CARLTON FIELDS

Five Steps to Prepare for Telehealth Data Breach Litigation

CORONAVIRUS | CYBERSECURITY AND PRIVACY | HEALTH CARE | MAY 4, 2020

Patricia S. Calhoun

Patricia M. Carreiro

As we've previously reported, COVID-19 has caused a surge in telehealth and has temporarily reduced the HIPAA Security Rule requirements placed on telehealth service providers. These relaxed Security Rule requirements, while helpful for providers scrambling to provide urgent care and patients needing such care, increase the risk of cybersecurity breaches. When the breaches happen, litigation is sure to follow, so here are five tips to position yourself for a more favorable litigation outcome.

1. **Avoid the Breach**

   Breaches always have costs, not the least of which include reputational costs and lost business. Don't let the temporary relaxing of HIPAA Security Rules lull you into settling for second-rate technology vendors. Even if you comply with HHS' current relaxed requirements, state laws can still be more stringent and patients may still sue you if their information is compromised. Accordingly, use a HIPAA-compliant telehealth service provider who agrees to sign a business associate agreement. For additional guidance on particular cybersecurity steps to follow, see here.

2. **Monitor and Prepare for the Breach**

   The longer a breach goes undetected, the greater the costs of cleaning it up. Make sure you have a process in place to monitor access to patients' PHI. Monitoring is particularly important in the health care context, where breaches resulting from intentional bad actors are more common. Beyond that, know what to do if a breach occurs by having an incident response plan in place. 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.

3. **Make a Paper Trail**

   Document your privacy and cybersecurity efforts, including facts and data sufficient to support the decisions. This should include a description of any reasonable equivalent alternative measures undertaken. Periodically review your documentation and update as needed in response to changes to your environment or operations. Maintain records of all risk assessments and of investigations into any prior security incidents. Consider the involvement of counsel so that any documentation, not otherwise required under HIPAA, may be protected by the attorney-client privilege.

4. **Be Mindful of Your Representations**

   When it comes to privacy and cybersecurity, as with anything else, know what you are promising and follow through on it, or you could face claims ranging from negligent misrepresentation to breach of contract or fraud. Always inform patients of the risks and get their consent to proceed.

5. **Involve Subject Matter Experts**

   If you have cyber insurance, notify your broker or carrier so that you can seek to maximize coverage and obtain the benefits of any preferred vendor lists maintained by the carrier. Those vendors could include forensic and incident response firms. Before working with those firms, obtain your carrier's approval and have your outside counsel retain the forensic firm so as to protect their work under the privilege.

©2020 Carlton Fields, P.A. Carlton Fields practices law in California through Carlton Fields, LLP. Carlton Fields publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information and educational purposes only, and should not be relied on as if it were advice about a particular fact situation. The distribution of this publication is not intended to

create, and receipt of it does not constitute, an attorney-client relationship with Carlton Fields. This publication may not be quoted or referred to in any other publication or proceeding without the prior written consent of the firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our Contact Us form via the link below. The views set forth herein are the personal views of the author and do not necessarily reflect those of the firm. This site may contain hypertext links to information created and maintained by other entities. Carlton Fields does not control or guarantee the accuracy or completeness of this outside information, nor is the inclusion of a link to be intended as an endorsement of those outside sites.