluetooth, and any other potential networking capabilities. Ensure all shared and networked drives are disconnected whether wired or wireless.

- **Turn off other computers and devices.** Power-off and segregate (i.e., remove from the network) the infected computer(s). Power-off and segregate any other computers or devices that shared a network with the infected computer(s) that have not been fully encrypted by ransomware. If possible, collect and secure all infected and potentially infected computers and devices in a central location, making sure to clearly label any computers that have been encrypted. Powering-off and segregating infected computers and computers that have not been fully encrypted may allow for the recovery of partially encrypted files by specialists.

- **Secure your backups.** Ensure that your backup data is offline and secure. If possible, scan your backup data with an antivirus program to check that it is free of malware.

Immediately report the ransomware attack to both *NMPSIA and [Beazley Breach Response (BBR)](#)*. Every insurance policy is considered a contract creating obligations for both the insured and the insurer. ***It should be noted that BBR requires that any claims be filed within the policy year or they will be automatically denied.***

Training
Poms & Associates has an online training available at no additional cost to your organization.

Cybersecurity: Practical Steps to Avoid Risk
The main objective of this training course is to describe common cybersecurity threats and what you can do to prevent them from happening to you at work or at home. At the end of the session you will be able to identify various types of cyber threats, such as malware, phishing and spam, and how to protect yourself when using email, social media, instant messaging and other communication systems. (Duration: 21:59)

It covers:
- Basic cybersecurity concepts
- Authentication
- Malware, viruses, and ransomware
- Mobile devices
- Phishing
- Social media

If you are interested in training for yourself and other employees, please contact us at pomsconnects@pomsassoc.com

INSECTS, SNAKES, AND ANIMALS

It often seems the least of a school's worries—that a student could get bitten by a snake or stung by an insect—but it is more common than many believe. For example, on November 4th, 2019 a student at Sandia Vista Elementary School in Rio Rancho was bitten by a rattlesnake while playing on the school's playground.

Although most insect bites and stings are no more than annoying and at time painful, there are cases where they can be more serious, and even lead to death if they go untreated. Certain animals and snakes can pose a serious threat from bites, scratches, or even just contact, especially if they carry a disease. There is always a risk of infection from bites and rabies is always a concern.

Here in New Mexico, we certainly have our share of stinging, biting, and crawling critters and animals. OSHA has a requirement that addresses working where harmful animals (and plants) are present. If you may be exposed to them, you must be informed about the potential hazards or dangers. This includes insects and snakes. How do you avoid them, and what are the first aid procedures you need to use in case of injury?

Snake Bites
Naturally, the most effective way to prevent a student or coworker from being bitten by a venomous snake at school or elsewhere is to prevent them from interacting with the snake in the first place.

Regarding snakes, over 99% of snakebites are below the knee, and usually in the ankle area. As you may know, snakes tend to lay around near rocks and in wood or scrap piles. (Again, tall leather boots are a good source of protection, and may prevent a bite). Here are a few general rules to follow in the event a worker suffers from a snakebite:

1. Allow the bite to bleed out for 15 to 30 seconds.
2. Clean and disinfect the bitten area.
3. Wrap the area with an elastic bandage but leave the bite marks open.
4. If available, apply venom extractor. If not available, apply hard, direct pressure on the bite with a gauze pad and then tape in place.
5. Cool the wound without the use of ice (this retards the venom movement) and seek medical attention.

If your employees do work in areas where snakes are likely to be a concern, snakebite kits should be available.

Insect Stings and Bites
Some personal protection measures you can use to avoid insect stings:

- Foot protection. Many insects are ground-dwellers or remain in low-lying foliage. Tall leather boots are effective.
- Avoid wearing sweet scented colognes, perfumes, or deodorants.
- When eating, remember that insects are naturally attracted to food odors.

If you get stung, scrape the stinger away from your body. Squeezing the stinger actually releases more venom. Apply some hydrocortisone cream or calamine lotion. Cold water or ice will reduce the pain. If you can, move inside because the venom from a wasp sting attracts other wasps.

Prior to beginning work in questionable areas, find out if there are any workers who are allergic to certain venoms or bee stings. These individuals require immediate medical attention, or they could die from a sting.

Other Animals
Many animals are instinctively attracted to shelters and waste areas. They also may be carrying serious diseases. Infections are not uncommon among them and rabies can be transmitted from not only wild animals but also from stray and wandering cats and dogs.

First aid for animal bites and scratches includes cleansing the wound area with soap and potable, or non-contaminated water, applying an antibiotic cream, and then covering it up.

WHEN THE ROMANCE ENDS, THE RISK OF SEXUAL HARASSMENT BEGINS

Colleges and Universities are usually aware of the liabilities surrounding student-on-student sexual harassment and assault and have enacted many trainings, programs, and services to mitigate the risks. However, many institutes of higher education have overlooked a significant area of risk: student-professor relationships.

A Wisconsin state university recently agreed to settle a sexual harassment lawsuit filed by a former student who alleged the university responded to her sexual harassment complaint "with deliberate indifference." According to court documents, the student engaged in a consensual relationship with an art professor, but experienced harassment when she tried to end the relationship. She stated the professor harassed her, emotionally traumatized her, destroyed her artwork, pressured her to have sex, and coerced her into taking "morning after" medication to avoid pregnancy.

The student claimed the head of the art department knew about the professor's relationship with her but took no action to report the misconduct. Two years later, the university investigated and determined the professor had violated the university's sexual harassment and consensual relationship policy. This led to the professor's resignation.

As part of the settlement, the university will pay the former student $325,000.

Commentary and Checklist
Relationships between students and professors are not unheard of, but even if they are consensual, they

can still lead to all sorts of problems. A professor is in a position of authority over a student, whether the professor is the student's teacher or supervisor, and relationships where one person is in a position of significant power over another can lead to sticky situations.

Sexual harassment involves comments and actions that are unwelcome and severe or pervasive. However, in educational settings, institutions often have internal policies prohibiting even consensual relationships between students and professors to avoid sexual harassment claims and avoid claims of favoritism and unjust grading.

Consensual relationships can end at any time, and when they do, sexual harassment risk arises, especially if one party begins to harass the other party about the breakup.

Here are some suggestions for educational institutions to help avoid sexual harassment risk:

- Develop a policy that prohibits workplace romances, especially between people of unequal power or authority (e.g., a professor and a student; a department head and an assistant professor).
- Educate all staff members on the risks associated with workplace relationships and inappropriate communication.
- If you allow relationships between employees, include a provision requiring them to report the relationship so any conflict of interest can be addressed.
- Offer multiple reporting mechanisms for any reports of sexual harassment or other sexual misconduct.
- Immediately investigate all sexual harassment reports regardless of who they involve. Take steps to protect the victim and the accused from further harassment and retaliation.

Poms & Associates strongly recommends implementing a policy that prohibits all consensual relationships between faculty and undergraduate students, regardless of whether a faculty member has ever had teaching, evaluative, or other supervisory authority over the student.

Below are some useful links with more information as well as model policies your school can enact.

- Northwestern University
- Stanford University
- University of Michigan
- Georgetown University

SAFE WINTER DRIVING

According to the US Department of Transportation, over 673,000 people are injured and around 7,400 people are killed each year in weather-related driving crashes. Winter driving can be hazardous and scary, especially in the New Mexico northern regions that get a lot of snow and ice. Additional preparations can help make a trip safer, and help you deal with any potential emergencies.

The following tips can help make your winter trips safer:

Remember the three Ps of Safe Winter Driving:
- **PREPARE** for the trip;
- **PROTECT** yourself;
- **PREVENT** crashes on the road.

PREPARE
Maintain your vehicle(s) by checking your brakes, lights, battery, tire tread, and windshield wipers to ensure they are all in good working order. Check your antifreeze level and use no-freeze fluid in your washer reservoir.

Have on hand: flashlight, jumper cables, abrasive material (sand, kitty litter, even floor mats), shovel, snow brush, and ice scraper, warning devices (like flares) and blankets. For long car trips, add food, water, any medication, and a cell phone and cell phone charger.

Stopped or Stalled? Stay in your car, don't overexert, put bright markers on antenna or windows and shine dome light, and, if you run your car, clear the exhaust pipe and run it just enough to stay warm.

Plan Your Route by allowing plenty of time to get to each destination. Check the weather on your route before you leave. Familiarize yourself with your directions and let others know of your route and arrival time.

Practice cold weather driving!
- During the daylight, rehearse maneuvers slowly on ice or snow in an empty lot
- Steer into a skid
- Know what your brakes will do: stomp on antilock brakes, pump on non-antilock brakes
- Stopping distances are longer on water-covered roads and ice
- Don't idle for a long time with the windows up or in an enclosed space

PROTECT
- Buckle up and use child safety seats properly
- Never place a rear-facing infant seat in front of an air bag
- Children age 12 and under are much safer in the back seat

PREVENT
- Drugs and alcohol never mix with driving
- Slow down and increase distances between cars
- Keep your eyes open for pedestrians walking in the road, or cars pulled off on the shoulder
- Avoid fatigue by getting plenty of rest before your trip, and stopping to stretch every three hours