FIVE THINGS EVERY DOCTOR SHOULD KNOW ABOUT HEALTH CARE LAW

Thomas S. Dean, Esq. [1]

Legal issues are intruding into physician practices much more since the March 2010 passage of the Affordable Care Act. Electronic health records or "EHRs" have replaced paper medical charts for almost all practices. With EHRs come some convenience and potential increased payments, but also governmental audits, heightened compliance duties, and new liabilities.

An EHR does reduce paper around the office and allow rapid searching for specific information. For those record systems that comply with the "Meaningful Use" rule, Medicare has paid some providers a modest sum to adopt and maintain them. However, they come with strings attached. Here are five things every doctor should know about the current state of Health Care Law:

1. The government has hired Figliozzi and Company, a private contractor, to audit your use of the EHR. If you claimed Meaningful Use payment, you may be audited for effectively following the rules. If your practice fails to respond to the audit fully, you may be required to repay all the funds you received for installing an EHR. It is therefore important to respond to the audit in a full and timely manner, and to be ready to appeal if the first response is unfavorable.

2. Your EHR probably makes you a "Covered Entity" under the Health insurance Portability and Accountability Act ("HIPAA"). HIPAA's Privacy Rule generally applies to clinical providers who file their bills electronically. You have probably always maintained patient confidentiality, but now the Office of Civil Rights ("OCR") will be looking over your shoulder.

The OCR supervises compliance with the Privacy Rule. If a patient complains that their privacy was violated, you will likely hear from the OCR. Reduce your risk as much as possible by completely destroying any paper records, and not store patient information on "jump drives" or other portable memory devices, which can fall into the wrong hands.

3. The Security Rule also applies to Covered Entities under HIPAA. You must perform a periodic Security Risk Assessment, to ensure you protect your patients' information with adequate safeguards: physical (locks and alarms on the practice building), technical (passwords and encryption on computers that store patient information) and administrative (educate your staff on their duties). If you are not performing an annual SRA, start now.

4. You must have a formal Compliance Program in place. Every practice that takes Medicare or Medicaid patients is required to identify a Compliance Officer, and that officer is responsible for maintaining a seven-part compliance program in accordance with federal guidance. If you do not have a program in place yet, it is very important to create one immediately.

---

[1] Thomas S. Dean is an attorney in the Miller Stratvert P.A. Albuquerque office

5. Make a plan for transferring your records when you leave practice. You are required to have such a plan. If anything happens to you, it will impose a legal risk on your heirs to have to handle your old records without the mandatory plan in place.

While these rules may seem daunting, the Centers for Medicare and Medicaid Services publish a number of online resources to help you comply with your obligations. A simple Google search will lead you to basic guidance on all of the topics above. And of course, there is professional help available if your practice finds one of these issues becoming problematic.