EXHIBIT 1

The Chattanooga Heart Institute is providing supplemental notice of additional Maine residents impacted by the incident reported to your office on July 28, 2023, October 6, 2023, and on February 13, 2024. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, The Chattanooga Heart Institute does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On April 17, 2023, The Chattanooga Heart Institute identified indications of a cybersecurity attack on its IT network. The Chattanooga Heart Institute immediately took steps to secure its network and began an investigation with the assistance of an external forensics vendor. The investigation determined that an unauthorized third party gained access to The Chattanooga Heart Institute's network between March 8, 2023, and March 16, 2023. On May 31, 2023, The Chattanooga Heart Institute learned that the unauthorized third party obtained copies of some of the data from its systems containing confidential patient information, however, the unauthorized third party did not retrieve data directly from The Chattanooga Heart Institute's Electronic Medical Record ("EMR"). While this review is still ongoing, in December 2023, The Chattanooga Heart Institute identified some employees and/or employee dependents whose data was involved. The Chattanooga Heart Institute then worked to identify accurate address information to provide notice to potentially affected individuals and completed these efforts in late January 2024.

The information that could have been subject to unauthorized access includes name, mailing address, email address, phone number, date of birth, driver's license number, Social Security number, account information, health insurance information, diagnosis/condition information, lab results, medications and other clinical, demographic or financial information.

Notice to Maine Residents

While its investigation is ongoing, on or about July 28, 2023, The Chattanooga Heart Institute began providing written notice of this incident. Following the identification of additional potentially impacted individuals, The Chattanooga Heart Institute continued providing written notice on October 5, 2023, February 13, 2024, March 12, 2024, and again on March 27, 2024 to five (5) additional Maine residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, The Chattanooga Heart Institute moved quickly to investigate and respond to the incident, assess the security of The Chattanooga Heart Institute systems, and identify potentially affected individuals. Further, Chattanooga Heart Institute notified federal law enforcement regarding the event. Upon discovering the unauthorized third-party access, The Chattanooga Heart Institute took quick action to protect its systems, contain the incident, begin an investigation, and maintain continuity of care. The Chattanooga Heart Institute is providing access

to credit monitoring services for one (1) year, through Epiq, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, The Chattanooga Heart Institute is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to be vigilant and review health care statements and report any services or charges that were not incurred. The Chattanooga Heart Institute is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

The Chattanooga Heart Institute is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion. The Chattanooga Heart Institute also notified the U.S. Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act (HIPAA).

EXHIBIT A

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>

October 6, 2023

Dear <<Name 1>>:

The Chattanooga Heart Institute takes the protection and proper use of your Protected Health Information ("PHI") very seriously. With that in mind, we are writing to tell you about a data security incident involving some of your PHI. We are writing to you to explain the incident, our response to it, and steps you can take to protect your personal information, should you feel it appropriate to do so.

What happened?
On April 17, 2023, The Chattanooga Heart Institute identified indications of a cybersecurity attack on its IT network. The Chattanooga Heart Institute immediately took steps to secure its network and began an investigation with the assistance of an external forensics vendor. The investigation determined that an unauthorized third party gained access to The Chattanooga Heart Institute's network between March 8, 2023, and March 16, 2023. On May 31, 2023, The Chattanooga Heart Institute learned that the unauthorized third party obtained copies of some of the data from its systems containing confidential patient information, however, the unauthorized third party did not retrieve data directly from The Chattanooga Heart Institute's Electronic Medical Record ("EMR").

What information was involved?
The Chattanooga Heart Institute's investigation shows that you may have been either a patient or guarantor of The Chattanooga Heart Institute. You are being notified because some of your information was identified as potentially having been accessed or acquired by the unauthorized third party. The information in the files may have included your name, mailing address, email address, phone number, date of birth, driver's license number, Social Security number, account information, health insurance information, diagnosis/condition information, lab results, medications and other clinical, demographic or financial information.

What we are doing.
Upon discovering the unauthorized third party access, The Chattanooga Heart Institute took quick action to protect its systems, contain the incident, begin an investigation, and maintain continuity of care. In addition, The

Chattanooga Heart Institute notified federal law enforcement. Once secured, systems were returned to the network with additional security and monitoring tools. To help relieve concerns and restore confidence following this incident, The Chattanooga Heart Institute has secured the services of Equifax to provide identity monitoring at no cost to you for <<one year/two years>>. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Enrollment Instructions.

Go to **www.equifax.com/activate**

Enter your unique Activation Code of **<<Activation Code>>** to activate and take advantage of your identity monitoring services. You have until **<<Enrollment Deadline>>** to activate your identity monitoring services.

For more information about Equifax and your Identity Monitoring services, you can visit www.equifax.com. Additional information describing services available at no cost to you is included with this letter.

Actions you may wish to take.

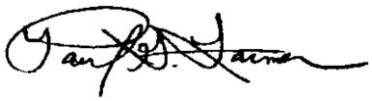
It is always prudent for patients to review health care statements for accuracy and report to your provider or insurance carrier any services or charges that were not incurred. Additionally, please review the enclosed "Additional Resources" section of this letter. That section describes further steps you can take to help protect yourself, including recommendations from 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, if you desire to do so.

For more information.

If you need more information about this IT security event, we have established a call center with a trusted third-party partner that can answer specific questions about this event. To contact this call center, please call 1-833-627-2719, Monday through Friday from 9:00 a.m. to 9:00 p.m. eastern time, excluding U.S. holidays.

We apologize for any concern this may cause. Protecting your information is important to us. We trust that this notification and additional resource information demonstrates our continued commitment to you.

Sincerely,



Paul G. Farmer, President
The Chattanooga Heart

Additional Resources

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, 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, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers 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 the consumer's 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 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 credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); 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 credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016

Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and 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 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 and your state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1- 410-576-6300 or 1-888-743-0023; and www.marylandattorneygeneral.gov/. Imagine360 is located at 1550 Liberty Ridge Dr. Suite 330 Wayne, PA 19087.

For 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 bureaus 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 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. We encourage you to 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 Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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; or 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.