Notice of HIPAA Privacy Breach

Cerebral, Inc. is issuing a notice about a recently discovered issue related to inadvertent information sharing and the steps Cerebral has taken to address it. This notice was drafted in accordance with HIPAA disclosure requirements.

What Happened? Like others in many industries, including health systems, traditional brick and mortar providers, and other telehealth companies, Cerebral has used what are called "pixels" and similar common technologies ("Tracking Technologies"), such as those made available by Google, Meta (Facebook), TikTok, and other third parties ("Third-Party Platforms"), on Cerebral's Platforms. Cerebral has used Tracking Technologies since beginning operations on October 12, 2019. Cerebral recently initiated a review of its use of Tracking Technologies and data sharing practices involving Subcontractors. On January 3, 2023, Cerebral determined that it had disclosed certain information that may be regulated as protected health information ("PHI") under HIPAA to certain Third-Party Platforms and some Subcontractors without having obtained HIPAA-required assurances.

What Information Was Disclosed? The information disclosed varied depending on what actions individuals took on Cerebral's Platforms, the nature of the services provided by the Subcontractors, the configuration of Tracking Technologies when the individual used our services, the data capture configurations of the Third-Party Platforms, how individuals configured their devices and browser, and other factors.

- If an individual created a Cerebral account, the information disclosed may have included name, phone number, email address, date of birth, IP address, Cerebral client ID number, and other demographic or information.
- If, in addition to creating a Cerebral account, an individual also completed any portion of Cerebral's online mental health self-assessment, the information disclosed may also have included the service the individual selected, assessment responses, and certain associated health information.
- If, in addition to creating a Cerebral account and completing Cerebral's online mental health self-assessment, an individual also purchased a subscription plan from Cerebral, the information disclosed may also have included subscription plan type, appointment dates and other booking information, treatment, and other clinical information, health insurance/ pharmacy benefit information (for example, plan name and group/ member numbers), and insurance co-pay amount.

Out of an abundance of caution, we are notifying anyone who fell into any of these categories, even if they did not become a Cerebral patient or provide any information beyond what was

necessary to create a Cerebral account. No matter how an individual interacted with Cerebral's Platforms, the disclosed information did not include Social Security number, credit card information, or bank account information.

What We've Done and Are Doing. Upon learning of this issue, Cerebral promptly disabled, reconfigured, and/or removed the Tracking Technologies on Cerebral's Platforms to prevent any such disclosures in the future and discontinued or disabled data sharing with any Subcontractors not able to meet all HIPAA requirements. In addition, we have enhanced our information security practices and technology vetting processes to further mitigate the risk of sharing such information in the future.

What Affected Individuals Can Do. We are not aware of any misuse of PHI arising from this incident. However, individuals can prevent the use of Tracking Technologies by blocking or deleting cookies or using browsers that support privacy-protecting operations, such as "incognito" mode. Individuals can also adjust privacy settings in Facebook, Google, and other platforms. Individuals may also wish to change their Cerebral user account password (and the use of that password for any other site if used a common password). It is also a best practice to monitor explanation of benefits, insurance member portal and other communications from health insurance providers to confirm that all charges are appropriate. Out of an abundance of caution, we are providing free credit monitoring and encourage individuals to remain vigilant against incidents of identity theft and fraud and review their account statements. Affected individuals are being provided with instructions to take advantage of the free credit monitoring and additional guidance to help them protect their information.

For More Information. Contact us at 800.785.8435 (toll-free) Monday through Friday from 8 am to 10 pm Central, or Saturday and Sunday from 10 am to 7 pm Central (excluding major U.S. holidays).