Health Information Compliance Alert

Pocket This Expert Advice for 2020 HIPAA Planning

Tip: Ensure your BAs and vendors know the HIPAA rules, too.

Just because your organization considers HIPAA compliance a top priority doesn't mean that you're not privy to a breach. That's why monthly audits and annual planning are essential to reevaluate where your risks are - and how to fix them.

Reminder: Some entities violate HIPAA because they don't fully understand the nuances of the Privacy, Security, and Breach Notification rules while others fail to emphasize the significance of the regulations to their staff. You can prevent both accidents and careless breaches by staying on top of HIPAA compliance.

As you prepare and update your HIPAA policies and procedures for 2020, you may want to review recent assessments and see where you're failing. Experts agree that most practices may need outside help to deal with data security and incident response.

For example, you may want to hire a health IT expert to review your networks and systems. "Most organizations cannot meet the standards of the HIPAA Security Rule for a risk analysis without help from a third party that specializes in performing risk analyses,” acknowledges **Jen Stone, MSCIS, CISSP, QSA,** a security analyst with **Security Metrics** in Orem, Utah. "Risk analysis is not a skill set you can reasonably expect your IT team to have.”

Incident response and breach management continue to plague organizations big and small, requiring professional insight from legal help to forensic investigators.

"My top advice for small providers dealing with a breach is to isolate the problem as quickly as possible and get the right support system in place to help guide them through the process, including attorneys, technical folks - depending on the type of breach,” advises attorney and shareholder, **Danielle L. Dietrich,** with **Tucker Arensburg** in Pittsburgh.

Consider adding these five steps from Dietrich to your compliance checklist:

1. Cultivate compliance. "Build a culture of compliance from the top down - from the CEO to the lowest person in the organization. If employees don't see their leaders taking these matters seriously, they are less likely to take it seriously themselves,” Dietrich counsels.

2. Outline and impose consequences for wrongdoers. "Have defined policies and penalties for breaking those policies. Enforce those penalties - if you don't enforce, the policies aren't worth anything,” she maintains.

3. Set up an incident response plan. "Have an initial response plan in place, so that there are no questions or hesitation of what to do when a problem is discovered,” urges Dietrich.

4. Scrutinize your associates and vendors. "Make sure that your vendors are also compliant - especially IT and anyone that touches patient information in any way. Ask for detailed information about their policies. Your contracts should include an indemnity clause in case that vendor is responsible for a breach,” she exhorts.

5. Educate staff on HIPAA from the get-go. "Have ongoing training and compliance and make such training a significant part of your on-boarding process with new employees,” Dietrich says.

Bottom line: While you may not think that HIPAA or data security are your responsibility, remember that an organization is only as secure as its least informed or most careless person.