TMC
TOTAL MEDICAL COMPLIANCE

888-862-6742
www.totalmedicalcompliance.com

NOVEMBER 2024

THE ADVISOR
MONTHLY COMPLIANCE COMMUNICATOR

OCR's Expectations for Preventing Ransomware in Healthcare

Key Lessons from the Cascade Eye and Skin Centers Settlement

The recent settlement between the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) and Cascade Eye and Skin Centers underscores OCR's expectations for healthcare providers regarding cybersecurity under the HIPAA Security Rule. Following a ransomware attack that compromised nearly 291,000 patient records, Cascade agreed to a $250,000 settlement and a corrective action plan.

This marks OCR's fourth ransomware-related settlement, as ransomware incidents in healthcare have increased by 264% since 2018. The Cascade case offers essential lessons for what OCR expects from healthcare organizations in protecting electronic protected health information (ePHI) and preventing future breaches.

Key OCR Expectations for HIPAA Compliance
OCR's investigation into Cascade's breach highlighted several critical cybersecurity gaps, which OCR requires HIPAA-covered entities to address:

1. Conducting a Thorough Risk Analysis
OCR expects healthcare organizations to perform detailed risk analyses to identify vulnerabilities in their systems. A comprehensive risk assessment must cover threats to the confidentiality, integrity, and availability of ePHI. Cascade's inadequate risk analysis was a core deficiency. OCR clarified that risk analysis must be an ongoing process, not a one-time task, allowing organizations to adapt to new technologies and emerging threats.

2. Implementing a Risk Management Plan
OCR requires organizations to create and maintain a risk management plan that addresses

Newsletter Content

identified vulnerabilities. Cascade's lack of a proactive risk management strategy left it exposed to cyber threats. OCR emphasizes the importance of documenting and routinely reviewing mitigation strategies to counteract risks before they lead to a breach, supporting a more resilient cybersecurity framework.

3. Monitoring System Activity and Access Controls

OCR mandates regular monitoring of ePHI system activity, including access logs and alerts for unusual behavior. Cascade failed to monitor its systems effectively, delaying its awareness of the ransomware attack. Real-time monitoring helps detect unauthorized access early, enabling organizations to respond quickly and minimize data exposure. With proper access controls and audit logs, monitoring is a foundational defense against cyber threats.

4. User Identification and Authentication

OCR expects healthcare entities to enforce strict user identification protocols, including unique identifiers and multi-factor authentication (MFA). Cascade's inadequate user tracking left it vulnerable to unauthorized access. Assigning unique identifiers and using MFA prevents unauthorized users from accessing ePHI, ensuring that only authorized personnel interact with sensitive data.

5. Emergency Preparedness for Cybersecurity Events

OCR's requirements include preparedness plans for handling cybersecurity incidents, such as isolating affected systems, restoring data, and notifying affected parties. Cascade's settlement outlines a need for emergency procedures to quickly address cyber events. OCR expects healthcare organizations to have a response plan that can be activated immediately, minimizing potential damage and protecting patient data.

6. Regular Review and Updating of Policies

OCR expects HIPAA-related policies and procedures to be up-to-date and reflective of the latest cybersecurity practices. Cascade's settlement underscores that outdated or poorly maintained policies put healthcare entities at risk. Regular policy reviews ensure compliance with current standards, addressing potential vulnerabilities before they result in enforcement actions.

Broader Cybersecurity Recommendations from OCR

Beyond these core compliance areas, OCR encourages additional practices to strengthen cybersecurity:

- Review all vendor and contractor relationships for HIPAA compliance and establish business associate agreements.
- Encrypt ePHI to prevent unauthorized access.
- Provide regular staff training on cybersecurity practices, underscoring each member's role in protecting patient data.

The Cascade Eye and Skin Centers case reinforces OCR's commitment to enforcing the HIPAA Security Rule amid rising cyber threats in healthcare. By adopting these best practices and staying vigilant, healthcare organizations can protect patient data, reduce vulnerabilities, and avoid costly penalties.

Instrument Processing Essentials: Steps for Effective Cleaning and Safe Packaging

Medical and Dental Instrument processing is a critical aspect of employee and patient safety and requires a series of steps. There are four steps in instrument processing: Cleaning, Packaging, Sterilization and Storage. This article will concentrate on cleaning and packaging. We will cover sterilization and storage next month.

Step 1: Cleaning Instruments
Before any instrument is disinfected or sterilized it is critical they are cleaned properly. This is the first step in instrument processing. Any contaminants that are present (dirt, blood, and other bodily fluids) must be removed prior to disinfection or sterilization. A contaminant being present acts as a barrier and prevents sterilization of the item. Contaminants should be removed as soon as possible to prevent drying of the material on the instruments.

There are two methods of cleaning instruments prior to disinfection/sterilization: manually and automated. Automated cleaning is the preferred method. Automated cleaning can be done either with an ultrasonic cleaner or washer-disinfectors. Household dishwashers are not recommended to be used. They can potentially harm the instruments and are not FDA approved to be used to clean instruments. Always follow manufacturers' instructions for use on the equipment used for cleaning. Only utilize FDA approved devices.

Automated cleaning reduces the handling of sharp instruments and reduces employee exposure risk. Manual cleaning, or hand scrubbing, puts workers in close contact with contaminated sharps and contaminated splashes and spatter generated during the cleaning process. The instruments should be scrubbed by utilizing a long-handled brush. Be sure to utilize the appropriate personal protective equipment, such as eye protection, utility gloves, mask and gown. Once instruments are cleaned, they must be rinsed thoroughly and allowed to dry before packaging.

Step 2: Packaging Instruments
Once the instruments are cleaned, dried, and inspected to ensure all contaminants are removed, they will need to be packaged. Guidelines from Association of Medical Instrumentation (AAMI) and other organizations should be followed. These guidelines state that hinged instruments should be opened and items with removable parts are to be disassembled unless the device manufacturer suggests otherwise. Follow manufacturer's instructions for preparing instruments such as concave surfaces placed downward and heavy items placed below light items to avoid damage. The wrapping must be done in a manner to prevent gaps and tenting.

There are different types of packaging material- plastic/peel pouches, paper bags, "blue" wraps for cassettes, and plastic tubing. Healthcare facilities can choose any of these options. When making a choice, the key is the packaging material must allow penetration of the sterilant, must be compatible with the type of sterilizer, and must be puncture resistant, durable, and have FDA clearance. The best practice is to always follow manufacturers' instruction on any packaging material. Not following these is considered off-label use of the product and has a negative impact on the efficacy and safety of the product used during sterilization of instruments. Plastic/peel packaging and wrapping of cassettes are the most common packaging materials utilized.

Plastic/peel packs are easy to use, easy to open after sterilization, and are widely utilized. Appropriate pouch sizes should be available to prevent overloading the pouches and to allow the sterilant to penetrate them. These packs are for small light weight items. They should not be more than 75% full of instruments. When the pack is laid flat on the counter, the instruments will lay in a single layer inside the pack. The pack must be sealed correctly, on the perforation. There should be an inch of space (finger width) on each side of the pouch.

Blue wraps or paper wraps are commonly used to wrap medical/dental cassettes. Cassettes have many advantages, including:

- less handling of contaminated instruments,
- save time in instrument processing,
- may decrease sharps injuries,
- help to maintain sterility during storage and allows an aseptic and organized presentation of instruments chairside.

Wrapping of the cassettes must be done in such a manner to avoid tenting and gapping. Double wrap is recommended, especially for surgical instruments. There is also a bonded double wrap available that can be used. There are two ways to wrap the cassette- gift style or envelope style. Either method is an acceptable way to wrap the cassette.

Healthcare facilities have many options available for cleaning and packaging instruments. You should choose the products that are suitable for your specific needs. There should be policies and procedures in place and checks and balances to ensure instruments are cleaned before packaging. Keep in mind, again, manufacturers' instructions are to be followed along with guidelines from AAMI and Centers of Disease Control.

It's Your Call – November 2024

HIPAA: How does ransomware spread?
Ransomware commonly spreads through phishing emails, malicious attachments, or compromised websites. Once a user clicks on a link or downloads infected content, the ransomware installs itself on the device, often spreading across the network to other systems.

OSHA: What should an employer do immediately after an employee reports a needlestick exposure?
The employer must provide a confidential medical evaluation at no cost, document the incident, report it to OSHA if required, and test the source patient (with consent or as permitted by law). The employer must also give the employee a written summary of the healthcare provider's evaluation within 15 days.
More information on this topic in this month's article.

Your Employee Had a Needlestick Exposure – What Do You Do?

STEP 1 – ARRANGE FOR AN IMMEDIATE MEDICAL EVALUATION

- The EMPLOYER is required to offer confidential medical evaluation, laboratory testing, and follow-up care at no expense to the employee.
- Early intervention is essential for effectively managing potential illness and preventing the transmission of bloodborne infections.
- NOTE: The employee who participates in post-exposure evaluation has the option to withhold consent for HIV testing. In this instance, the employer must ensure that the blood sample is preserved for at least 90 days if they change their mind.

STEP 2 – DOCUMENT EVERYTHING!

- Employers are required to evaluate the circumstances surrounding the exposure.
- employee injury report, witness statements, etc.

STEP 3 – REPORT THE INCIDENT (if required)

- Reporting to OSHA or other respective state agencies identifies the source individual to reduce or stop further transmission.
- Any employer who is required to maintain a log of occupational injuries and illnesses under OSHA's Recordkeeping regulation (29 CFR Part 1904) is also required to maintain a sharps injury log. Employers must record all work-related needlestick injuries contaminated with another person's blood or other potentially infectious material (as defined by 29 CFR 1910.1030) on the OSHA 300 Log.
- If an employer is exempt from the OSHA recordkeeping rule, the employer does not have to maintain a sharps log.

STEP 4 – TEST THE SOURCE PATIENT

- If the status of the source individual is unknown, the employer is required to test them as soon as possible, provided the individual consents or identification is feasible.
- If they do not consent, the employer must establish that legally required consent cannot be obtained or is prohibited by state or local law.
- State or local law may allow testing without the source individual's consent.
- When the source individual is already known to be infected with Hep B or HIV, testing for the source individual's status need not be repeated.

STEP 5 – PROVIDE RESULTS

- The employer must obtain and provide the employee with a copy of the healthcare professional's written opinion within 15 days.
  - According to OSHA's standard 1910.1030(f)(5), the written opinion should ONLY include:
    - Was hepatitis B vaccination recommended?
    - Did the employee receive the vaccination?
    - Did the healthcare provider inform the employee of the results and any medical conditions resulting from exposure that require further evaluation or treatment?
    - **Any other findings should not be included in the written report**

- When medically indicated, post-exposure prophylaxis must be offered.
- Counseling must include implications of the exposure, infection status, and how to protect others.
- The employee must be informed of laws and regulations regarding disclosing the source's identity and infectious status.
- Note: In accordance with OSHA's Standard for Access to Employee Exposure and Medical Records, 29 CFR 1910.1020, employee medical records must be accessible to both the employee and OSHA representatives.

Discover TMC's Latest Online Course Offerings

Total Medical Compliance is excited to announce the launch of its new suite of online courses designed to enhance the skills and knowledge of healthcare professionals. These courses address crucial aspects of healthcare operations, from ethical business practices and the appropriate use of company assets to maintaining physical security and managing disruptive patients. Each course offers practical insights and strategies tailored to the unique needs of healthcare providers, ensuring they can deliver the highest standards of care while safeguarding their facilities and resources. Whether you are a physician, dentist, healthcare administrator, or support staff, these courses provide valuable training to help you navigate the complexities of today's healthcare environment.

Appropriate Use of Company Assets Course
$15.00
This course is designed to educate employees on the responsible use of company resources. As an employee, you utilize various company assets such as the building, equipment, office supplies, computers, phones, cars, and even corporate credit cards. This course delves into both physical and intangible assets, providing general guidelines on how to safeguard and use these assets appropriately. By understanding and adhering to these guidelines, you can ensure that you use company resources responsibly and maintain the trust your company places in you.

A Good Guide to Business Ethics Course
$35.00
This course emphasizes the importance of ethical conduct for business success and addresses the challenges of making the right decisions under stress, overwhelm, or uncertainty. Participants will learn the fundamentals of business ethics and their significance, discover seven key principles to guide ethical behavior in the workplace, and understand how to overcome rationalizations that hinder ethical decision-making. The course also explores common ethical pitfalls and strategies to avoid them, emphasizes the importance of reporting unethical behavior, and provides comprehensive guidance on maintaining proper conduct in a professional environment.

Using Physical Security to Keep Facilities and Assets Safe Course
$15.00
In today's world, cyber threats like data breaches and phishing scams often make headlines, but the risk doesn't always come from behind the firewall; sometimes it originates within the building

itself. Cybersecurity is just one aspect of the broader information security landscape, with physical security being another crucial component that can sometimes be neglected. Our new online course offering delves into the essentials of physical safety, exploring how both organizations and individuals can implement effective strategies to protect their data and assets. The course covers various topics, including how to protect your data using physical security measures, differentiating between intentional and unintentional threats, and understanding responsibilities for physical security.

Secure Storage of Protected Health Information (PHI) Course
$15.00
This course covers the critical aspects of securing PHI, emphasizing its importance in healthcare, potential security threats, and effective safeguarding methods. Priced at $15.00, this course is invaluable for physicians, dentists, healthcare administrators, IT personnel, compliance officers, and administrative staff, helping them understand the significance of secure PHI and their roles in protecting patient data. Attendees will learn why secure storage of PHI is necessary, the importance of physical storage and security of PHI, tips on protecting digital storage of PHI, and best practices for secure cloud storage. With the flexibility to engage with the material at their own pace, this 15-minute course is perfect for busy healthcare professionals seeking to enhance their skills while balancing professional responsibilities.

Dealing with Disruptive or Threatening Patients Course
$20.00
Our new online course offering, “Dealing with Disruptive or Threatening Patients,” is designed to equip healthcare practitioners, office administrators, and staff with the knowledge and skills needed to manage disruptive patient behaviors while maintaining a safe and professional environment. This course covers general procedures, handling verbal or physical threats, addressing profanity and abusive language, managing physically violent patients, post-incident documentation, breaking bad news to patients, and terminating a patient’s relationship with the practice. Participants can engage with the 15-minute course at their own pace, making it ideal for busy healthcare professionals looking to enhance their skills while balancing professional responsibilities.

Substance Abuse & Related Mental Health Disorders for Dentistry Course
$50.00
Our new online course, “Substance Abuse & Related Mental Health Disorders for Dentistry,” is available for $50.00 and offers 1.0 credit hour. This course helps dental professionals address substance abuse and disorders like Opioid Use Disorder, following guidance from the ADA, CDC, and NIMH.
Key objectives include understanding mental health disorders linked to substance abuse, identifying at-risk patients, following ADA dosage recommendations for pain relievers, exploring alternative pain relievers, and discussing substance abuse with patients. It also provides strategies for using healthcare and community resources to support patients.

HIPAA Fraud, Waste, and Abuse Awareness Course
$30.00

Our new online course on HIPAA regulations equips employees to combat fraud, waste, and abuse in healthcare. Participants will learn to identify, prevent, and report these issues, ensuring compliance with HIPAA and protecting patient privacy and resources.
Course objectives include understanding HIPAA's role in preventing fraud, waste, and abuse, recognizing common types and warning signs, reporting suspected cases, and understanding the consequences of non-compliance. This essential course helps healthcare professionals maintain ethical standards and regulatory compliance.

EMTALA Compliance Training Course
$30.00
Ensure your hospital or healthcare facility meets federal regulations with our Emergency Medical Treatment and Labor Act (EMTALA) Compliance Training course for just $30. This comprehensive course equips healthcare professionals with the knowledge and tools necessary to comply EMTALA, ensuring all patients receive essential emergency medical care regardless of their ability to pay. Learn key provisions, documentation requirements, and the importance of policies and staff training to maintain compliance. Enroll now to provide your team with the skills to navigate EMTALA complexities and uphold the highest standards of emergency care.

Business Associate HIPAA Online Course for IT Professionals
$20.00
The Business Associate HIPAA Online Course for IT Professionals provides essential training for IT teams handling protected health information (PHI) in compliance with HIPAA regulations. For $20.00, this course covers the relationship between Business Associates and Covered Entities, responsibilities under the HIPAA Privacy and Security Rules, the HITECH Act requirements, PHI identification, and implementing safeguards. Participants gain practical insights and best practices to ensure HIPAA compliance in their IT operations.

Dental Infection Control Course: Creating a Safe Patient Environment
$20.00
The Dental Infection Control Course: Creating a Safe Patient Environment offers a thorough review of current infection control standards for dental practices for $20.00. Covering topics such as instrument processing and sterilization, the Spaulding classification of instruments, surface disinfection, and CDC guidelines, this 1.0 credit hour course helps participants deepen their understanding of effective sterilization and disinfection techniques to maintain a safe patient environment.

Hurricane Preparedness Course
Free
The Hurricane Preparedness Course is a free resource designed to help you and your staff effectively prepare for the threat of hurricanes. This course provides valuable insights into understanding hurricanes, assessing current readiness, creating a comprehensive survival plan, and following a recovery checklist to ensure safety and resilience. Equip your office and team with the knowledge needed to respond confidently to potential hurricane impacts.

Waste Anesthesia Gases (WAG) Course
$35.00
The Waste Anesthesia Gases Course is available for $35.00 and provides an in-depth look at the management of gases that escape during anesthesia procedures. Participants will learn what

WAGs are, the associated health risks, regulatory guidelines, and risk management strategies. The course covers the implementation of administrative and engineering controls, the use of appropriate personal protective equipment, and emergency procedures for WAG exposure to ensure safety in medical environments.

Our new online courses offer a comprehensive and accessible way for healthcare professionals to stay informed and compliant within the industry. By investing in these courses, healthcare professionals can improve their operational efficiency, uphold ethical practices, and ensure the safety and security of their patients and facilities. These courses are not only a testament to TMC's commitment to excellence in healthcare but also a valuable resource for professionals seeking to enhance their expertise and maintain the trust of their patients and colleagues. Enroll today to take the next step in your professional development and ensure the highest level of care in your practice.

TMC
TOTAL MEDICAL COMPLIANCE

888-862-6742
www.totalmedicalcompliance.com

NOVEMBER 2024

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

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