



2_0000165



[REDACTED]



December 23, 2025

Re: Notice of Data Breach

Dear [REDACTED]:

Sunspire Health Florida, LLC d/b/a White Sands Treatment Center takes privacy and security very seriously. As part of that commitment, we are writing to notify you of a data privacy incident involving your personal information. This notice explains the incident, our response, and steps you can take to help protect your personal information.

What Happened: On July 8, 2025, we became aware that a former employee of White Sands may have taken patient information without authorization. Upon discovery, we took immediate action to conduct an investigation into the incident to determine what, if any, unauthorized activity occurred. After a thorough investigation, on August 4, 2025, it was determined that on April 1, 2025, just prior to her last day of employment, the former employee stole a file containing patient information, limited to names, contact information, and admission and/or discharge dates.

What Information Was Involved: Our review of the files determined your first and last name, in combination with your address, phone number, email address, and admission and/or discharge date, were present within the file.

What We Are Doing: Upon learning of this incident, we took immediate steps to mitigate the risk of similar incident occurring in the future, including implementing enhanced security protocols and safeguards as well as revised our policies and provided internal trainings.

What You Can Do: To date, we are not aware of any reports of identify fraud as a result of the information impacted by this incident. However, it is always prudent for patients to review health care statements for accuracy and report to your provider or insurance carrier any services or charges that were not incurred. Additionally, there are further steps and protections that individuals can take (see enclosure), including those recommended by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For More Information: If you have any questions or concerns, please contact our dedicated assistance line at 1-833-[REDACTED], Monday through Friday, 8:00 a.m. to 8:00 p.m. EST, excluding major U.S. holidays. Please know that the security of information is of the utmost importance to us. We remain committed to protecting the information entrusted in our care. We continue to be thankful for your support during this time.

Sincerely,

Sunspire Health Florida, LLC d/b/a White Sands Treatment Center

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts and Credit Reports: It is good practice to remain vigilant of incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-██████. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

Fraud Alert Services: You have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

Credit Freeze Instructions: As an alternative to a fraud alert, you have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit.

Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you should provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver’s license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1- 800-916-8800 www.transunion.com TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000 TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Experian 1-888-397-3742 www.experian.com Experian Fraud Alert P.O. Box 9554 Allen, TX 75013 Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	Equifax 1-888-378-4329 www.equifax.com Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069 Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788
--	---	--

Additional Information: You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them.

The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.



You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For Maine Residents, the Maine Attorney General may be contacted at 6 State House Station, Augusta, ME 04333; 207-626-8800; and <https://www.maine.gov/ag/>.

For Maryland Residents, the Maryland Attorney General may be contacted at Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202; 1-888-743-0023; and www.marylandattorneygeneral.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; and <https://ag.ny.gov>.

For North Carolina Residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island Residents, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 3 Rhode Island residents whose data was impacted by this incident.

For Vermont Residents, the Vermont Attorney General's Office may be contacted at 109 State Street, Montpelier, VT 05609; 802-828-3171; and ago.info@vermont.gov.



[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

December 23, 2025

Re: Notice of Data Security Incident

Dear [REDACTED]:

White Sands Treatment Center of Tampa, LLC (“White Sands”) takes privacy and security very seriously. As part of that commitment, we are writing to notify you of a data privacy incident involving your personal information. This notice explains the incident, our response, and steps you can take to help protect your personal information.

What Happened: On July 8, 2025, we became aware that a former employee may have taken patient information without authorization. Upon discovery, White Sands took immediate action to conduct an investigation into the incident to determine what, if any, unauthorized activity occurred. After a thorough investigation, on August 4, 2025, it was determined that on April 1, 2025, just prior to her last day of employment, the former employee stole a file containing patient information, limited to names, contact information, and admission and/or discharge dates.

What Information Was Involved: Our review of the files determined your first and last name, in combination with your address, phone number, email address, and admission and/or discharge date, were present within the file.

What We Are Doing: Upon learning of this incident, we took immediate steps to mitigate the risk of similar incident occurring in the future, including implementing enhanced security protocols and safeguards as well as revised our policies and provided internal trainings.

What You Can Do: To date, we are not aware of any reports of identify fraud as a result of the information impacted by this incident. However, it is always prudent for patients to review health care statements for accuracy and report to your provider or insurance carrier any services or charges that were not incurred. Additionally, there are further steps and protections that individuals can take (see enclosure), including those recommended by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For More Information: If you have any questions or concerns, please contact our dedicated assistance line at 1-833-[REDACTED], Monday through Friday, 8:00 a.m. to 8:00 p.m. EST, excluding major U.S. holidays. Please know that the security of information is of the utmost importance to us. We remain committed to protecting the information entrusted in our care. We continue to be thankful for your support during this time.

Sincerely,

White Sands Treatment Center of Tampa, LLC

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts and Credit Reports: It is good practice to remain vigilant of incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-██████. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

Fraud Alert Services: You have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

Credit Freeze Instructions: As an alternative to a fraud alert, you have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit.

Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you should provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver’s license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1- 800-916-8800 www.transunion.com TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000 TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Experian 1-888-397-3742 www.experian.com Experian Fraud Alert P.O. Box 9554 Allen, TX 75013 Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	Equifax 1-888-378-4329 www.equifax.com Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069 Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788
--	---	--

Additional Information: You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them.

The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.



You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For Maryland Residents, the Maryland Attorney General may be contacted at Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202; 1-888-743-0023; and www.marylandattorneygeneral.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; and <https://ag.ny.gov>.

For North Carolina Residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Texas Residents, the Texas Attorney General may be contacted at 300 W. 15th Street, Austin, TX 78701; 800-621-0508; and texasattorneygeneral.gov/consumer-protection/.