Does Private Internet Access Comply With HIPAA?

Travis - 2021-03-15 - Frequently Asked Questions

No, Private Internet Access is not HIPAA compliant.

The Health Insurance Portability and Accountability Act of 1996 (**HIPAA;** Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996) was enacted by the United States Congress and signed by President Bill Clinton in 1996.

If you collect, process, store or transmit health information (PHI) including medical records, you will need to pass an audit to meet HIPAA compliance. As such certain technologies and procedures are recommended for people who deal with PHI, even if they're not explicitly stated in HIPAA standards.

The rules and regulations in the Code of Federal Regulations (CFR) that pertain to HIPAA dictate that Online Tech, as a business that deals with clients' PHI, must:

1. Protect the availability, integrity, and confidentiality of PHI
2. Have Business Associate Agreements (BAAs) with clients who have PHI
3. Report any violations of PHI misuse to the OCR (the Office of Civil Rights that audits, fines, and charges companies and individuals for HIPAA violations).

However HIPAA guidelines regarding data retention state that the logs (access/activity) and protected health information documentation proving that the covered entity is adhering to the HIPAA Security Rule are retained for six years. This regulation mandates that records are to be retained for essentially any interaction with patient PHI and personally identifiable information (PII), which is covered under HIPAA.

In the event that a breach has occurred or is alleged to have occurred, it is important to be able to prove that the Security Rule and the other facets of HIPAA have been followed. HIPAA requires that internal audits of this data are performed regularly. Furthermore, in the event that a breach has occurred, it is required by HIPAA laws that the covered entity be able to produce this information when subpoenaed. As Private Internet Access does not log, we cannot provide the required information if subpoenaed by HIPAA laws.

And this, in summary, is why Private Internet Access cannot comply with HIPAA requirements and as such cannot provide VPN for HIPAA services.

Tags

HIPAA