CARLTON FIELDS

HIPAA Compliance for Work-From-Home or Telehealth Programs: Five Frequently Overlooked Considerations

CORONAVIRUS | CYBERSECURITY AND PRIVACY | HEALTH CARE | JUNE 15, 2020

Patricia S. Calhoun

Patricia M. Carreiro

COVID-19 has challenged health care providers to change the way they offer services — from shifting to an increasingly remote workforce to diving into telehealth. These adjustments have privacy implications. The following are five of the most commonly overlooked steps that providers should take to remain compliant with applicable privacy laws.

1. **Complete a new HIPAA risk analysis.**

   HIPAA requires providers to perform periodic technical and nontechnical evaluations in response to environmental or operational changes affecting the security of electronic protected health information (ePHI), as appropriate, to ensure the continuing security of that information. In light of providers' rapid transition to employees working from home and the offering of telehealth services, a new HIPAA risk analysis (and documentation of that analysis) may be necessary. As an initial question, providers need to ask themselves, "Where is the ePHI within my organization?" If the answer shows that ePHI is now frequently found outside the protected realm of the provider's existing HIPAA policies, it indicates the need to complete a full risk analysis.

2. **Revise your policies accordingly.**

   Changes to the way your practice operates almost certainly mean that revisions to policies are required to ensure that you have sufficient physical, technical, operational, and administrative policies in place to meet HIPAA's standards for your work-from-home employees and/or telehealth offerings. For some cybersecurity considerations to keep in mind, see our earlier alerts here and here. Given hackers' current increased focus on targeting health care providers, incident response plans are likely one of the most urgent policy updates for any provider.

3. **Test your contingency plans.**

   In addition to updating their policies, and also in light of hackers' recent focus, providers should test their newly revised incident response and other contingency plans. This is one HIPAA requirement that may actually save money for providers. According to the Ponemon Institute, companies that have and extensively test their incident response plans save more than $1 million in costs after a breach.

4. **Adjust your privacy notices and consents.**

   Make sure your privacy notices and consents accurately reflect any new methods of data collection, use, storage, and sharing. Also, if you've started using new vendors or technologies, you may be required to include certain disclosures in your privacy policy. Be sure to review the applicable contract and terms of use, and include any required disclosures in your privacy notices and consents.

5. **Make sure your contracts are compliant with applicable privacy laws.**

   If new contracts were executed to support the rapid shift to remote work and telehealth programs, make sure you have

required business associate agreements in place. While the Office for Civil Rights has temporarily relieved providers of the need to have such an agreement with some telehealth service providers, there was no such exemption made for work-from-home arrangements. Even with telehealth, having a business associate agreement in place is still wise for several reasons, from litigation risk to facilitating post-COVID HIPAA compliance. In addition, providers subject to the California Consumer Privacy Act (CCPA) and hoping to portray their new relationship as a “service provider” relationship, rather than a “sale,” should verify that their contracts for information outside the CCPA’s partial HIPAA exception include the required restrictions and certifications.