ID Experts
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

To Enroll, Please Call:
(833) 719-0129
Or Visit:
https://ide.myidcare.com/sbhg
Enrollment Code: <<XXXXXXX>>

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

<<Date>>

NOTICE OF DATA BREACH

Dear <<First Name>> <<Last Name>>,

Sunshine Behavioral Health Group, LLC ("Sunshine") is writing to notify you of an event that may have affected the security of some of your protected health information. Sunshine provides business services to several health care providers, including Monarch Shores, Chapters Capistrano, Willow Springs Recovery and Mountain Springs. This letter provides details of the incident, our response, and resources available to you. We are not aware of any malicious misuse of your protected health information, but we are notifying you out of an abundance of caution so you can take steps to help safeguard your protected health information, should you feel it is appropriate to do so.

What Happened?

On September 4, 2019, Sunshine became aware that a cloud-based system used to store certain patient records on behalf of the above health care providers was inadvertently set-up in such a manner that permitted the records to be made available on the Internet. Sunshine immediately took steps to change the settings, and, on November 14, 2019, took additional actions to remove the records from general Internet access. Sunshine confirmed that patient protected health information was affected by the incident, and began an investigation to identify the patients and types of protected health information involved. Through our investigation, on December 23, 2019, we learned that some protected health information related to you was stored in the affected system.

What Information Was Involved?

Our ongoing investigation confirmed the protected health information present in the impacted storage folder may have included your credit or debit card number, as well as the expiration date and/or security code; clinical information, such as diagnosis, medical conditions, treatment information, lab results, and medication information; demographic information, such as your name, address, date of birth, email address, and telephone number; health insurance and claims information; account balance information; and an electronic or digital signature.

What We Are Doing.

Upon learning of this incident, we immediately took steps to address the incident and confirm the security of our systems. We modified access controls for the affected system and reviewed our company policies and procedures relating to the security and privacy of patient records. We are also notifying affected individuals, including you, so that you may take further steps to best safeguard your protected health information, should you feel it is appropriate to do so. To that end, we are working with ID Experts to offer MyIDCare protection for 24 months at no cost to you. MyIDCare protection is explained in more detail below.

What You Can Do.

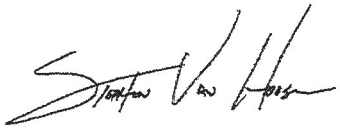
You may review the information contained in the attached document titled "Recommended Steps to Help Protect Your Information." We also encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling (833) 719-0129 or going to https://ide.myidcare.com/sbhg and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 9:00 a.m. to 9:00 p.m., EST. Please note that the deadline to enroll is April 24, 2020. We encourage you to take full advantage of this service offering.

For More Information.

We recognize that you may have questions not addressed in this letter. If so, we encourage you to call our dedicated assistance line at (833) 719-0129 (toll free), Monday through Friday, 9:00 a.m. to 9:00 p.m., EST.

For more detailed instructions on signing up for the MyIDCare protection, please review the attached "Recommended Steps to Help Protect Your Information" document. Note that you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this document. Please call (833) 719-0129 or go to https://ide.myidcare.com/sbhg for assistance or for any additional questions you may have regarding MyIDCare.

Sincerely,



Stephen Van Hooser
Director of Compliance

(Enclosure)

MyIDCare

Recommended Steps to Help Protect Your Information

1. Website and Enrollment. Go to https://ide.myidcare.com/sbhg 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) 719-0129 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

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

You should also know that you have the right to file a police report if you ever experience identity theft. 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.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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 it may also delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order credit reports from all three bureaus, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files. In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning the identity theft.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118, Frankfort, KY 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing to the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, Telephone: 401-274-4400.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.