EXHIBIT 1

By providing this notice, McLaren Health Care ("McLaren") 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 or about August 5, 2024, McLaren became aware of suspicious activity related to certain McLaren/Karmanos computer systems and they immediately activated their emergency response processes. Additionally, McLaren launched an investigation with the assistance of third-party forensic specialists to secure their network and to determine the nature and scope of the activity.

Through the investigation, it was determined that there was unauthorized access to the network between July 17, 2024, and August 3, 2024. Following the cybersecurity attack, updates were provided on the mclaren.org and karmanos.org pages and a call center was established to answer questions from McLaren's patients and their communities.

As part of the investigation, McLaren undertook an extensive forensic review of the potentially impacted files to determine whether any sensitive information was present. It was through this process, which concluded on May 5, 2025, that McLaren determined that personal information and protected health information pertaining to individuals was contained within the files involved.

The information that could have been involved includes name, Social Security number, driver's license number, medical information, and health insurance information.

Notice to Maine Residents

On or about June 20, 2025, McLaren began providing written notice of this incident to twenty-five (25) 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, McLaren moved quickly to investigate and respond to the incident, assess the security of McLaren systems, and identify potentially affected individuals. McLaren is also working to implement additional safeguards and training to its employees. McLaren is providing access to credit monitoring services for twelve (12) months, through IDX, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, McLaren is providing impacted individuals with guidance on how to better protect against identity theft and fraud. McLaren 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.

McLaren is providing written notice of this incident to relevant state and federal regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

EXHIBIT A

McLaren
HEALTH CARE
P.O. Box 989728
West Sacramento, CA 95798-9728

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

Enrollment Code: <<ENROLLMENT>>
To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://app.idx.us/account-creation/protect

June 20, 2025

McLaren Health Care values our relationship with every patient and family we serve, and maintaining your trust and confidence is important to us. Our organization was the target of a cybersecurity attack by an international ransomware group that impacted the McLaren Health Care and Karmanos Cancer Institute computer network. We are writing today to inform you about what happened, what information was involved, what we have done to address the situation and what you can do to help protect yourself against possible misuse of information.

What Happened?
On or about August 5, 2024, we became aware of suspicious activity related to certain McLaren/Karmanos computer systems and we immediately activated our emergency response processes. Additionally, we launched an investigation with the assistance of a third-party forensic specialists to secure our network and to determine the nature and scope of the activity.

Through the investigation, it was determined that there was unauthorized access to the network between July 17, 2024, and August 3, 2024. Following the cybersecurity attack, updates were provided on the mclaren.org and karmanos.org pages and a call center was established to answer questions from our patients and our communities.

As part of our investigation, we undertook an extensive forensic review of the potentially impacted files to determine whether any sensitive information was present. It was through this process, which concluded on May 5, 2025, that we determined that information pertaining to you may have been included in the impacted files.

What Information Was Involved?
The information involved may include some combination of the following data types: name, <<Variable Text 3: Data Elements>>.

What We Are Doing
McLaren takes the security of your information seriously. Upon learning of this incident, we immediately took steps to secure our network and maintain clinical operations in a safe and secure fashion to continue serving the community. As part of our ongoing commitment to the privacy of personal information in our care, we continue to review our existing policies and procedures and implement additional administrative and technical safeguards to further secure the information on our systems. We remain committed to fully complying with all state and federal requirements and maintaining timely and transparent communication with our patients and the community.

What You Can Do
While there is currently no evidence that your information has been misused, we recommend that you remain vigilant, monitor and review all your financial and account statements and explanations of benefits, and report any unusual activity to the institution of record and to law enforcement. You may also review the guidance contained in the enclosed *Steps You Can Take to Protect Personal Information*. In addition, we are offering <<12/24>> of identity theft

protection services through IDX. You will find detailed instructions for enrollment through the enclosed guidance. We encourage you to enroll in these services as we are not able to do so on your behalf. The deadline to enroll is September 20, 2025.

For More Information

For assistance with questions regarding this incident, please call 1-855-201-0136 or go to mclaren.org/notice. Representatives are available Monday through Friday from 9 a.m. to 9 p.m. Eastern Time. You may also write to McLaren at One McLaren Parkway, Grand Blanc, MI 48439.

Steps You Can Take To Protect Personal Information

Enroll in Monitoring Services

1. Website and Enrollment. Scan the QR image or go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. 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.

3. Telephone. Contact IDX at 1-855-201-0136 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

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 a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any 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 a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of 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 they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, 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/data-breach-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, 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, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

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 https://www.marylandattorneygeneral.gov/.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their 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 consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately 8 Rhode Island residents that may be impacted by this event.