FLORIDA HEART
ASSOCIATES

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Florida Heart Associates ("FHA") writes to notify you of a data security incident that may have impacted you as a current or former FHA patient. This letter is to inform you about the incident, our response, and steps you may take to protect against possible misuse of your personal information, should you feel it appropriate to do so.

***What Happened?*** On or about May 19, 2021, FHA became aware of unusual activity within select computer in our network environment. We immediately engaged a team of experts and law enforcement to mitigate the effects of the incident, secure personal information, restore IT functions, and protect FHA's servers from future incidents. Our investigation revealed that malicious actors may have gained access to our network between May 9 and 19, 2021. FHA security systems diminished the impact of the intrusion; however, an unknown actor still gained access to company servers and may have obtained information within. To date, we have not received any indication that your information has been misused by an unauthorized individual.

***What Information Was Involved?*** It is possible that your Social Security number, member identification number, date of birth, and health insurance information may have been seen or accessed. This information is called your personal information or protected health information.

***What We Are Doing.*** We take the confidentiality, privacy, and security of information in our care seriously. Upon discovery, we immediately reported the incident to law enforcement and commenced an investigation to determine the nature and scope of the incident. While investigation remains ongoing, we are taking steps now to implement additional safeguards and review policies and procedures relating to data privacy and security.

FHA has implemented additional security measures designed to prevent a reoccurrence of such incidents, and to protect the privacy of our patients. Among other steps taken, we have installed an endpoint detection and response tool, strengthened our system's architecture, and implemented stronger policies to prevent future attacks.

***What You Can Do.*** We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. We also encourage you to review the "Steps You Can Take to Help Protect Your Information" pages enclosed herein.

***For More Information.*** We understand that you may have some questions about this incident that are not addressed in this letter. Should you have additional questions, please contact the call center we set up to respond to this event at 1-855-545-1951 9:00 a.m. to 6:30 p.m. Eastern Standard Time, Monday through Friday excluding major US holidays.

We understand how important it is for our clients to receive uninterrupted cardiac care services and will resume our regular services and care as soon as possible. We apologize for any inconvenience that may have arose as a result of this incident. In the meantime, we ask for your understanding and patience.

Sincerely,

Todd Rauchenberger, MBA, CEO
Florida Heart Associates

## Steps You Can Take to Help Protect Your Information

### Check Your Accounts

We urge you to stay alert for incidents of identity theft and fraud, review your account statements, and check your credit reports for shady activity. Under U.S. law, you are eligible for one free credit report each year from each of the three major credit reporting bureaus. To order your free credit report, visit annualcreditreport.com or call toll-free 877-322-8228. You may also reach out to the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a security freeze on your credit report. The security freeze will stop a consumer reporting agency from giving out personal or financial information in your credit report without your consent. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. Note: using a security freeze to take control over who gets access to your credit report may delay or prevent any new loan, credit, mortgage, or any other credit extension request or application you make from being approved timely. Under federal law, you cannot be charged to place or lift a security freeze on your credit report. If you wish to place a security freeze, please reach out to these major consumer reporting agencies:

**Experian**
P.O. Box 9554
Allen, TX 75013
888-397-3742
experian.com/freeze/center

**TransUnion**
P.O. Box 160
Woodlyn, PA 19094
888-909-8872
transunion.com/credit-freeze

**Equifax**
P.O. Box 105788
Atlanta, GA 30348-5788
800-685-1111
equifax.com/personal/credit-report-services

To request a security freeze, you will need to provide these items:

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

Instead of a security freeze, you have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Businesses are required to take steps to verify a consumer's identity before extending new credit once they see a fraud alert on a credit file. If you are a victim of identity theft, you are eligible for an extended fraud alert. This is a fraud alert lasting seven years. If you wish to place a fraud alert, please reach out to any one of these agencies:

**Experian**
P.O. Box 9554
Allen, TX 75013
888-397-3742
experian.com/fraud

**TransUnion**
P.O. Box 2000
Chester, PA 19016
800-680-7289
transunion.com/fraud-victim-resource/place-fraud-alert

**Equifax**
P.O. Box 105069
Atlanta, GA 30348
888-766-0008
equifax.com/personal/credit-report-services

### More Information

You can learn more about identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by reaching out to:

- The consumer reporting agencies.
- The Federal Trade Commission at: 600 Pennsylvania Ave. NW, Washington, DC 20580, identitytheft.gov, 877-ID-THEFT (877-438-4338); TTY: 866-653-4261.

    - The FTC also urges those who learn their information has been misused to file a complaint with them. Reach out to the FTC for steps to file such a complaint.
- Your state Attorney General.

You have the right to file a police report if identity theft or fraud ever happen to you. Note: to file a report with law enforcement for identity theft, you will need to give some proof you have been a victim. Also, you must report cases of known or presumed identity theft to law enforcement and your state Attorney General.

**All U.S. Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave. NW, Washington, DC 20580, consumer.gov/idtheft, 877-IDTHEFT (877-438-4338), TTY: 866-653-4261.

**Florida Residents:** Office of the Attorney General of Florida, 1-866-966-7226 (Fraud Hotline), http://myfloridalegal.com/identitytheft.