THE ADVIS♥R
MONTHLY COMPLIANCE COMMUNICATOR

NEW ONLINE TRAINING COURSES

Have you been to our new portal?

We think the new portal is easier to use. But don't just take our word for it. Click here to get to all the OSHA and HIPAA compliance training you need AND be sure to check out our Brand-New Course Topics:

- Human Resources
- Disaster Recovery Plan
- Safety
- Cyber Security
- Ethics
- Active Shooter
- Contingency Plan
- Anti-Kickback Statute
- Stress Management

Don't see what you need? Please let us know a topic you need as we are adding new classes all the time!

All courses are available à la carte so you can customize your training and create a safe and fun workplace for your customers and employees.

**CLICK HERE
TO LEARN MORE**

CLICK HERE TO
START YOUR TRAINING TODAY!
HIPAA OSHA INFECTION CONTROL BUSINESS ASSOCIATES

HIPAA COMPLIANCE

HIPAA PRIVACY AND CORONAVIRUS

While preparing and treating patients that have or might have novel coronavirus (2019 nCoV), it is important to remember your patient's privacy rights. HIPAA permits the sharing of patient's protected health information (PHI) for public health activities such as this without a patient authorization.

With whom and when can you share PHI for public health activities? Generally, PHI can be shared with:

- entities that are permitted by law to collect and receive health information for the purpose of preventing or controlling disease such as the CDC or a state or local health department,

- organizations such as the American Red Cross,

- others at risk of contracting or spreading a disease or condition if state law authorizes the covered entity to notify others as necessary to prevent or control the spread of the disease, and

- others involved in the patient's care such as family and friends. Providers should use their professional judgement here and obtain verbal consent from the patient, if possible.

PHI should not be shared with the media or others not involved in a patient's care without the patient's authorization.

The HIPAA minimum necessary standard still applies to the use and disclosure of PHI. The U.S. Department of Health and Human Services says that entities may rely on representations from the CDC or other public health department that the PHI requested by them about all patients exposed to or suspected or confirmed to have novel coronavirus (2019-nCoV) is the minimum necessary. In addition, a covered entity should continue to limit access to PHI to only those workforce members who need it to carry out their duties.

CLICK HERE TO
START YOUR TRAINING TODAY!
HIPAA OSHA INFECTION CONTROL BUSINESS ASSOCIATES

CORONAVIRUS: BE DILIGENT AND DON'T PANIC!

The Coronavirus is very newsworthy at this point, but it is also very important to realize that during the 2018-2019 influenza season, the United States reported an estimated 16.5 million people went to a health care provider for the flu and more than 34,000 people died in the U.S. We need to keep a focus on the impact of influenza and infection prevention measures to reduce the spread of this dangerous virus.

Coronaviruses are a family of viruses that can cause respiratory viruses which present like the common cold but may also cause severe pneumonias. You may be familiar with two other coronavirus illnesses, the Middle East Respiratory Syndrome (MERS) and Severe Acute Respiratory Syndrome.

At present we are dealing with a new or novel coronavirus (2019 nCoV) first detected in Wuhan City, China. This infection which originally was spread from animals to humans has now been spread person to person and has been reported in many international locations including the United States.

While the numbers are very low, now is the time to plan. To start with, there are two concepts that should serve as the foundation of your plan: Be diligent and DON'T panic! The CDC is constantly monitoring this rapidly developing situation and has provided many resources to assist healthcare providers as the situation continues to unfold. As always, be strict about basic infection control: hand hygiene, appropriate use of personal protective equipment (PPE), respiratory hygiene and cough etiquette.

OSHA COMPLIANCE

CREATE A PLAN

It is important to monitor reliable resources for indication of illness that may be present in your community. The CDC is the go to agency for the US at this time and will provide guidance to state and local health departments through the CDC Health Alert Network (HAN).

For healthcare providers the following direction on patient evaluation has been provided by the CDC.

CLINICAL FEATURES	and	EPIDEMIOLOGIC RISK
Fever **or** signs/symptoms of lower respiratory illness (e.g. cough or shortness of breath)	and	Any person, including health care workers, who has had close contact with a laboratory-confirmed 2019-nCoV patient within 14 days of symptom onset
Fever **and** signs/symptoms of a lower respiratory illness (e.g., cough or shortness of breath)	and	A history of travel from **Hubei Province**, China within 14 days of symptom onset
Fever **and** signs/symptoms of a lower respiratory illness (e.g., cough or shortness of breath) requiring hospitalization[4]	and	A history of travel from mainland **China** within 14 days of symptom onset

Click here for the complete flowchart on patient assessment and provision of safe care.

Patients meeting these criteria should be immediately reported to your local health department. Implement the following infection control measures in your facility.

1. Minimize chance of exposure. When possible, patients with respiratory illness should be identified prior to arrival through a triage process. Any patient with respiratory symptoms should be provided a face mask and encouraged to perform hand hygiene and cough etiquette. If the patient meets the criteria for possible 2019 nCoV they should be placed as quickly as possible in an exam room. The best-case scenario is to be placed in an Airborne Infection Isolation Room, but for most outpatient facilities, this is not possible.

2. Patient care should be delivered by a dedicated team in order to minimize worker exposure. Appropriate PPE should be utilized including gloves, gown, eye protection (goggles or face shield) and a mask. The N-95 respirator mask provides the highest level of protection against respiratory viruses but must be utilized in conjunction with a written Respiratory Protection Program.

3. Isolation of patients with possible infection should be determined on a case by case basis in conjunction with the CDC.

The CDC offers the following direction for this potential health threat: "The risk to individuals is dependent on exposure. At this time, some people will have an increased risk of infection, for example healthcare workers caring for 2019-nCoV patients and other close contacts. For the general American public, who are unlikely to be exposed to this virus, the immediate health risk from 2019-nCoV is considered low. The goal of the ongoing U.S. public health response is to prevent sustained spread of 2019-nCov in this country."

NOTE: This is a BRIEF recap of basic infection control measure. Complete guidance is provided on the CDC 2019 Novel Coronavirus webpage. **Remember: Be diligent and don't panic.**

CYBER INSURANCE

Every business should have one or more types of insurance policies to protect it from certain issues or accidents. A type of insurance still relatively new to the marketplace is cyber insurance. Since it is an immature product in many aspects, there can be a lot of confusion as to what a business should consider when evaluating the need for cyber insurance. It is rare that general liability or umbrella policies extend to the special circumstances caused by a cyberattack. The record number of ransomware attacks in 2018 and 2019 and their crippling impact on small to medium sized businesses and state and local government agencies is rapidly making cyber insurance a must-have.

According to the National Association of Insurance Commissioners, the premiums paid for cyber insurance policies in 2018 were approximately $2 billion. As with other insurance policies, it is important to know the coverage options. Work with your risk management or insurance provider to be sure you have adequate coverage. They can help you avoid buying coverage that you do not need.

> **RANSOMWARE** ATTACKS IN 2018 AND 2019 HAD A **CRIPPLING IMPACT** ON SMALL TO MEDIUM SIZED BUSINESSES...

HIPAA COMPLIANCE

The following information was obtained from the Federal Trade Commission (FTC) and the Department of Homeland Security. There are two main types of cyber insurance: first-party and third-party. They cover very different aspects of a cyber incident.

First-party insurance covers direct losses your business incurs from a cyberattack such as data theft, denial of service, and ransomware, among others. It covers the business's own damages for the incident such as the cost of providing notices to patients and providing credit monitoring services to patients, which is becoming a common state law requirement. It can also help cover costs related to any specialized technological services like data recovery and repair.

Third-party insurance covers damages that others, like patients or customers, might have because of the attack, penalties required by law, or costs related to litigation. You may also want to ensure your vendors carry if they handle any of your practice's sensitive business information or patient data.

Cyber insurance can provide a certain level of protection, but it should not be used as a substitute for proper security controls, or incident response, business continuity, or disaster recovery plans. It is common for cyber insurance policies to exclude cyber-related incidents that could be prevented by a standard security measure — like having a firewall set up. If an employee maliciously mishandles patient information or network credentials and it causes a cyberattack, it may not be covered under this type of policy.

For more information, you can review the checklist provided by the FTC on its website (www.ftc.gov): Tips & Advice > Business Center > Protecting Small Businesses > Cybersecurity > Cyber Insurance and talk with your risk management or insurance provider.

IT'S YOUR CALL

OSHA:
If we have an employee stay less than a year, are we obligated to keep their medical records?
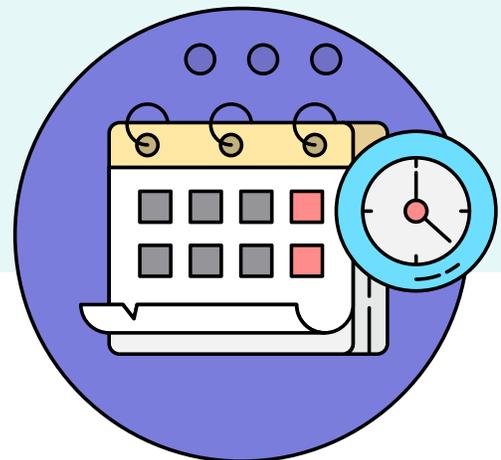
HIPAA:
By law, where should the Notice of Privacy be posted?

CLICK HERE FOR ANSWERS

WHAT IS THE DEADLINE FOR REPORTING A BREACH TO HEALTH AND HUMAN SERVICES (HHS)?

The breach if less than 500 records must be reported to the Secretary within 60 days of the end of the calendar year in which the breach was discovered. If you had a breach in 2019, the deadline for reporting is February 29, 2020.

THE ADVIS♥R

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