TMC
TOTAL MEDICAL COMPLIANCE

888.862.6742
www.totalmedicalcompliance.com

MARCH 2022

THE ADVISOR

MONTHLY COMPLIANCE COMMUNICATOR

COVID-19: WHAT NOW?

Numbers of new cases of COVID-19 infections are at the lowest they have been in months. In fact, many states, as well as counties, are easing restrictions such as mask mandates indoors. These decisions are based on new tools created by the CDC to reduce risk of exposure and possibly infection and to reduce the burden this pandemic has placed on especially the hospital system. This comes as a welcomed relief for many but may be a source of confusion for those in healthcare because the recommendations included in this new tool do NOT apply to healthcare facilities. Discussed below are the two different tools designed to be used to reduce risk of exposure and possibly infection and to reduce the burden this pandemic has placed on especially the hospital system. There are two different tools available.

- √ Community Transmission: Applies to all healthcare entities
- √ Community Levels: Applies to the general population

Community Transmission

Community transmission is based on the numbers of new COVID-19 cases and communities positivity testing rate. When there is evidence of community transmission, the likelihood of coming into contact with an individual who is either asymptomatic or pre-symptomatic is increased. This situation leads to an increased risk of being exposed to the virus and possible infection.

IN THIS ISSUE

OSHA COMPLIANCE

Each practice or facility should continue to follow the existing CDC infection control guidance based on their county's level of community transmission. The OSHA Compliance tool should be checked on a weekly basis to identify the level of community transmission in your area. Some infection control measures could be adjusted based on the transmission level. For instance, when performing aerosol generating procedures in an area with substantial to high levels of community transmission, an N-95 respirator should be used. Once the transmission levels fall below substantial, a decision may be made to move forward with the procedures with a surgical mask and eye protection.

TMC has received numerous questions about masking in general, as the guidance can be confusing. To be honest there is no simple "...Yes of No..." answer on whether to wear a mask. The current infection control guidance includes universal masking except in very limited areas of the facility where only staff congregate. As part of assessing the hazard of this activity, it would be important to review current data about community transmission, the vaccination rate of employees, as well as the number of employees who have had COVID-19 in the past 90 days. In short, each practice must be in constant assessment mode to determine how they can best protect their workers and the patients receiving care.

On the other hand, Federal OSHA has been very direct. They have withdrawn the COVID-19 Healthcare Emergency Temporary Standard. Most state OSHA programs have either withdrawn or are in the process of withdrawing their standards. This means for the most part there are no "laws" outlining safeguards which must be in place to protect workers against exposure to this virus. Employers must still be aware of the risk, evaluate their situation and provide safety measures in the workplace referencing the requirements of the General Duty Clause and creating a safe workspace.

Community Levels

In late February the CDC created the Community Levels tool to provide direction for the general public to avoid COVID-19 infection or re-infection. Currently the CDC's new COVID-19 Community Levels recommendations do NOT apply to healthcare and does NOT change any of the infection control recommendations. This new tool assigns risk levels, which can be low, medium, or high by looking at the following data:

1. Hospital beds being used
2. Hospital admissions
3. Total number of new COVID-19 cases

Focusing on these three data points and implementing additional measures IF community levels increase can prevent strain to local health care systems which has been a continuing issue since the beginning of the pandemic.

Recommended Prevention Strategies Based on Community Level

https://www.cdc.gov/coronavirus/2019-ncov/your-healthcovidbycounty.html

Low	Medium	High
• Stay up to date with COVID-19 vaccines • Get tested if you have symptoms	• If you are at high risk for severe illness, talk to your healthcare provider about whether you need to wear a mask and take other precautions • Stay up to date with COVID-19 vaccines • Get tested if you have symptoms	• Wear a mask indoors in public • Stay up to date with COVID-19 vaccines • Get tested if you have symptoms • Additional precautions may be needed for people at high risk for severe illness
People may choose to mask at any time. People with symptoms, a positive test, or exposure to someone with COVID-19 should wear a mask.		

OSHA COMPLIANCE

In reviewing the recommended actions, you will see that mask use indoors is only included when the community level is considered high for most individuals. This change does allow for fewer masking restrictions in many areas of the country, but again, these masking recommendations do not apply to those providing healthcare services.

It has been a very long two years with many challenges. While communities move to what would be a more normal way of life, it is still important to remain diligent in the mundane. Assessment of workers and patients, the appropriate use of personal protective equipment, handwashing and clear concise communication of expectations will all work together for the safety of workers and patients.

CYBERSECURITY INSURANCE

Every business should have more than one type of insurance policy to protect it from certain issues and accidents. The healthcare industry has had a record number of cybersecurity incidents over the past two years. Ransomware has been the most devastating and preferred form of attack. This increase has forced cybersecurity insurance providers to write stricter policies and increase premium prices. Many business owners are still confused about what to consider when evaluating the need for cybersecurity insurance. General liability or umbrella policies do not cover the specific and special circumstances involved in a cyberattack. Work with your risk management or insurance provider to be sure you have the appropriate coverage since cybersecurity coverage is a supplemental or separate policy.

Here are some of the elements and costs to consider including in your policy's coverage:

- Loss and recovery of data (forensics)
- Identity protection for patients
- System restoration costs
- Breach notification costs
- Incident management by IT and office staff
- Ransom payments and possible extortion demands*
- Legal and defense costs
- Regulatory fines or other financial penalties from legal actions
- Business interruptions (e.g., due to EHR downtime)
- Reputational harm/lost business
- Professional liability

*Extortion is a newer component of ransomware and data theft incidents. It happens when the cybercriminal threatens to release or sell sensitive data after collecting a ransomware payment or uses the threat as a way to increase the likelihood of collecting a ransomware payment.

HIPAA COMPLIANCE

Cybersecurity insurance provides a certain level of protection, but it should never be used as your only protection. It can never be a substitute for proper security controls and practices, employee training and awareness, and plans for incident response, business continuity, and disaster recovery. It is common for cybersecurity insurance policies to exclude cyber-related incidents that could have been prevented by a standard security measure such as firewalls or current offline backups of critical data. Other things that might not be covered include an employee maliciously misusing or sharing patient information or causing a breach or cyberattack by sharing their username and password. Those inappropriate activities may not be covered under this type of policy. It is important to work with your risk management or insurance provider to understand your policy coverage.

You should also consider making it a contractual requirement for your vendors and business associates to have similar insurance policies in place. This will help protect the patient information and other sensitive business and financial information they manage on your behalf.

For more information, you can review the checklist provided by the FTC on its website (www.ftc.gov): Cyber Insurance and talk with your risk management or insurance provider.

CLICK HERE TO

START YOUR TRAINING TODAY!

HIPAA OSHA INFECTION CONTROL BUSINESS ASSOCIATES

OSHA NEWS

OSHA NATIONAL NEWS RELEASE

U.S. Department of Labor
February 17, 2022

WASHINGTON, DC — U.S. healthcare workers experienced a staggering 249 percent increase in injury and illness rates in 2020, based on employer-reported data, as they encountered serious safety and health hazards while serving those in need and labored countless hours battling the pandemic. In fact, healthcare and social assistance workers combined for more injuries and illnesses than any other industry in the nation.

As the nation observes National Caregivers Day on Feb. 18, the U.S. Department of Labor's Occupational Safety and Health Administration urges healthcare employers, and those in related industries, to take immediate actions to help make 2022 safer for these workers.

"We recognize our caregivers for the extraordinary sacrifices they continue to make working on the frontline throughout the pandemic to keep us healthy and safe – and we owe it to them to ensure their employers are doing all they can to protect them," said Assistant Secretary of Labor for Occupational Safety and Health Douglas Parker. "The dangers healthcare workers face continue to be of the highest concern and measures to prevent the spread of COVID-19 are still needed to protect them."

OSHA is working expeditiously to issue a final standard to protect healthcare workers from COVID-19. As the agency works towards a permanent regulatory solution, employers must continue to comply with their obligations under the General Duty Clause, the Personal Protective Equipment and Respiratory Protection Standards, as well as other applicable OSHA standards to protect their employees against the hazard of COVID-19 in the workplace.

To combat workplace injury and illness most effectively, employers should create and use a proactive safety and health program that addresses hazards, training and preventive measures to keep workers safe.

IT'S YOUR CALL

OSHA:

Q. What are some other common airborne pathogens aside from covid-19 that our office should keep in mind?

HIPAA:

Q: HIPAA covers 3 types of security controls. Two of them are administrative (processes and policies), and technical (firewalls, anti-virus, etc.). What is the 3rd?

Click Here
For Blog Link

SECURITY SCOUT

Social Media & Practice Reviews/Posts

Avoid the urge to reply to social media posts or reviews with information specific to the person who has posted. Even if it is a good review or post, you may inadvertently cause a breach.

Even though your practice did not initiate the communication, it is still your practice's unauthorized disclosure [breach] if you post a reply that:

- Acknowledges the poster is a patient or the person mentioned in the post is a patient, and/or
- Provides more information about them or their situation.

It's best to use a standard response that invites the poster to contact your office directly to discuss and resolve any issues privately.

TMC
TOTAL MEDICAL COMPLIANCE

888.862.6742
www.totalmedicalcompliance.com

MARCH 2022

THE ADVISOR

MONTHLY COMPLIANCE COMMUNICATOR

	SIGNATURE	PRINT	DATE
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			
18.			
19.			
20.			
21.			
22.			
23.			
24.			
25.			

INSTRUCTIONS

Print and post newsletter in office for staff review. Each member should sign this form when completed. Keep on file as proof of training on these topics.

IN THIS ISSUE