RISK MANAGEMENT RESOLUTIONS

LinkedIn Posts by the PRMS Risk Management Team
Donna Vanderpool, MBA, JD
David Cash, JD, LLM
Ann McNary, JD
Justin Pope, JD

Here are 12 easy to implement risk management resolutions you may want to consider in 2017:

PATIENT SAFETY

- When treating patients with suicidal behavior, ensure that an adequate risk assessment is done - and documented. We suggest that you utilize a tool to ensure that nothing is missed. One such tool is the SAFE-T protocol. For an article on treating suicidal patients, click here.

- Even if not legally required to, consider checking the state Prescription Monitoring Program (PMP) before prescribing controlled substances. For an article on PMPs, click here.

- Ensure any lab work you order, such as lithium levels, is done and reviewed by you. Tracking of lab work, or more accurately failing to track, is not an uncommon fact in the lawsuits we see.

TECHNOLOGY

- Before posting anything on social media, even if privately or anonymously, look your post over to see if you would be happy with all of the following seeing it:
  Your patients
  Your employer
  Your employees
  Your licensing board
  And plaintiff's attorney in a malpractice case against you.
  If you have any misgivings about all of the above seeing it, don't post it. For more risk management advice, click here for our primer on social media in psychiatric practice.

- When using an EHR to document a patient visit, try to use free form text as much as possible, especially to document your reasoning behind clinical decisions. Relying solely on checkboxes and pull-down menus tends to make all of your entries look the same. For more information on the safe use of EHRs, click here for our primer.

- When treating patients remotely via telepsychiatry, ensure the technology used is HIPAA-compliant. Specifically, you will need a Business Associate Agreement, under which the vendor promises many things, including to maintain the confidentiality and security of your patients' information. For more information, click here for our telepsychiatry primer.

PRACTICE MANAGEMENT

- Consider developing a contingency plan to assist others in closing your practice and finding care for patients in the event of your sudden death or incapacity. For our article discussing contingency planning, click here.

- Consider implementing formal office policies on such topics as fees for missed appointments, prescription refills, and after hours coverage to better manage patient expectations and make your office run more smoothly. You can find sample office policies in this article.

- For those patients who have seemingly dropped out of treatment, consider following up with them, and if they are no longer interested in treatment, formally terminate the treatment relationship by sending a letter. For more information on this, and model termination letters, click here.

DATA PROTECTION

- Educate office staff on the importance of protecting patient information and discuss any obligations your practice may have under HIPAA. The government's online training resources, specifically a patient privacy course and privacy and security training games, may be helpful tools when training staff on a yearly basis. Also, consider having office staff sign a confidentiality agreement which acknowledges their obligation to maintain the privacy of patient information. Such an agreement can be reviewed with employees during annual training. A model employee confidentiality agreement may be found here.

- Avoid having patient information on portable devices. If patient information must be on a portable device, the information should be appropriately encrypted - consistent with the National Institute of Standards and Technology (NIST) guidance, using the Advanced Encryption Standard (AES). With appropriate encryption, in the event of a breach, the "safe harbor" would apply, meaning patients would not have to be notified.

- Regularly assess your practice for new threats to protected health information and address vulnerabilities. Have you determined what type of PHI you store and the manner in which you store it? Do you know who has access to your PHI? These are two questions that would likely need to be addressed in a thorough risk assessment. The U.S. Department of Health and Human Services has provided guidance on risk analysis and offers a security risk assessment tool.

PRMS
Manager of The Psychiatrists' Program
Medical Professional Liability Insurance for Psychiatrists
1-800-245-3333
Email: TheProgram@prms.com
Visit: PsychProgram.com
Twitter: @PsychProgram