Health & Retirement Services of Illinois

Newsletter September 2020

OUR NEWS LETTER HRSI

PROTECT YOURSELF WHEN PICKING UP PRESCRIPTIONS

It's important to keep taking your medications as prescribed during the COVID-19 pandemic. Here are some tips to help you protect yourself from COVID-19 when getting your prescriptions:

- If possible, call in prescription orders ahead of time.
- Use drive-thru windows, curbside services, mail-order, or other delivery services.
- Try to make one trip, picking up all medicine at the same time.
- If you go into the pharmacy, remember to wear a face covering and maintain social distance.

During this time, you may also want to contact your Medicare prescription drug plan to see if they've temporarily waived certain requirements to help prevent the spread of COVID-19 — like waiving prescription refill limits or relaxing restrictions on home delivery or mail delivery of prescription drugs. You can also ask your Medicare drug plan about **extended-day supplies.**

For more general information about COVID-19 and your Medicare coverage, visit **Medicare.gov.**

In Our Newsletter

Create your online Medicare account

Have you created your official **online Medicare account** yet? It's a secure way for you to access your personal Medicare-related information anytime.

It takes just a few minutes to create your account. Then you'll be able to:

- **View your claims** as soon as they're processed.
- **Add your prescriptions and pharmacies** to help you better compare health and drug plans in your area.
- **Sign up to go paperless.** Get your yearly "Medicare & You" handbook and claims statements (called "Medicare Summary Notices") electronically, instead of by mail.
- **Print a copy of your official Medicare card** — and more.

Start managing your Medicare information online — create your account today!

What to know about contact tracing

If you've been in close contact with someone who tested positive for COVID-19, you may be contacted by a contact tracer or public health worker from your state or local health department in an effort to help slow the spread of the disease. Here's what to know if you get a call:

- **A contact tracer may call** to let you know you may have been exposed to someone with COVID-19. All information you share with a contact tracer, like who you've been in contact with and your recent whereabouts, is confidential.
- **You may be asked to self-quarantine for 14 days.** This means staying home, monitoring your health, and maintaining social distance from others at all times.
- **You may be asked to monitor your health and watch for symptoms of COVID-19.** Notify your doctor if you develop symptoms, and seek medical care if your symptoms worsen or become severe.

Revealed – the top states for data breaches

by Ryan Smith 07 Aug 2020

California has suffered more data breaches since 2005 since any other state, according to a new analysis by Comparitech.

Comparitech analyzed both the number of data breaches and the total number of records exposed from 2005 to the present. Key findings of the analysis included:

- California suffered the most data breaches – 1,777 since 2005. It also had the most records exposed at 5.6 billion. California was followed by New York (863 breaches), Texas (819), Florida (638) and Illinois (533).
- North Dakota, South Dakota, Wyoming, West Virginia and Puerto Rico reported the fewest data breaches, with each having 33 or fewer over since 2005.
- Since 2005, 12,098 data breaches have occurred across the country, involving more than 11.1 billion records.
- The current cost of each lost or stolen record averages $150, amounting to more than $1.66 trillion lost since 2005.
- 2017 holds the record for most US data breaches in a year at 1,683.
- 2016 holds the record for number of records exposed at 4.6 billion.

“The number of breaches is not always proportionate to the number of records exposed,” Comparitech said. “In many cases, a single severe data breach accounts for the vast majoriy of records exposed in a state over the last decade.”

Wrongful use of data: The next cyber storm brewing on the horizon

by Bethan Moorcraft 17 Aug 2020

It's one storm after another for the cyber insurance market. Five years ago, the biggest concern for cyber insurers was the protection and security of payment card industry (PCI) data. This is thanks partly to the infamous Target breach in 2013, through which the retail giant lost 40 million payment card credentials and 70 million customer records at the height of the holiday shopping season. The Target breach was followed closely by an even bigger breach at Home Depot in 2014, whereby hackers infiltrated the retailer's point of sale (POS) system and stole more than 50 million customer credit card numbers and 53 million email addresses.

Eventually, cyber risk controls caught up with the losses and the PCI data breach storm subsided … but it was blown over by the equally menacing storm of ransomware. Nick Economidis (pictured), vice president, eRisk at Crum & Forster, commented: "We're right in the middle of the ransomware storm, but it's not going to last forever. We're seeing some significant improvements in risk controls, and I'm optimistic we're going to see some effective responses from law enforcement to clamp down on the problem. This doesn't mean ransomware will go away completely, but it will become a lot more manageable."

With cyber insurers, risk managers and regulators starting to get to grips with ransomware, what's the next cyber storm brewing on the horizon? Economidis has his sights set on issues surrounding the wrongful use or wrongful collection of data.

"We're already starting to see this storm in the form of class action lawsuits arising from the collection of biometric information in the state of Illinois," he said. "Illinois has a fairly unique law that governs the use and collection of biometric information and the disclosures that need to be made to the consumer when that information is collected. We're seeing a fair amount of class action claims being made against entities in Illinois for their failure to meet the terms of those requirements."

While biometric data suits are limited so far to the state of Illinois, there are lots of other privacy laws and regulations that companies can easily trip up on. Two of the big ones at the moment include the European General Data Protection Regulation (GDPR), which has extra-territorial reach that applies strict regulation on any company offering goods or services to EU residents or monitoring the behavior of EU residents, as well as the California Consumer Privacy Act (CCPA), the strictest privacy law to be enforced in the US so far.

"As these laws go into effect, we'll start to see regulators looking to enforce them. They'll probably start with some soft enforcement, but then I think they'll start looking for people that they want to make examples out of," said Economidis. "Regulators often target the larger entities first, but then they'll go after smaller entities if they feel they aren't managing the law the way they want it managed. They want to set some examples and put some precedents in the world, and I think we'll soon start to see that more clearly with both GDPR and CCPA.

"Closely following that, I think we're going to see some attorneys, particularly plaintiff class action attorneys, looking at these privacy laws and trying to figure out how they can put these laws to use. I think they're going go after people in the market that they think are examples of the worst behavior, or at least examples of behavior that they don't want to see continued in the market. As they do that, I think we're going see more and more litigation around what is fair use and what is fair collection of information - and that litigation is going to be expensive, and someone's going to have to pay for it."

When asked whether he felt insureds really understand the connection between data collection, data security, and the cyber insurance policy, Economides said a lot of insureds overestimate the reach of a typical cyber policy.

"I think people expect their cyber policies to do a lot more than they actually do," he told Insurance Business. "It's like automobile insurance, where people expect their automobile policy to cover everything to do with their automobile. It's the same when it comes cyber; they expect their cyber policy to cover everything to do with their computer system, and so lots of people try to make claims for things that are far beyond the intention of the policies. Historically, when cyber policies first came out, they were limited to a failure of computer security, and very specifically a failure of the insured's computer security. They have broadened out significantly over time, partly because customers kept trying to make claims for things that were not covered. They just saw the word cyber and thought that gave them protection for all cyber-related risks."

Insurance carriers are somewhat tentative about providing coverage for wrongful use or wrongful collection of information because it's still very much an evolving risk. They don't have the loss data and they don't have a good understanding of what the aggregate cost will be, therefore it's a hard risk to price for. Forecasting such a gray area is "an area of difficulty and uncomfortableness for a lot of carriers," according to Economidis.

"There's also a bit of a maintenance problem," he added. "Cyber risks are constantly changing, and the policies need to be constantly updated, which is a lot of work for the insurers. They need to do the maintenance on their policy forms so they're covering the risks that are important to their policyholders today, but, at the same time, they're a little uncomfortable because these are new risks so they don't have a lot of data and they're not really sure what the ultimate costs are going to be. I think the dynamic between those two things makes this a little challenging for insurers.”

What's the rub on cleaning and disinfection?

by Gabriel Olano 20 Aug 2020

One of the changes borne out of the COVID-19 pandemic is increased mindfulness about cleanliness and sanitation to help stem the spread of the disease. With most people having become neat freaks over the past few months, businesses make sure to keep their premises clean to avoid violating health regulations and facing possible liability in case of COVID-19 transmission.

According to Eric Hu, senior risk engineer at Swiss Re Corporate Solutions, COVID-19 has made cleaning and disinfection a top risk management and C-suite-level concern. This is a huge departure from half a year ago, when CEOs were unlikely to lose sleep over how often surfaces were cleaned and how.

Cleaning and disinfection may seem synonymous to each other, but, according to Hu, it is especially important during a pandemic to know the distinction between the two.

“Cleaning is the removing of soiling – visible or invisible – on a surface, and is a key step to take prior to disinfection, in which the presence of even a small particle of dust or dirt renders itself ineffective,” said Hu. “Not appreciating the differences, businesses may unknowingly disinfect before cleaning or disinfect without cleaning, both of which would not effectively eliminate the COVID-19 virus.”

Due to the current health crisis, the process of cleaning and disinfecting has changed dramatically and, because of that, proper training of staff undertaking this task is essential for effectiveness and safety of employees and customers when reopening public spaces, he said.

What are the risks involved?

Hu said that companies should also thoroughly vet all third party contractors hired to undertake the cleaning and disinfection process on their behalf.

Due to the increased demand for such services, many cleaning companies who have previously not been very active in the field are now aggressively marketing their services.

“It is important that businesses consider the third party’s qualifications and track record of providing such services and also have an auditing program in place to ensure the job is being done to the level of detail needed to be effective,” Hu said.

Another important consideration when selecting a third-party provider is whether they have adequate general liability cover.

“Take the example where you’re an office tower, and the cleaning and disinfection is outsourced to an external service provider,” Hu said. “In the case where someone contracts COVID-19 and it is traced back to the building, while the owner of the building would be liable, the cost would be borne by the third party provider and covered under their general liability policy.”

Increased storage of disinfectant agents containing high percentages of alcohol puts premises at higher risk of fires, while certain disinfectants can cause irritation to skin without the proper protective measures, and prolonged exposure to UV lights may damage skin and eyes.

“Cleaning too often or with agents that are too harsh for the surface’s material could result in physical damage due to erosion,” Hu added. This could lead to additional costs to replace the damaged material or surface. Disinfecting too often with an unsuitable agent may also cause resistant germs to emerge.

Hu reminded businesses to always refer to their local government, health agencies and the industry bodies or the guidance and standards required when it comes to cleaning and disinfection.

Importance of proper information dissemination

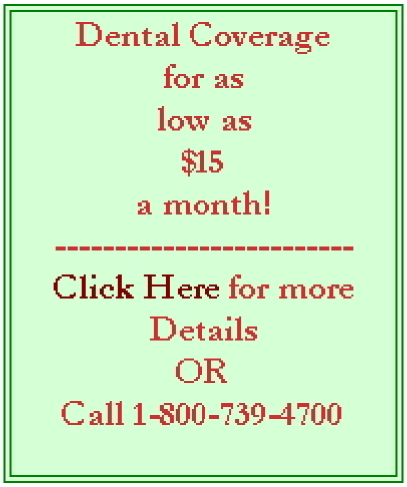
While best practices may vary depending on many factors including industry, size, the organization’s purpose and customer demographics, it is important that cleaning and maintenance staff know what to do in advance as well as receive training. They must also know how to handle any new materials and equipment they need to carry out their part of the cleaning and disinfection plan.

Aside from cleaning and maintenance staff, customer-facing staff must also be well-informed, so they are able to address questions from customers.

“Customers need to know what you are doing and why you are doing it to feel comfortable and understand any role they have to play, such as hand sanitization and wearing face masks,” Hu said.

Furthermore, Hu reminded organizations to put more effort into disseminating information and avoid relying solely on email or posters.

“Communicate the plan on a personal basis where possible, especially to those who it will impact the most, such as cleaning staff, and those who need to communicate the plan to others, such as reception and HR staff,” he said. “Communication is key to the adherence to a plan. People need to understand why they must do things. If they do not understand this, then they are far more likely to cut corners.”



Dental Coverage
for as
low as
$15
a month!

Click Here for more
Details
OR
Call 1-800-739-4700

To contact us: go to www.healthcareil.com or Call (800) 739-4700