Major Compliance Concerns for DME
About Your Speaker

Mary Ellen Conway

▪ Nurse, healthcare consultant specializing in post-acute areas of home health, DME, hospice, pharmacy and physician practice

▪ President of Capital Healthcare Group
  • A consulting provider in Bethesda, MD, founded in 2000
  • Helping both large and small providers in managing their audit and regulatory compliance issues
  • Accreditation and state licensure survey issues
The Top Ten Compliance Concerns for DME

- Review the Top Ten Compliance Concerns for DME Suppliers- what they are and how to meet them.
- Items ranked from #10 to #1
- Tips to Consider
- Sample Compliance Scenarios
Issue # 10

- Using the Correct Method to Make/Approve Changes in the Medical Record
  - As you review your medical records for providers, ensure that corrections they make in their handwritten or typed records are done correctly
    - Strike through incorrect documentation
    - Always initialed
    - All corrections are dated
  - CMS will not accept and documentation that does not have corrections performed correctly
  - This applies to your own documentation in a record as well
Issue #9

Maintaining Your Accreditation

- Since 2008, all DME providers who wish to do business with Medicare must be approved by a Medicare-approved accreditation organization.
- Your accreditor communicates directly (weekly) with Palmetto/Novitas to inform them of all of their accredited organizations, the organization's address, PTAN/NPI Number and the products they have been accredited to provide.
  - Before you add any additional products you intend to provide, you must contact your accreditor to see what their requirements are so that they can add this product to your Comprehensive Product List on file with Palmetto/Novitas so that your claims can be processed - otherwise they will be rejected.
  - Working on your renewal before your three-year accreditation renewal/expiration is key to ensuring that this happens well in advance of that renewal/expiration date.
Issue #8

- Updating Your Organizational Chart
  - This is a common problem, that organizations do not keep their Organizational Chart updated.
    - Label your chart with the current month/year when you have reviewed/revised it (each year makes sense) EX: Rev 4/2023 in lower right corner
    - Make sure you identify all employment areas/departments, the reporting structure
    - Start with Leadership and work your way down
    - Use separate charts if you need to which you can show as continuation of each other
    - Include any satellite offices
    - When possible, make it easier on yourself by not including names, just titles
    - Show direct reports as a solid line and indirect reports as a dotted line
Issue #7

- Perform Annual Evaluations
  - Ensure that your evaluations are performed by reviewing the tasks included in that employee’s job description
    - Can be bi-annually if annually is too frequent for a small company
    - Make sure your policy matches
  - Have a place for both the employee and their supervisor to sign and date
  - Can be done at one designated time for all or can be on the employee’s anniversary date
    - Might be easier for a large group to do them on an employee’s anniversary date rather than having a HUGE amount to do at the end of each year
Issue #6

- Complete Your Annual Educational Requirements
  - Review your accreditation standards to ensure that you cover all of the required topics each year. This can be done in a variety of ways:
    - Subscribe to an educational service
    - Offer educational opportunities through your local health department or hospital
    - Offer your own monthly “Lunch and Learn” Program utilizing videos, webinars, local speakers/experts
  - There is not requirement to the manner in which you do this, as long as you offer this to all employees at the owner’s expense.
  - CEU’s for licensure are not included in this requirement
Issue #5

- Complete the Correct I-9 Form and Keep Them Readily Accessible in the Event of an Audit
  - Check the Date on Your I-9 Form. It may have expired
Check the date on your form.

No need to get updated I-9s on staff, but be aware if you do, that you have the reason why you did it.
Issue #4

- Update Your Emergency Plan Annually or As Needed
  - Your Emergency Plan Should be evaluated and tested annually. Read your accreditation standard for what is required in an Emergency Plan to ensure that you have identified all required areas of risk and mitigation.
  - After activating an Emergency Plan (or after annual testing) evaluate what works and what did not work so that updates can be made for the future.
Issue #3

- Remote Workers and PHI
  - In these days of remote working, the opportunity for non-secure PHI is a major concern
    - It used to be that we were concerned about having write-on boards with patient names that anyone could see in the workplace, or protecting our files from cleaning personnel who might come into the office afterhours.
    - Explain to remote employees the requirements for keeping Personal Health Information (PHI) secure
      - Make sure they keep information confidential- away from others in their residence- that their work area is protected (having them provide a picture works)
    - Ensure that the mechanism that you provide for them to work in your system is secure and that all data is encrypted
Issue #2

Maintaining Current Licenses and Licensed Staff

- Maintain YOUR state DME licenses as well as copies of those for your licensed staff
  - Create a management system (excel tracking sheet) where you are proactively monitoring your license renewals and reach out to your state if you have not heard from them 3 months in advance of your expiration/renewal date
    - Especially during the pandemic, some states were VERY behind in getting renewals out in a timely manner
  - For licensed staff (where a license is required to perform their job - EX: Respiratory Therapist) ensure that your licensed staff bring you a copy of their renewed license as the current one is expiring. Place any staff on temporary suspension if they do not comply with their requirement to maintain an active license
Issue #1

Implementing a Federally Mandated Seven-Element Compliance Plan

1. Implement written policies, procedures and standards of conduct
   • Policies and procedures should promote the organization’s commitment to compliance and address specific areas of risk.

2. Designating a Compliance Officer and a Compliance Committee
   • The Compliance Officer is charged with operating and monitoring the Compliance Program. The Compliance Committee should include members of key functions within the organization that can support and advise the Compliance Officer, such as legal, information technology and privacy.

3. Conducting effective training and education
   • All staff receive training on fraud and abuse, regulatory requirements and the compliance program.
Implementing a Federally Mandated Seven-Element Compliance Plan

4. Developing effective lines of communication
   • All employees must feel comfortable reporting internally and there should be multiple reporting avenues such as the Compliance Officer and an anonymous hotline. All reports must be taken seriously and conduct a follow-up with employees, when applicable.

5. Conduct internal monitoring and auditing
   • This involves an ongoing process of evaluation and assessment to deter bad behavior and ensure the effectiveness of education and corrective action(s). The compliance program should also monitor compliance with privacy and provide a risk assessment of potential privacy issues
Issue #1 (continued)

- Implementing a Federally Mandated Seven-Element Compliance Plan

  6. Enforcing standards of conduct through well publicized and disciplinary guidelines.

    - Standards of conduct outline an organization’s rules, responsibilities, proper practices and/or expectations of its employees. Compliance should work with Human Resources to ensure that the standards and consequences for violations are strictly enforced.

  7. Responding promptly to detected offenses and undertaking corrective actions

    - Failure to ensure timely and effective remediation for offenses can create additional exposure for the organization.
Some Common Mistakes Suppliers Have Made

1. Not having a Complete Compliance Program
2. Not naming a Compliance Officer or a Compliance Committee
3. Not having an annual meeting documented
4. Not conducting internal audits---responding to external audits is not the same
5. Not offering employees an anonymous reporting line/mechanism
6. Not being consistent with responses to detected offenses
Steps You Should Take

What Steps Does The Government Expect You To Take When A Compliance Issue Is Identified

▪ A well-designed compliance program will have an efficient and trusted mechanism by which employees can anonymously or confidentially report allegations of a breach of the company’s code of conduct, company policies, or suspected or actual misconduct.
  • Are there proactive measures that create a workspace atmosphere without fear of retaliation?
  • Is the process mapped out to include routing to proper personnel, timely response, as well as appropriate follow up and discipline?
Guidelines for Conducting an Investigation

- Assure records are maintained on compliance investigations
- Participate in negotiation with regulatory agencies
- Assure that overpayments to payers are refunded in a timely manner
- Collaborate with legal counsel regarding voluntary disclosures
- Coordinate investigations to preserve privileges, as applicable
- Facilitate independent investigations when necessary
- Recommend modification of corrective action plans
Common Compliance Concerns

- Signatures of prescribers not matching
- Signatures of client not matching what is on file
- Anonymous reporting line concerns not being forwarded and documented
- Fragmented orientation for new employees--- not being oriented to expectations of compliance
Sample Scenarios

Example #1

Data Breech/Data Ransom

Steps are to be taken to inform all customers that their PHI may have been compromised. Steps include:

- Notifying all patients in writing of the possible breech (printing and mailing)
  - Following up on any undeliverable mail
- 30, 60 and 90 day required tasks
- Putting a statement on the supplier’s website
- Providing a mechanism for customers to ask questions/receive answers about the breech
  - ~90 days
- Offering links to credit reporting services of customer desires
- Reporting the breech to the Office of Civil Rights (when the breech affects more or less than 500 customers)
  - “Safeguards in place...” and “Actions taken in response...”

Retain documentation of everything.
Sample Scenario

▪ Example #2

▪ Sales Person A comes to you to tell you that he has “heard through the grapevine” that Sales Person B is personally signing all of the orders they directly receive.
  • Conduct an investigation
  • Interview ALL staff
  • Apply discipline promptly and completely
  • Assess if there are any refunds that need to be made
  • Make the refunds promptly
Questions?
Thank you
Mary Ellen Conway
Capital Healthcare Group
MaryEllen@CapitalHealthcare Group.com
301-896-0183