Mental Health PARTNERS

Healthy minds, healthy lives, healthy communities

To Enroll, Please Call:
(833) 573-0856
Or Visit:
https://ide.myidcare.com/mhpprotect
Enrollment Code: <<XXXXXXX>>

C/O ID Experts
P.O. Box 1907
Suwanee, GA 30024

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

August 21, 2020

Subject: Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>:

I am writing to inform you of a data security incident that may have affected your personal information. At Mental Health Partners ("MHP"), we take the privacy and security of your personal information very seriously and regret any concern that this incident may cause you. That is why we are contacting you and informing you about steps you can take to protect your information and resources that are available to assist you.

What Happened? In late March of 2020, we learned of unusual activity involving an MHP employee's email account. Upon discovering this activity, we immediately began an investigation and took steps to secure all MHP employee email accounts. We also engaged an independent computer forensics firm to determine what happened and whether personal information had been accessed or acquired without authorization. As a result of this investigation, after receiving confirmation that six employee email accounts had been accessed without authorization, we learned on July 22, 2020 that some of your personal information was contained within an impacted email account. We then took steps to identify current mailing addresses so that we could notify potentially impacted individuals.

Please note that this unauthorized access was limited to information transmitted via email and did not affect any other information systems. In addition, we are not aware of the misuse of any potentially impacted information.

What Information Was Involved? The affected information may have included your name, <<Variable Text>> <<Variable Text2>>.

What Are We Doing? As soon as we discovered this incident, we took the steps described above. We have also implemented additional safeguards to help ensure the security of our email environment and to reduce the risk of a similar incident occurring in the future. These safeguards include implementing multi-factor authentication, installing additional firewalls and cybersecurity scanning appliances, and restricting network communications. In addition, we are providing you with information about steps that you can take to help protect your personal information and, out of an abundance of caution, we are offering you credit monitoring and identity theft restoration services at no cost to you through ID Experts®, a leader in risk mitigation and response. These services include credit and CyberScan™ monitoring, a $1,000,000 insurance reimbursement policy, exclusive educational materials, and fully managed identity theft recovery services. With this protection, ID Experts® will help you to resolve issues if your identity is compromised.

To receive the MyIDCare™ services, you must be over the age of 18, have established credit in the United States, have a Social Security number issued in your name, and have a United States residential address associated with your credit file. Please note that the deadline to enroll in the MyIDCare™ services is November 21, 2020.

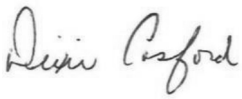
What Can You Do? We recommend that you review the guidance included with this letter about how to help protect your information. You can also contact ID Experts® with any questions and to enroll in the free MyIDCare™ services by calling (833) 573-0856 or going to https://ide.myidcare.com/mhpprotect and using the Enrollment Code provided above. MyIDCare™ representatives are available to assist you Monday through Friday from 7:00 am – 7:00 pm Mountain Standard Time.

We encourage you to take full advantage of this service offering. ID Experts® representatives are fully versed on the incident and can answer questions or respond to concerns you may have. More information is enclosed with this letter.

For More Information: Further information about how to help protect your personal information appears on the following page. If you have questions or need assistance, please call (833) 573-0856, Monday through Friday from 7:00 am – 7:00 pm Mountain Standard Time.

We take your trust in us and this matter very seriously. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,



Dixie Casford, MBA, LPC
Co-Chief Executive Officer
Mental Health Partners

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant and review your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can also contact one of the following three national credit reporting agencies:

Equifax	**Experian**	**TransUnion**	**Free Annual Report**
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000	P.O. Box 105281
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-800-525-6285	1-888-397-3742	1-877-322-8228	1-877-322-8228
www.equifax.com	www.experian.com	www.transunion.com	www.annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. There is no charge to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Contact information for the FTC is: **Federal Trade Commission**, 600 Pennsylvania Ave, NW, Washington, DC 20580, www.consumer.ftc.gov or www.ftc.gov/idtheft, 1-877-438-4338. Residents of New York, Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

New York Attorney General	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
Bureau of Internet and Technology Resources	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
28 Liberty Street	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
New York, NY 10005	oag.state.md.us	ncdoj.gov	http://www.riag.ri.gov
ifraud@ag.ny.gov	1-888-743-0023	1-877-566-7226	401-274-4400
1-212-416-8433			

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

Personal Information of a Minor: You can request that each of the three national credit reporting agencies perform a manual search for a minor's Social Security number to determine if there is an associated credit report. Copies of identifying information for the minor and parent/guardian may be required, including birth or adoption certificate, Social Security card and government issued identification card. If a credit report exists, you should request a copy of the report and immediately report any fraudulent accounts to the credit reporting agency. You can also report any misuse of a minor's information to the FTC at https://www.identitytheft.gov/. For more information about Child Identity Theft and instructions for requesting a manual Social Security number search, visit the FTC website: https://www.consumer.ftc.gov/articles/0040-child-identity-theft. Contact information for the three national credit reporting agencies may be found below.

MyIDCare™

Recommended Steps to help Protect your Information

1. **Website and Enrollment.** Go to https://app.myidcare.com/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your MyIDCare™ membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare™ will be able to assist you.

3. Telephone. Contact MyIDCare™ at (833) 573-0856 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so you receive a free report from one of the three bureaus every four months.

If you discover any suspicious items and have enrolled in MyIDCare™, notify them immediately by calling or by logging into the MyIDCare™ website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.