Cerebral

2093 Philadelphia Pike #9898
Claymont, DE 19703

March 1, 2023

[Patient First] [Patient Last]
[Patient Street Address 1]
[Patient Street Address 2]
[Patient City], [Patient State] [Patient Zip Code]

Dear [Patient First] [Patient Last]:

Cerebral Inc. ("Cerebral")[1] takes your privacy seriously. We write to provide transparency regarding Cerebral's prior data sharing practices via Tracking Technologies (as defined below) on portions of its websites and mobile applications ("Cerebral's Platforms") and with certain subcontractors and other service providers ("Subcontractors").

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.[2] Cerebral has used Tracking Technologies since we began 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 you took on Cerebral's Platforms, the nature of the services provided by the Subcontractors, the configuration of Tracking Technologies when you used our services, the data capture configurations of the Third Party Platforms, how you configured your device and browser, and other factors.

- If you created a Cerebral account, the information disclosed may have included your 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, you also completed any portion of Cerebral's online mental health self-assessment, the information disclosed may also have included your selected service, assessment responses, and certain associated health information.
- If, in addition to creating a Cerebral account and completing Cerebral's online mental health self-assessment, you 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 you interacted with Cerebral's Platforms, the disclosed information did not include your Social Security number, credit

[1] References to "Cerebral" herein also include Cerebral Inc.'s contractually affiliated medical groups.

[2] A pixel is a snippet of computer code installed into a website or mobile application to help understand user activity by collecting specific pieces of data. This code can be used to track activity to help with website optimization, identifying trends, and improving the user experience.

.

Cerebral

2093 Philadelphia Pike #9898
Claymont, DE 19703

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 similar incidents in the future.

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

For More Information. We regret that this incident occurred and any concern it may cause you. If you have any questions regarding this incident, or if you would like additional information regarding what you should do as a result, please do not hesitate to 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). Be prepared to provide your engagement number [B########]

Sincerely,

David Mou, M.D., M.B.A.
Chief Executive Officer
Cerebral

Cerebral

2093 Philadelphia Pike #9898
Claymont, DE 19703

GENERAL INFORMATION ABOUT IDENTITY THEFT PROTECTION

To help protect your identity, we are offering complimentary access to Experian IdentityWorks SM for twelve (12) months. If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for twelve (12) months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary twelve-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you enroll by [Enrollment End Date] (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: [Enrollment URL]
- Provide your activation code: [Activation Code]

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [Experian TFN] by [Enrollment End Date]. Be prepared to provide engagement number [B######] as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- Experian credit report at signup: See what information is associated with your credit file. Daily credit reports are available for online members only.*
- Credit Monitoring: Actively monitors Experian file for indicators of fraud.
- Identity Restoration: Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- Experian IdentityWorks ExtendCARE TM : You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- $1 Million Identity Theft Insurance**: Provides coverage for certain costs and unauthorized electronic fund transfers.

You should remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

* Offline members will be eligible to call for additional reports quarterly after enrolling.
** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Cerebral

2093 Philadelphia Pike #9898
Claymont, DE 19703

You should remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

Credit Reports. Under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling 1-877-322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. **You may contact the nationwide credit reporting agencies at:**

Equifax	Experian	TransUnion
P.O. Box 105788 Atlanta, GA 30348 www.equifax.com 1-800-525-6285	P.O. Box 9554 Allen, TX 75013 www.experian.com 1-888-397-3742	P.O. Box 2000 Chester, PA 19016 www.transunion.com 1-800-680-7289

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Place a Security Freeze on your Credit Report. You also have the right to place a security freeze on your credit report by contacting any of the credit bureaus listed at above. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line or a written request. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. You can place a freeze and lift a security freeze on your credit report free of charge.

You may contact the Federal Trade Commission (FTC) and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should contact the FTC and/or your state's attorney general office for information on how to prevent or avoid identity theft. You can contact the FTC at: **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20508, www.ftc.gov, 1-877-IDTHEFT (438-4338).

For District of Columbia Residents: District of Columbia Office of the Attorney General, 400 6th St. NW, Washington, DC 20001, https://oag.dc.gov, (202) 727-3400.
For Iowa Residents: State law advises you to report any suspected identity theft to law enforcement or to the Iowa Attorney General, Consumer Protection Division, 1305 E. Walnut St., Des Moines, IA 50319, 1-888-777-4590.
For Maryland Residents: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.
For Massachusetts Residents: You have the right to obtain a police report if you are the victim of identity theft.
For New Mexico Residents: You have certain rights pursuant to the federal Fair Credit Reporting Act (FCRA). For more information about the FCRA, please visit www.ftc.gov.
For New York Residents: the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.
For North Carolina Residents: North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.com, 1-877-566-7226.

Cerebral

2093 Philadelphia Pike #9898
Claymont, DE 19703

For Rhode Island Residents: the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 6,257 Rhode Island residents impacted by this incident.