CORE BANK

Healthcare Banking Bulletin

Issue 21 - November 20, 2023

Prepare for End of Year

A Five-Part Series: Compliance and Risk Assessments

It's month four of our five-part series preparing for 2024. So far we've covered budgets and fee schedules and insurance reminders. Next month we will cover staff celebrations but before that let's talk about compliance and risk assessments.

The challenge with compliance and risk assessments is that we so often perform them after an incident has occurred when instead we should proactively plan to complete them. The best practice is to perform risk assessments at least annually and doing them prior to your next budget is ideal just in case you turn up anything that requires the management of additional cost.

Month Four: Risk & Compliance

Prevention through planning. That's our goal for compliance and risk assessments, that means looking at the opportunities to assess your organization and proactively creating a strategy to mitigate risks. Some tasks are required to perform annually whereas others

are considered best practice as opposed to mandatory activities.

Foundational Compliance Setup

As a medical practice there are a few essential things to have in place and review annually which are comprehensively reviewed in the Compliance Plan provided by the Office of the Inspector General (OIG) which includes the seven elements of a successful compliance plan.

1. Written Policies & Procedures
2. Compliance Leadership & Oversight
3. Training & Education
4. Effective Lines of Communication with the Compliance Officer and Disclosure Programs
5. Enforcing Standards
6. Risk Assessment, Auditing, and Monitoring
7. Responding to Detected Offenses and Developing Corrective Action Planning

FOLLOW US ON LINKEDIN FOR OUR MONTHLY HEALTHCARE BULLETIN AND WATCH FOR QUARTERLY WEBINAR AND LUNCH & LEARN OPPORTUNITIES
@CORE-BANK | #HEALTHCAREBANKINGBULLETIN | COREBANK.COM/WEBINAR

AUTHORED BY:

Taya Gordon, EMBA, CMPE, CMOM

LinkedIn: https://www.linkedin.com/in/tayamoheiser/

Twitter: https://twitter.com/tayamoheiser

The OIG recently updated their Compliance Plan in November 2023 and includes implementation strategies for practices of different sizes. More information is available here.

Security Risk Assessment

- If you are a covered entity, you are required to perform this assessment every year.
- This requirement is not satisfied merely by having a certified HER.
- Failure to comply can result in fines or loss of incentive payments.
- Outsourcing an SRA is not required, this can be done in-house.
- Relying on the IT support at your EHR vendor to 'have it covered' is insufficient.
- You do not need to fully re-evaluate every section of the SRA every year.
- There are free tools available to help you stay in compliance.

HHS has a great tool to help walk you through your SRA, you can access that tool here.

Other Risk & Compliance Activities

- Penetration (Pen) Testing – this is a simulated attack of your computer system to identify areas of vulnerability for potential attacks.
- PCI Compliance – this is a review and attestation of how you store and protect cardholder data.
- Phishing Testing – this is a safe way to see if your employees will click on dangerous emails.
- Business Associate Audits – this is a review of all business associates to confirm they are all in compliance with your HIPAA and data standard requirements.
- Ransomware simulations – this simulates a ransomware attack so your organization can identify how to proceed in the event you are targeted.
- Evaluate Internal Controls – this is the process of reviewing how money enters and leaves your organization and solving for any potential areas of revenue loss.

The OIG updates their work plan on a monthly basis to identify their primary areas of focus and audit at the moment. At all times the OIG is looking for fraud, waste, and abuse related to the Medicare program. For the above reasons and so many others it is critical that you have and maintain a comprehensive compliance plan.

Call to Action: If you do not have your plan in place or need assistance putting one together reach out to our Healthcare Division for support.

AUTHORED BY:

Taya Gordon, EMBA, CMPE, CMOM

LinkedIn: https://www.linkedin.com/in/tayamoheiser/

Twitter: https://twitter.com/tayamoheiser