Elitecare EMERGENCY HOSPITAL
2530 Gulf Fwy S. League City | www.elite24er.com
P.O. Box 989728
West Sacramento, CA 95798-9728

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://response.idx.us/ERLC

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

September 16, 2024

Notice of Data Breach

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

This notice is from Elitecare Emergency Hospital, formerly known as Elitecare Emergency Room ("Elitecare," "we," "our"), about a recent cybersecurity incident. This incident involved the unauthorized access to personal information and/or protected health information (collectively "PHI") in our network.

Elitecare takes the privacy and security of your PHI very seriously, and our review of the incident is ongoing. Although we have not detected any attempted or actual misuse of your PHI, Elitecare is providing this notice to help you understand what happened, let you know that your information may have been impacted, and give you information on steps you can take to protect your privacy. We are also offering to provide you with two years of complimentary credit monitoring and identity theft protection services at no cost to you.

What happened?

Elitecare identified suspicious activity on its computer systems on July 10, 2024, and took immediate steps to stop the activity. Specifically, we disconnected and turned off systems to prevent further impact, retained an outside cybersecurity incident response team to augment our information technology company's resources, began an investigation, and contacted federal law enforcement. On July 17, 2024, we determined the incident was a cybersecurity breach and worked with the incident response team to conduct a forensic analysis. The investigation confirmed that the intruder accessed PHI, but we have not identified evidence this incident spread beyond the original intruder.

What information was involved?

While Elitecare cannot confirm exactly what data was affected for each impacted individual, information involved for affected individuals may have included contact information (such as first and last name, address, date of birth, phone number, and email) and one or more of the following:

- Health insurance information (such as primary, secondary, or other health plans/policies, insurance companies, member/group ID numbers, and Medicaid-Medicare-government payor ID numbers);
- Health information (such as medical record numbers, providers, diagnoses, medicines, test results, images, care, and treatment);
- Billing, claims, and payment information (such as claim numbers, account numbers, billing codes, payments made, and balance due); and/or

- Other personal information such as Social Security numbers, driver's licenses or state ID numbers.

The information that may have been involved will not be the same for every impacted individual and may vary further depending on whether your relationship with Elitecare was as a patient or as a guarantor.

What we are doing.

The safety, privacy, and security of our patients are our priorities. Elitecare, along with leading external industry experts, continue to monitor the internet and dark web for any indication that the affected personal information is being circulated. To date, we have seen no indications. Following the incident, Elitecare has reinforced its policies and implemented additional technological safeguards to reduce the risk of similar incidents in the future.

What you can do.

In addition to the steps taken by Elitecare, there are steps individuals can take to protect themselves:

- Any individual who believes their information may have been impacted by this incident can enroll in two years of complimentary credit monitoring and identity protection services. Elitecare is offering to pay for these services for two years.
- Individuals should be on the lookout and regularly monitor the explanation of benefits statements received from their health plan and statements from health care providers, as well as bank and credit card statements, credit reports, and tax returns, to check for any unfamiliar activity.
- If individuals notice any health care services they did not receive listed on an explanation of benefits statement, they should contact their health plan or doctor.
- If individuals notice any suspicious activity on bank or credit card statements or on tax returns, they should immediately contact their financial institution and/or credit card company or relevant agency.
- If an individual believes they are the victim of a crime, they can contact local law enforcement authorities and file a police report.

Individuals may have additional rights available to them depending on the state they live in and should refer to the Reference Guide for additional information.

For more information.

As Elitecare continues to work with leading industry experts to analyze data involved in this cyberattack, immediate support and robust protections are available to individuals who may be concerned about their information.

Elitecare regrets any inconvenience or concern caused by this incident and has established a dedicated call center to offer additional resources and information to people who believe they may have been affected by this incident. Individuals can visit https://response.idx.us/ERLC for more information and details on these resources or call the toll-free call center, which also includes trained clinicians to provide support services. The call center's number is: (877) 225-2067, available Monday through Friday, 8 a.m. to 8 p.m. CT.

How to Enroll in IDX Credit and Identity Monitoring Services

We encourage you to contact IDX with any questions and to enroll in 24 months of free identity protection services by calling (877) 225-2067 or going to https://response.idx.us/ERLC or scanning the QR image and using the Enrollment Code provided above. 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 letter. The enrollment deadline is December 16, 2024.

Individuals must enroll for the available services to go into effect, and the monitoring included in the membership must be activated to be effective. Please note that credit monitoring services may not be available for individuals who have not established credit or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score. If you need assistance, IDX will be able to assist you.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

REFERENCE GUIDE

Review Your Account Statements

Carefully review statements sent to you from your healthcare providers, insurance company, and financial institutions to ensure that all of your account activity is valid. Report any questionable charges promptly to the provider or company with which you maintain the account.

Provide Any Updated Personal Information to Your Health Care Provider

Your health care provider's office may ask to see a photo ID to verify your identity. Please bring a photo ID with you to every appointment if possible. Your provider's office may also ask you to confirm your date of birth, address, telephone, and other pertinent information so that they can make sure that all of your information is up-to-date. Please be sure and tell your provider's office when there are any changes to your information. Carefully reviewing this information with your provider's office at each visit can help to avoid problems and to address them quickly should there be any discrepancies.

Order Your Free Credit Report

To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

Upon receiving your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case. Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security Number).

If you see anything you do not understand, call the credit bureau at the number on the report. Errors may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

Contact the U.S. Federal Trade Commission

If you detect any unauthorized transactions in any of your financial accounts, promptly notify your payment card company or financial institution. If you detect any incidents of identity theft or fraud, promptly report the matter to your local law enforcement authorities, state Attorney General and the FTC.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the contact information below:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft/

Place a Fraud Alert on Your Credit File

To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect against the possibility of an identity thief opening new credit accounts in your name. When a credit grantor checks the credit history of someone applying for credit, the credit grantor gets a notice that the applicant may be the victim of identity theft. The alert notifies the credit grantor to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows flagging of your file with a fraud alert at all three credit bureaus.

Equifax	P.O. Box 105069 Atlanta, Georgia 30348	1- 888-766-0008	**www.equifax.com**
Experian	P.O. Box 9554 Allen, Texas 75013	1-888-397-3742	**www.experian.com**
TransUnion	P.O. Box 2000 Chester, PA 19016	1-800-680-7289	**www.transunion.com**

Security Freezes

You have the right to request a credit freeze from a consumer reporting agency, **free of charge**, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit bureau. To place a security freeze on your credit report, you must contact the credit reporting agency by phone, mail, or secure electronic means and provide proper identification of your identity. The following information must be included to request a security freeze (NOTE - if you are requesting a security freeze 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 include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

Below, please find relevant contact information for the three consumer reporting agencies:

Equifax Security Freeze	P.O. Box 105788 Atlanta, GA 30348	1-800-685-1111	**www.equifax.com**
Experian Security Freeze	P.O. Box 9554 Allen, TX 75013	1-888-397-3742	**www.experian.com**
TransUnion	P.O. Box 160 Woodlyn, PA 19094	1-888-909-8872	**www.transunion.com**

Once you have submitted your request, the credit reporting agency must place the security freeze no later than 1 business day after receiving a request by phone or secure electronic means, and no later than 3 business days after receiving a

request by mail. No later than 5 business days after placing the security freeze, the credit reporting agency will send you confirmation and information on how you can remove the freeze in the future.

For Residents Of	Additional Information
District of Columbia	You may contact the D.C. Attorney General's Office to obtain information about steps to take to avoid identity theft: D.C. Attorney General's Office, Office of Consumer Protection, 400 6th Street, NW, Washington DC 20001, 1-202-442-9828, **www.oag.dc.gov**.
Iowa	You may contact law enforcement or the Iowa Attorney General's office to report suspected incidents of identity theft. The Iowa Attorney General's Office can be reached at: Iowa Attorney General's Office, Director of Consumer Protection Division, 1305 E. Walnut Street, Des Moines, IA 50319, 1-515-281-5926, **www.iowattorneygeneral.gov**.
Maryland	You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, **http://www.marylandattorneygeneral.gov/**.
Massachusetts	You have the right to obtain a police report with respect to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.
New Mexico	New Mexico consumers have the right to obtain a security freeze or submit a declaration of removal. You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following: (1) the unique personal identification number, password or similar device provided by the consumer reporting agency; (2) proper identification to verify your identity; and (3) information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report. A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone. A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act. If you are actively seeking a new credit, loan, utility, telephone or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone,

	the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.
New York	You may also obtain information about security breach response and identity theft prevention and protection from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, **www.ag.ny.gov**.
North Carolina	You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-919-716-6000, **www.ncdoj.gov**.
Oregon	State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. Contact information for the Oregon Department of Justice is as follows: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301, 1-877-877-9392, **www.doj.state.or.us**.
Rhode Island	You have a right to file or obtain a police report related to this incident. You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General: Office of the Attorney General, 150 South Main Street, Providence, RI, 02903, 1-401-274-4400, **www.riag.ri.gov**.