TMC TOTAL MEDICAL COMPLIANCE

888-862-6742
www.totalmedicalcompliance.com

MARCH 2025

THE ADVISOR
MONTHLY COMPLIANCE COMMUNICATOR

How Often Does a Safety Data Sheet (SDS) Need to Be Updated, and Who Is Responsible?

Understanding the requirements for updating Safety Data Sheets (SDS) is crucial for anyone managing hazardous chemicals or overseeing workplace safety. This article outlines when SDS updates are necessary and why accurate SDS information is vital for safeguarding employees and ensuring regulatory compliance.

But First: What Is an SDS and Why Is It Important?
An SDS, previously known as a Material Safety Data Sheet or MSDS, is a comprehensive document that provides critical information regarding the handling, storage, and risks associated with a chemical substance. SDSs are essential in workplaces where chemicals are used, stored, or transported, and they serve as a key resource for educating personnel who work with hazardous materials.

Each SDS follows a standardized format, consisting of 16 sections, each providing specific details to ensure safe handling and effective emergency response.

Newsletter Content

SDS Sections:

1. Identification: Information about the product, supplier, and recommended uses
2. Hazard Identification: Classifications, pictograms, and precautionary statements
3. Composition Information on Ingredients: Chemical ingredients, components, or concentrations
4. First-Aid Measures: Steps to take if someone is exposed to the chemical
5. Fire-Fighting Measures: Guidance on how to handle a fire involving the chemical
6. Accidental Release Measures: Procedures for responding to a chemical spill or leak
7. Handling and Storage: Instructions on safely handling and storing the chemical
8. Exposure Controls/Personal Protection: Safety equipment, Personal Protective Equipment (PPE), and exposure limits
9. Physical and Chemical Properties: Chemical characteristics, such as appearance, boiling point, or pH

10. Stability and Reactivity: Chemical stability and potential hazardous reactions
11. Toxicological Information: Potential adverse health effects
12. Ecological Information: The impact of the chemical on the environment
13. Disposal Considerations: Proper disposal
14. Transport Information: Guidelines for safe transport
15. Regulatory Information: Legal requirements and applicable safety standards
16. Other Information: Additional safety measures or revisions

SDSs are crucial in helping employees identify chemical hazards and providing clear, detailed guidance to minimize risks. They are vital in reducing accidents and injuries.

The Globally Harmonized System (GHS) of Classification and Labeling of Chemicals mandates that an SDS accompany every chemical to ensure consistency and transparency. This enables employers and employees to make informed decisions regarding the use of chemicals in their workplace. SDSs may also recommend safer alternatives or additional precautions to mitigate potential hazards.

Who Is Responsible?
Chemical Manufacturers and Suppliers:
Manufacturers and suppliers must create and maintain SDSs for each chemical product they produce or distribute. Under the Hazardous Substances Act and OSHA regulations, these SDSs must include critical information on chemical hazards, exposure scenarios, and safety measures.

Employers:
Although employers are not responsible for authoring or modifying SDS content, they play a key role in maintaining accessibility and compliance.

Employers must:

- Ensure that the most recent SDSs are readily available to employees.
- Organize an up-to-date SDS library.
- Train employees in safe chemical handling practices.
- Comply with OSHA's Hazard Communication Standard.

Up-to-date SDSs help prevent workplace incidents, ensure compliance during inspections, and support a safety-oriented workplace culture.

How Often Should SDSs Be Updated?
There is no set schedule for updating SDSs. Manufacturers are required to revise them when:

- New information about a chemical's hazards becomes available.
- Changes are made to protective measures or safe handling practices.
- Regulatory updates necessitate modifications.

Employer Best Practices
To maintain compliance and ensure employee safety, employers should follow recommended practices:

- Stay in Touch with Suppliers: Proactively contact your chemical suppliers to check for updated SDSs, especially after receiving a new chemical product.
- Regular SDS Reviews: Conduct annual audits of your SDS library to verify that all documents are current and relevant to your workplace. A chemical inventory can help identify missing or outdated SDSs.

- Employee Access: Use electronic management systems to make SDSs accessible. This approach aligns with OSHA's emphasis on easy access to hazard information.

Consequences of Outdated SDSs
Failing to maintain accurate SDSs can result in significant consequences, including:

- Regulatory Penalties: Non-compliance with OSHA's Hazard Communication Standard can lead to substantial fines and legal issues.
- Increased Safety Risks: Outdated information may fail to communicate crucial hazard details or protective measures, leading to workplace accidents or chemical exposures.

To minimize these risks, employers could invest in electronic SDS management systems that automatically update information as manufacturers release new versions.

Managing Safety Data Sheets is more than just a regulatory requirement; it is a fundamental aspect of workplace safety. By keeping SDSs accurate and accessible, businesses can minimize risks, ensure compliance with OSHA standards, and promote a safer work environment.

Rising Measles Cases: What You Need to Know

Measles is an illness that was declared eliminated in the United States in 2000, but recently there have been documented cases in the U.S. Currently, there is an outbreak in the states of Texas and New Mexico. There are also reported cases in New York, Alaska, California, Georgia, Kentucky, New Jersey, and Rhode Island.

As of March 6th, 2025, the CDC reports there are 222 confirmed measles cases in the U.S. On the contrary, as of March 11, 2025, Texas is reporting 223 cases. Most of the Texas cases are of school age children. It is reported that 95% of the cases are among those who are unvaccinated or have unknown vaccination status. Sadly, one child has died in Texas and one adult in New Mexico. Neither were vaccinated. The death of the adult in New Mexico is still being investigated for the official cause of death, but the individual did test positive for measles. More cases are expected to occur with this rapidly expanding outbreak.

The CDC has issued a Health Alert Network Health Advisory to alert clinicians, public health officials, and potential travelers about the outbreak in Texas and New Mexico. They are offering guidance and monitoring.

What is measles?
Measles is a highly contagious and serious illness. Measles can be dangerous for babies and young children. Symptoms of the illness begin 7-14 days after being exposed. Symptoms of measles include:

- High fever
- Cough
- Runny nose
- Red, watery eyes
- Rash (3-5 days after symptoms begin)

Some complications from measles include:

- Diarrhea
- Ear Infections
- Lung Infection (pneumonia)
- Brain swelling (encephalitis)
- Rare but fatal brain disease (subacute sclerosing panencephalitis)
- Death

These complications are most common in children under 5 and adults.

How does measles spread?

Measles is airborne and can spread when an infected person coughs or sneezes. It is so contagious that if one person has it, up to 10 people around them will become infected if they are not protected. You can get the illness for up to two hours after someone with measles leaves the room. An infected person can spread measles to others before knowing they have the disease, up to 4 days before developing the rash and 4 days afterward.

Prevention

Vaccination is the best way to prevent the spread of measles. The vaccine for measles also protects against the mumps and rubella. It is known as the measles, mumps, and rubella (MMR) vaccine. Two doses of the vaccine are 97% effective at preventing measles; one dose is 93% effective. The first dose should be given at 12-15 months and second dose between 4-6 years of age.

Healthcare personnel (HCP) should have immunity against measles, mumps, and rubella. HCP born in 1957 or later without serologic evidence of immunity or prior vaccination should be given two doses of the MMR vaccine at 4 weeks apart.

Being born before 1957 is considered acceptable evidence of measles immunity; however, it should be considered to administer two doses of the vaccine unless they have laboratory evidence of disease or immunity to measles and/or mumps.

Patients with measles

Patients that are known or suspected of having measles should wear a facemask when they enter a healthcare facility. They should be told before entering a facility any instructions such as which entrance to use and how to notify the staff when they have arrived. Patients with suspected or confirmed measles should be placed in an airborne infection isolation room (AIIR). Once a patient is in the AIIR, their facemask can be removed if they stay in the room. If an AIIR is not available, transfer to a facility with an AIIR should be made as soon as possible.

Attending to a patient with measles

Healthcare personnel should follow standard and airborne precautions. If possible, only healthcare personnel with evidence of immunity to measles should attend to the patient and they must use N-95 masks. Immediately report the suspected case to the local health department. Once the patient has been dismissed, disinfection procedures using an EPA registered hospital level disinfectant should be used. Manufacturers' instructions for use should be followed, including the contact time of the disinfectant. Used, disposable personal protective equipment for measles patients should be managed as regulated waste or as directed by state and local guidelines.

Training should be provided to all HCP on standard, airborne precautions, and prevention of the spread of measles and other airborne illnesses. HCP should be educated, trained, and demonstrate competency in the proper use of PPE in caring for patients with suspected or confirmed measles. Ensuring training takes place will provide a safer workplace for employees and in turn provide a safe patient environment.

How to Handle Threatening Patient Behavior

Healthcare professionals often work in high-stress environments where emotions can run high, occasionally leading to threatening or aggressive behavior from patients. Handling such situations effectively is essential to ensure the safety of everyone involved while maintaining professionalism and compassion.

1. **Recognize Early Warning Signs –** Understanding the early signs of agitation can help prevent escalation. Early warning signs of threatening behavior include:

- Raised voice or yelling
- Aggressive gestures or posturing
- Excessive pacing or restlessness
- Verbal threats or hostile language

2. Maintaining a calm demeanor is critical when faced with a threatening patient

- Avoid mirroring their aggression or raising your voice.
- Use a steady, non-confrontational tone and keep your body language open but non-threatening

3. De-escalation Techniques

- Active Listening: Show empathy by listening to the patient's concerns without interruption
- Validate Their Feelings: Acknowledge their emotions by saying things like, "I understand this is frustrating for you."
- Set Boundaries: Clearly communicate acceptable behavior, e.g., "I want to help you, but I need you to speak calmly so I can understand your concerns."
- Offer Solutions: Provide options to address their concerns, if possible

4. Ensure Safety

- Maintain a safe distance and ensure you have an exit route
- Avoid turning your back on the patient
- Remove any objects that could be used as weapons
- Signal for help discreetly if needed, using a code word or alarm system

5. **Engage Support Systems** –When de-escalation efforts are not effective, notify law enforcement if the patient becomes physically aggressive

6. Follow Institutional Protocols

Familiarize yourself with your organization's policies for handling threatening behavior. These protocols often include reporting the incident, completing the necessary documentation, and participating in debriefings to identify areas for improvement.

7. Ongoing Training

- Regular training in conflict resolution, de-escalation, and personal safety is vital. Simulation exercises and role-playing scenarios can help healthcare workers feel more prepared to handle real-life situations.
- TMC provides a training course in their catalog for Dealing with Disruptive or Threatening Patients – https://totalmedicalcompliance.com/product/dealing-with-disruptive-or-threatening-patients-course/

Threatening patient behavior poses challenges for healthcare professionals, but these situations can often be managed effectively with the right skills and strategies. By staying calm, using de-escalation techniques, and prioritizing safety, healthcare workers can protect themselves and their patients while maintaining a compassionate and professional approach.

HIPAA Compliance Starts With You: Avoiding Common Data Breach Mistakes

In today's digital healthcare environment, protecting patient information is not just the responsibility of IT or compliance officers—it is a shared duty among all employees. Data breaches can occur anywhere, from large hospitals to small clinics, and human error is often the primary cause. A single mistake, such as sending an email to the wrong recipient or leaving a workstation unlocked, can expose sensitive information. This can lead to HIPAA violations, financial penalties, and loss of patient trust.

The good news is that most data breaches are preventable. By recognizing potential risks and adopting best practices, employees can significantly contribute to data security and regulatory compliance.

Common Causes of Data Breaches

Data breaches can happen for various reasons, but some of the most common causes include:

- Lost or stolen devices – Laptops, tablets, and smartphones containing patient data can be misplaced or accessed by unauthorized individuals.
- Improper disposal of PHI – Patient information stored in paper files, hard drives, or digital formats must be properly destroyed or erased to prevent unauthorized access.
- Unauthorized access – Employees accessing patient records out of curiosity or sharing login credentials can result in major compliance violations.
- Unsecured communication – Sending protected health information (PHI) through unencrypted emails or text messages can expose sensitive data.
- Phishing attacks and cyber threats – Cybercriminals often trick employees into revealing login credentials or downloading malware through deceptive emails and fraudulent websites.

Best Practices for Preventing Data Breaches

Employees play a critical role in preventing data breaches by following these security measures:

1. Follow the “Minimum Necessary” Standard
2. Only access or share patient information when required for job-related tasks. Unauthorized access, even out of curiosity, can lead to serious consequences.
3. Secure Workstations and Devices
4. Always lock your computer or mobile device when leaving your workstation. If using personal devices for work, ensure they are encrypted, password-protected, and comply with security policies.
5. Use Secure Communication Channels
6. Never send PHI through unsecured emails or text messages. Always use approved encrypted platforms to communicate sensitive information. When in doubt, consult your compliance officer.
7. Be Cautious with Emails and Links
8. Phishing scams are a leading cause of data breaches. Avoid clicking on unexpected links or attachments in emails, especially those that request login credentials or urgent actions.
9. Create Strong Passwords and Enable Multi-Factor Authentication (MFA)
10. Use complex passwords or passphrases and update them regularly. Multi-factor authentication adds an extra layer of security against unauthorized access.
11. Dispose of PHI Properly
12. Shred paper records and securely erase digital files when they are no longer needed. Never discard PHI in regular trash or leave sensitive information unattended.
13. Report Security Concerns Immediately
14. If you notice suspicious activity, such as phishing emails, unauthorized access, or a lost device, report it immediately to your supervisor or IT department. Quick action can help prevent a potential breach.

Why Employee Awareness Matters

Most breaches result from avoidable mistakes, such as leaving patient records exposed or clicking on phishing links. Fortunately, these errors can be prevented with awareness and good security practices. By following best practices, using secure communication channels, and staying alert to threats, employees actively contribute to safeguarding patient information and maintaining organizational compliance.

TMC
TOTAL MEDICAL COMPLIANCE

888-862-6742
www.totalmedicalcompliance.com

MARCH 2025

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

How Often Does a Safety Data Sheet (SDS) Need to Be Updated, and Who Is Responsible?

Rising Measles Cases: What You Need to Know

How to Handle Threatening Patient Behavior

HIPAA Compliance Starts With You: Avoiding Common Data Breach Mistakes

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