Notice of Data Security Event

At Brevard Skin and Cancer Center ("Brevard"), we take privacy seriously. Thus, we are notifying individuals of an event that may affect the security of certain personal information retained by Brevard. Importantly, we currently do not have any evidence that any personal information has been subject to identity theft as a result of the data security incident. Please be aware that this incident will not disrupt or interfere with the care provided by Brevard. Nonetheless, we are providing information about the event, our response to it, and ways to help prevent any potential harm.

What Happened?

On October 14, 2025, Brevard became aware of a breach of security of certain protected health information ("PHI") and personally identifiable information ("PII") maintained in its data systems. When the incident was first discovered, Brevard immediately retained cybersecurity experts, took actions to contain the incident, began investigating the matter, and worked to remediate its electronic environment. The investigation is on-going, but Brevard discovered that on or around September 28, 2025, an unauthorized third party accessed some of its data systems and exfiltrated certain data. Brevard has been working hard to discover the identities of all affected individuals and the types of PHI and PII accessed in order to provide adequate notice.

What Information Was Involved?

While the investigation is ongoing, Brevard believes the categories of PHI that may have been affected as a result of the incident include one or more of the following elements for current or former patients: full name, date of birth, home address, Social Security Number, phone number, diagnosis and clinical information, e-mail address, and billing and claims information.

Brevard believes the categories of PII that may have been affected as a result of the incident include one or more of the following elements for current or former employees: full name, date of birth, home address, Social Security Number, phone number, health condition included in FMLA form, and e-mail address.

The information is not believed to include financial account numbers, banking information, or credit or debit card information.

What Are We Doing?

We took immediate steps to contain and secure our environment. We have worked vigilantly with our IT and cybersecurity team, and legal counsel to thoroughly review the affected systems, establish the integrity of our data, investigate the incident, and implement heightened security protections. We reported this incident to the FBI, and we are in the process of reporting the incident to applicable regulators, as required by law.

In light of this incident, we are reviewing our privacy and security policies and procedures, and we are continuing to evaluate our network security for opportunities to incorporate further safeguards to protect our systems from potential future incidents.

To the extent required by applicable law, we will be providing notice to potentially affected individuals for whom we have a valid mailing address, so that they may take further steps to protect their information as appropriate. As a safeguard, we have arranged for affected individuals to have the option to enroll, at no cost, in an online credit monitoring service, IDX, to provide twenty-four (24) months of complimentary credit monitoring services, which provides monitoring of all three (3) major credit reporting agencies –

Equifax, Experian, and TransUnion. IDX identity protection services also provide CyberScan monitoring, a $1,000,000 insurance reimbursement policy, fully managed id theft recovery services, and lost wallet assistance. With this protection, IDX will help resolve issues if an individual's identity is compromised. Additional information is provided below on further steps you can take to protect your personal information, a toll-free number to call to determine if your information was impacted as a result of this incident and, if so, how to register for the complimentary credit monitoring.

Please note that credit monitoring services may not be available for individuals who do not have an address in the United States and a valid Social Security Number.

What Can You Do? We encourage everyone to remain vigilant against incidents of identity theft and fraud, to review account statements, explanation of benefits, and credit reports for suspicious activity and to detect any errors over the next 12 to 24 months. Please review the information contained on the following page

For More Information. Further information about how to protect personal information appears on the following page, *Recommended Steps to Help Protect Your Information*. If you have questions about whether your data was impacted as a result of this incident, and, if so, how to enroll in the free identity protection services, please call IDX's call center at 1-833-779-4803 (toll-free). Representatives are available Monday through Friday from 9 am - 9 pm Eastern Time, except holidays. You may also contact us at Brevard Skin and Cancer Center, 1286 S. Florida Ave., Rockledge, FL 32955; Phone: 321-301-4740.

Recommended Steps to Help Protect Your Information

1. **Monitoring.** We encourage you to remain vigilant against potential identity theft and fraud, to review your account statements and explanation of benefits, and to monitor your credit reports for suspicious activity.

2. Activate the credit monitoring. If your information was impacted as part of the incident, activate the credit monitoring provided as part of your IDX identity protection 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, IDX will be able to assist you. If you have any questions about whether your data was affected as a result of this incident and/or about enrolling in the credit monitoring service, please contact IDX at 1-833-779-4803 (toll-free). The deadline to enroll is February 13, 2026.

3. Telephone. Contact IDX at 1-833-779-4803 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 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 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 IDX identity protection, notify IDX immediately by calling or by logging into the IDX 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 IDX 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 IDX Care Specialist who will work on your behalf 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.

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 the websites. 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. 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 all three credit reports, 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. You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security freeze to take control over who gets access to the personal and financial information in your credit report 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554 Allen, TX 75013	P.O. Box 160	P.O. Box 105788
888-397-3742	Woodlyn, PA 19094	Atlanta, GA 30348-5788
www.experian.com/freeze/center.html	888-909-8872	800-685-1111
	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order to request a security freeze, you may need to provide the following information:

- Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
- Social Security Number;
- Date of Birth;
- If you have moved in the past 5 years, provide the addresses where you have lived over the past 5 years;
- Proof of current address, such as a current utility bill or telephone bill;
- A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
- 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 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 can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been

misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above.

You can also review the Federal Trade Commission's steps to "Protect Your Personal Information and Data" (available at www.consumer.ftc.gov/articles/protect-your-personal-information-and-data), as well as the "Guidance for Families" provided by the Cybersecurity Infrastructure & Security Agency (available at www.cisa.gov/shields-guidance-families). You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

8. Contact Information for State Attorney Generals

For Alabama residents, the Attorney General can be contacted at: 501 Washington Avenue, Montgomery, AL 36104; 1-800-392-5658 or 334-242-7335; or www.alabamaag.gov.

For California residents, the Attorney General may be contacted at: P.O. Box 944255 Sacramento, CA 94244-2550; 916-210-6276 or 800-952-5225; or https://oag.ca.gov.

For Florida residents, the Attorney General may be contacted at: PL-01, The Capitol, Tallahassee, FL 32399-1050; 866-966-7226; or www.myfloridalegal.com.

For Idaho residents, the Attorney General may be contacted at: 700 W. Jefferson Street, Suite 210, P.O. Box 83720, Boise, ID 83720-0010; 208-334-2400; or https://www.ag.idaho.gov/.

For Kansas residents, the Attorney General may be contacted at: 120 SW 10th Ave., 2nd Floor, Topeka, KS 66612; 785-296-2215; or https://www.ag.ks.gov/home.

For Louisiana residents, the Attorney General may be contacted at: 1885 North Third Street, Baton Rouge, LA 70802; 1-877-297-0995; or https://www.ag.state.la.us/home.

For Maryland residents, the Attorney General may be contacted at: 200 St. Paul Place, Baltimore, MD 21202; 410-576-6300; or https://oag.maryland.gov/pages/oag.aspx.

For Michigan residents, the Attorney General may be contacted at: 525 W. Ottawa St. Lansing, MI 48906; 517-335-7622; or https://www.michigan.gov/ag.

For New York residents, the Attorney General may be contacted at: The Capitol, Albany, NY, 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the Attorney General may be contacted at: 114 West Edenton Street, Raleigh, NC 27603; 919-716-6400; or https://ncdoj.gov.

For Ohio residents, the Attorney General may be contacted at: 30 E. Broad St., 14th Floor, Columbus, OH 43215; (800) 282-0515; or https:/www.ohioattorneygeneral.gov.

For Oregon residents, the Attorney General may be contacted at: 1162 Court Street NE, Salem, OR 97301-4096; 503-378-6002; or https://www.doj.state.or.us.

For Pennsylvania residents, the Attorney General may be contacted at: General Strawberry Square, Harrisburg, PA 17120; 717-787-3391; or https://www.attorneygeneral.gov.

For Rhode Island residents, the Attorney General may be contacted at: 150 South Main Street, Providence, RI 02903; 401-274-4400; or https://riag.ri.gov.

For Texas residents, the Attorney General may be contacted at: PO Box 12548, Austin, TX 78711-2548; 512-463-2100; or https://www.texasattorneygeneral.gov.

For Virginia residents, the Attorney General may be contacted at: 202 North Ninth Street, Richmond, VA 23219; 804-786-2071; or https://www.oag.state.va.us/.

For Washington residents, the Attorney General may be contacted at: 1125 Washington Street SE, PO Box 40100, Olympia, WA 98504-0100; 360-753-6200; or https://www.atg.wa.gov.

For West Virginia residents, the Attorney General may be contacted at: State Capitol Complex, Bldg. 1, Rm E-26, 1900 Kanawha Blvd. E, Charleston, WV 25305; 304-558-2021; or https://ago.wv.gov/pages/default.aspx.

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