Health Information Compliance Alert

Compliance: Consider 7 Expert Tips to Enhance 2020 HIPAA Planning

Tip: Don't brush violations under the rug - deal with them in real time.

Whether your organization aces HIPAA compliance on the daily or struggles to keep patient privacy under wraps, there is always room for improvement. Moreover, lax procedures often lead to complacency - and before you know it, your practice may need more than just an audit to rectify its issues.

As you revisit policies and procedures and outline your 2020 HIPAA program, take advantage of those internal audits done on a regular basis to maintain and encourage compliance, suggests attorney **Lauren M. Ramos**, with **McGuireWoods LLP** in Richmond, Virginia.

Add these seven top tips from Ramos to your HIPAA checklist:

1. Monitor practice HIPAA protocols and procedures.

Many violations are a result of neglect somewhere in the compliance checklist, and that's why it's crucial to keep on top of issues. "Conduct ongoing monitoring of HIPAA compliance on an entity-wide basis," Ramos advises.

2. Don't skimp on risk assessments.

"Ensure compliance with the HIPAA Security Rule, including conducting security risk assessments on a routine basis," she maintains. Plus, if the **HHS Office for Civil Rights** (OCR) sees that your organization has a steady - and well-documented - track record of assessing, analyzing, and managing risks, it's more likely to work with you to minimize the breach penalties.

3. Consult a compliance expert.

"Providers who do not have the capacity to conduct their own risk assessment can hire one of many expert consultants to conduct the risk assessment for them," counsels Ramos. And remember, smaller practices may feel like they don't have the budget to seek HIPAA help, but the financial and professional costs of a breach often far outweigh the minimal fees of engaging a compliance expert.

4. Address and attend violations promptly.

"If you experience a breach, follow all breach requirements and protocols on a short timeline," Ramos warns. "Do not sit on a suspected breach."

Remember that a covered entity (CE) must notify impacted individuals without "unreasonable delay" no later than 60 days after the "discovery" of the breach, OCR guidance reminds.

5. Update policies accordingly.

It's a great idea to do a monthly check-up and an annual audit of your policies and procedures, but it is especially critical to address your organization's shortcomings after an incident. "Review your HIPAA compliance program anytime a breach or suspected breach occurs," says Ramos.

6. Enforce strict social media rules.

It can be particularly troublesome for practices to successfully navigate the various social media platforms without sinking the proverbial ship. CEs that plan to utilize Twitter or Facebook to promote their businesses must use caution and keep HIPAA in mind before posting online.

"Have a strict social media policy and make sure employees are aware of it. Often when breaches involve social media, the person disclosing the information did not realize that it constituted protected health information [PHI]," she instructs.

7. Train staff on HIPAA.

Educating your staff on the nuances of HIPAA is not only essential to protect your patients and business, but it's required under the Privacy Rule. "Employee training is critical. In addition to comprehensive training required by HIPAA, making sure employees consistently know their resources and first points of contact goes a long way," explains Ramos.

She continues, "Employees should know who the privacy officer is with a direct line of access and be encouraged to ask questions or report anything unusual. An open, ongoing discussion about HIPAA compliance makes it more likely that employees will catch any issues."