THE**ADVISOR**
MONTHLY COMPLIANCE COMMUNICATOR

Staying Ahead of Respiratory Illness Season: Best Practices for Healthcare Workers

Respiratory illness season is fast approaching once again and typically peaks in fall and winter. The CDC expects that the upcoming fall and winter virus season will likely have a similar or lower peak number of combined hospitalizations from COVID-19, influenza (flu), and Respiratory Syncytial Virus (RSV) compared to last year. At the time of this article, flu and RSV are being reported low nationally; COVID is elevated nationally, but there are signs of decline in many areas.

These viruses take root in the nose, mouth, airway, and/or lungs. Illnesses that have been reported are the flu, RSV, and COVID-19. Common signs and symptoms among all these illnesses range from fever, cough, runny/stuffy nose, chills, sore throat, and muscle/body aches. Some additional illness-specific symptoms include:

- COVID-19: new loss of taste or smell
- RSV: wheezing
- COVID-19 and influenza can present similar symptoms. Testing is the only way to distinguish between the two.

Illness Transmission
All these illnesses are transmitted differently. COVID-19 is reportedly transmitted through contact with respiratory fluids. A person can be exposed when an infected person coughs or speaks near them. They can also be exposed by inhaling aerosol particles. These particles can travel up to 6 feet and may be carried through the air in droplets so small that they stay in air currents, hence being at risk of being inhaled.

The flu virus is reportedly spread by large droplets when a person coughs, talks or sneezes. RSV can be spread through contact with droplets from the nose and throat of infected people when they cough and sneeze, direct contact (such as kissing the face of a child) or touching a surface with the virus on it (such as a doorknob), and then touching your face without washing your hands.

There are similar ways to prevent the spread of these illnesses. Hand hygiene is the single most critical measure in reducing transmitting organisms to your patients and your coworkers. Frequent hand washing, washing visibly soiled or dirty hands, and hand sanitizer use are three best practices when it comes to hand hygiene. The CDC also reports that vaccinations are one of the best things you can do to help protect yourself from serious diseases.

Preventing Transmission
However, there are other everyday ways to prevent transmission that can be done in healthcare to reduce the spread of these illnesses. To prevent the spread of respiratory illnesses, the CDC states that source control (masking) should be utilized when hospital admission rates are high and when levels of illness are high in your community. To alert patients of masking requirements, signs can be posted at the entrance of your facility and/or messaging on your business website, or a message can be included in their appointment reminders. Non-urgent treatment should be postponed for patients with suspected or confirmed respiratory illnesses.

Personal Protective Equipment (PPE) should be utilized and available during the delivery of healthcare. Use is determined based on the risk of exposure to blood, body fluids, saliva, and possible respiratory illness. PPE is to be provided and maintained by the employer. The different types of PPE are gowns, gloves, masks, eye protection, and N-95 respirators. N-95 respirators should be available and considered to be used during any aerosol generating procedures. Commonly known procedures that create aerosols in medical facilities are intubation, tracheotomy, CPR, bronchoscopy, and sputum induction. Dental equipment known to create aerosols are ultrasonic scalers, high-speed handpieces, air/water syringe, air polishing and air abrasion. It should be noted that fit testing is required for all N-95s prior to their first use and annually thereafter when they are used.

Employee Guidance
If a healthcare employee is sick with a respiratory illness, they should follow the CDC's guidance on when to <u>return to work</u>:

1. COVID-19:
a) HCP with <u>mild to moderate illness</u> who are not <u>moderately to severely immunocompromised</u> could return to work after the following criteria have been met:
- At least 7 days have passed since symptoms first appeared if a negative viral test* is obtained within 48 hours prior to returning to work (or 10 days if testing is not performed or if a positive test at day 5-7), **and**
- At least 24 hours have passed since last fever without the use of fever-reducing medications, **and**
- Symptoms (e.g., cough, shortness of breath) have improved.

*Either a NAAT (molecular) or antigen test may be used. If using an antigen test, HCP should have a negative test obtained on day 5 and again 48 hours later

b) HCP who were asymptomatic throughout their infection and are not <u>moderately to severely immunocompromised</u> could return to work after the following criteria have been met:

- At least 7 days have passed since the date of their first positive viral test if a negative viral test* is obtained within 48 hours prior to returning to work (or 10 days if testing is not performed or if a positive test at day 5-7).

*Either a NAAT (molecular) or antigen test may be used. If using an antigen test, HCP should have a negative test obtained on day 5 and again 48 hours later

c) HCP with <u>severe to critical illness</u> who are not <u>moderately to severely immunocompromised</u> could return to work after the following criteria have been met:
- At least 10 days and up to 20 days have passed since symptoms first appeared, and
- At least 24 hours have passed since last fever without the use of fever-reducing medications, and
- Symptoms (e.g., cough, shortness of breath) have improved.

2. Flu: Employees with confirmed flu who have a fever should be fever free for 24 hours without the use of fever-reducing medicine. Employees with suspected or confirmed flu, who do not have a fever, should stay home from work at least 4-5 days after the onset of symptoms.

3. RSV: Employees with RSV are contagious for 3 to 8 days. Employees can return to work when fever free for at least 24 hours and symptoms have improved.
With these measures in place and following the guidance from the CDC and other resources, we can provide a safe, healthy environment for our patients as well as our employees.

OSHA's New Severe Injury Report Dashboard

Earlier this month, the U.S. Department of Labor's Occupational Safety and Health Administration (OSHA) introduced a new online tool to enhance workplace safety awareness. This tool allows users to search its extensive severe injury report database and analyze trends related to workplace injuries in states under federal OSHA jurisdiction.

The Severe Injury Report dashboard makes it easy to search and download data by year, industry, state, establishment name, and Occupational Injury and Illness Classification System (OIICS) codes. It includes detailed information on all severe injuries reported by employers since 2015.

Designed for employers and employees, this dashboard is valuable for understanding how severe injuries occur within specific industries. By leveraging OSHA's tools and data, users can take proactive steps to prevent future workplace injuries.

https://www.osha.gov/severe-injury-reports

Log onto the website and use the search criteria to learn more about your area.

TRUE or FALSE? Federal law requires employers to notify OSHA of a work-related hospitalization, amputation, or loss of an eye within 24 hours of the incident?

TRUE: Standard Number 1904.39(a)(3) states you must report inpatient hospitalization, amputation, or loss of an eye within 24 hours using one of the following methods:
- By telephone or in-person to the OSHA Area Office nearest the incident's site.
- By telephone to the OSHA toll-free number, 1-800-321-OSHA (1-800-321-6742).
- By electronic submission using the reporting application on OSHA's Web site at www.osha.gov.

What information will OSHA ask for?
- The establishment name
- The location of the work-related incident
- The time of the incident
- The type of reportable event (i.e., hospitalization, amputation, or loss of an eye)
- The number of employees involved
- The names of the employees involved
- A company contact person's information
- A brief description of the incident

What happens if there is a fatality?
Employers are required to report any worker fatalities to OSHA within **8 hours** of the incident. The reporting methods remain the same as previously outlined, with the only difference being the shortened timeframe. OSHA will investigate all work-related fatalities at covered workplaces and has up to six months to complete the investigation and decide if citations will be issued.

REMEMBER: Ensure that all recordable injuries, severe injuries, and fatalities are entered into your OSHA Injury/Illness 300 logs by the end of the year. This proactive step will ensure you are fully prepared to meet the submission deadline.

It's Your Call – September 2024

OSHA: TRUE or FALSE? Federal law requires employers to notify OSHA of a work-related hospitalization, amputation, or loss of an eye within 24 hours of the incident?
TRUE: Standard Number 1904.39(a)(3) states you must report inpatient hospitalization, amputation, or loss of an eye within 24 hours using one of the following methods:
- By telephone or in-person to the OSHA Area Office nearest the incident's site.
- By telephone to the OSHA toll-free number, 1-800-321-OSHA (1-800-321-6742).
- By electronic submission using the reporting application on OSHA's website at www.osha.gov.

HIPAA: Why do healthcare providers need specialized healthcare IT providers instead of regular IT providers?
Healthcare IT providers are essential because they understand the unique requirements of healthcare organizations, particularly when it comes to regulatory compliance like HIPAA, patient data security, and industry-specific software integration. Regular IT providers may not be equipped to handle the strict privacy standards and specialized technology needs of medical practices, putting sensitive patient data at risk and potentially exposing the provider to legal consequences. Healthcare IT providers ensure both the functionality and legal security necessary for medical operations.

What to Look for in a Healthcare IT Company

Selecting the right IT company for a healthcare organization is critical to safeguarding data security, regulatory compliance, and optimal operational performance. Healthcare providers need to find a partner that can meet their specific needs while maintaining high standards of compliance, particularly with regulations like HIPAA. Below is a breakdown of key factors to consider when evaluating healthcare IT companies, along with critical questions to ask.

1. Experience and Expertise

A healthcare IT company should have substantial experience working within the healthcare sector. This experience ensures that they understand the unique challenges and requirements specific to healthcare organizations, such as patient data management and regulatory compliance.
Questions to Ask:

- What experience do you have working with healthcare organizations?
- Can you provide examples of similar projects or clients in the healthcare sector?

2. Compliance and Security

Healthcare IT providers must prioritize compliance with industry regulations, including HIPAA, and ensure that their security measures adequately protect sensitive patient information. Ask about their approach to compliance and data security to safeguard your organization from potential violations and breaches.
Questions to Ask:

- How do you ensure compliance with healthcare regulations such as HIPAA?
- What measures are in place to protect patient data and ensure data security?
- Are alerts set up for unusual activity?
- Are you willing to sign a Business Associate Agreement (BAA)?

3. Service Scope and Customization

Not all healthcare organizations have the same IT needs. A provider that offers customizable services tailored to your organization's specific requirements can provide more value.
Questions to Ask:

- What specific IT services are included in your managed services package?
- Can your services be customized to meet the unique needs of our organization?

4. Support and Response Time

In a healthcare setting, quick and reliable IT support is crucial. Understanding the company's support structure, response times, and availability will give you confidence in their ability to resolve issues promptly.
Questions to Ask:

- What is your standard response time for support requests?
- How is technical support provided (e.g., 24/7, on-site, remote)?

5. Disaster Recovery and Business Continuity

Having a robust disaster recovery and business continuity plan is vital for healthcare organizations. IT providers should offer solutions that protect your operations in the event of an IT failure.
Questions to Ask:

- What disaster recovery solutions do you offer?
- How do you ensure business continuity in case of an IT failure?
- Are backups completed, and how often?

6. Performance Metrics and Reporting

To maintain transparency and accountability, IT companies should offer regular performance metrics and reports that track the health and quality of your IT systems.

Questions to Ask:
- How do you measure and report on IT performance and service quality?
- Can you provide regular reports and analytics on system health and service levels?

7. Auditing Functions

IT providers should have robust auditing processes to ensure ongoing compliance and security. Regular audits of system changes, user activity, and hardware integrity help prevent issues before they arise.

Questions to Ask:
- How do you handle regular security audits and vulnerability assessments?
- What is your process for tracking and documenting system changes and access logs?
- How do you ensure audit trails are maintained and accessible for compliance checks?
- How do you address and resolve findings from internal or external audits?
- What types of audits can you complete, and what is the frequency?
  - Hard drive audit
  - User activity reviews
  - User account status/validation
  - Windows, network access

8. Cost and Contract Terms

Clear and transparent pricing is critical. Understanding the overall cost of services and any additional fees that may arise ensures there are no surprises later.

Questions to Ask:
- What is the pricing structure for your services?
- Are there any additional costs or fees not covered in the initial contract?

9. Scalability and Future Needs

A healthcare organization's IT needs may grow over time, so it's essential to choose a provider that can scale with your organization and integrate new technologies seamlessly.

Questions to Ask:
- How scalable are your services if our needs change or expand?
- How do you handle updates and integration with new technologies?

10. Onboarding and Transition

The transition to a new IT provider should be smooth and minimize disruption to your operations. Understanding their onboarding process can help you gauge how seamless this transition will be.

Questions to Ask:
- What is your process for onboarding a new client?
- How do you ensure a smooth transition and minimize disruptions during the initial setup?

By thoroughly evaluating potential IT providers using these questions, healthcare organizations can find the right partner that meets their needs, ensures compliance, and safeguards their data and operations.

THE ADVISOR
MONTHLY COMPLIANCE COMMUNICATOR

PRINT	SIGNATURE	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.

Newsletter Content

Staying Ahead of Respiratory Illness Season: Best Practices for Healthcare Workers

OSHA's New Severe Injury Report Dashboard

It's Your Call

What to Look for in a Healthcare IT Company

Need to contact us? Scan the QR code for all the ways to get in touch!