FAIRCHILD MEDICAL CENTER

C/O IDX
P.O. Box 1907
Suwanee, GA 30024

November 25, 2020

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

Dear <<First Name>> <<Last Name>>:

Fairchild Medical Center ("FMC") writes to notify you of an event that may affect the security of some of your personal information. While, to date, we have no evidence that your information has been misused, we are providing you with information about the event, our response to it, and resources available to you to help protect your information, should you feel it appropriate to do so.

What Happened? In late July 2020, FMC was made aware of an issue involving a misconfiguration on one of its servers through a communication from a third-party security company unaffiliated with FMC. FMC immediately commenced an investigation and began working with third party computer specialists to determine the nature and scope of the issue. FMC also immediately addressed the misconfiguration and took steps to secure the server. A third party security company verified that the server security change resolved the issue. Through the investigation, FMC determined that a misconfiguration existed from approximately December 16, 2015 to July 31, 2020 that allowed external individual(s) access to the server. On November 5, 2020, following an extensive review of forensic evidence associated with the server, FMC's investigation determined that it could not conclusively rule out unauthorized access to records present on the server during the window of time when the misconfiguration was in place.

As such, out of an abundance of caution, FMC reviewed the server to determine what records were present during that window. While the investigation did not confirm that your record was specifically accessed without authorization, in an abundance of caution, FMC is providing you with notice of this incident because your record was present on the server.

What Information Was Involved? The information contained on the server includes a medical image, your name, date of birth, patient identification number, exam identification number, the ordering provider, and the date of the exam. Please note, this incident did ***not*** affect your full medical record. Additionally, this incident did ***not*** affect your Social Security number, nor your financial information.

What Are We Doing? Information privacy and security are among our highest priorities. FMC has strict security measures in place to protect information in our care. Upon learning of this incident, we moved quickly to respond. This included conducting an investigation with the assistance of third-party forensic specialists and engaging in steps to ensure the security of the one affected server. The security change of the server was verified by a third party security firm to confirm resolution of the server security issue.

What Can You Do? We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements and explanation of benefits, and to monitor your free credit reports for suspicious activity and to detect errors. Please review the information contained in the attached "Steps You Can Take to Protect Personal Information."

For More Information. We recognize that you may have questions not addressed in this letter. If you have additional questions, please contact our dedicated assistance line at (833) 752-0849 from 6:00 am to 6:00 pm Pacific Time, Monday through Friday, except holidays. You may also write to FMC at 444 Bruce Street, Yreka, California 96097.

Sincerely,

Jonathon Andrus

Chief Executive Officer
Fairchild Medical Center

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Monitor Your Accounts

Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact 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, 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	P.O. Box 160	P.O. Box 105788
Allen TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-800-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

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

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior 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, military identification, etc.);
7. 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.

As an alternative to 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 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 agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Additional Information

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.

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); 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. 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; 1-410-528-8662; or www.oag.state.md.us.

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 agencies 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 provides resources regarding identity theft protection and security breach response at www.ag.ny.gov/internet/privacy-and-identity-theft. The New York Attorney General may be contacted: by phone at 1-800-771-7755; toll-free at 1-800-788-9898; or online at www.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; or www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General can be reached contacted at 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov, or 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There is 1 Rhode Island resident potentially impacted by this incident.

For Washington, D.C. residents, the Office of Attorney General for the District of Columbia may be contacted at: 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001; 1-202-442-9828; or https://oag.dc.gov.

Notice of Data Incident
November 25, 2020

Fairchild Medical Center ("FMC") is notifying individuals of an event that may affect the security of some personal information. While, to date, we have no evidence that information has been misused, we are providing information about the event, our response to it, and resources available to help protect information.

What Happened? In late July 2020, FMC was made aware of an issue involving a misconfiguration on one of its servers through a communication from a third-party security company unaffiliated with FMC. FMC immediately commenced an investigation and began working with third party computer specialists to determine the nature and scope of the issue. FMC also immediately addressed the misconfiguration and took steps to secure the server. A third party security company verified that the server security change resolved the issue. Through the investigation, FMC determined that a misconfiguration existed from approximately December 16, 2015 to July 31, 2020 that allowed external individual(s) access to the server. On November 5, 2020, following and extensive review of forensic evidence associated with the server, FMC's investigation determined that it could not conclusively rule out unauthorized access to records present on the server during the window of time when the misconfiguration was in place.

What Information Was Involved? The information contained on the server includes a medical image, an individual's name, date of birth, patient identification number, exam identification number, the ordering provider, and the date of the exam. Please note, this incident did *not* affect an individual's full medical record. Additionally, this incident did *not* affect any individual's Social Security number, nor financial information.

What Is FMC Doing? Information privacy and security are among FMC's highest priorities. FMC has strict security measures in place to protect information in our care. Upon learning of this incident, we moved quickly to respond. This included conducting an investigation with the assistance of third-party forensic specialists and engaging in steps to ensure the security of the one affected server. The security change of the server was verified by a third party security firm to confirm resolution of the server security issue.

What Can Individuals Do? Please review the information listed below in the "Steps You Can Take to Protect Personal Information" section of this page.

For More Information. We recognize that individuals may have questions that were not addressed here. If you have additional questions, please contact our dedicated assistance line at (833) 752-0849, 6 a.m. - 6 p.m. Pacific Time, Monday through Friday, except holidays.

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements and explanation of benefits, and to monitor your free credit reports for suspicious activity and to detect errors. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact 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, 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	P.O. Box 160	P.O. Box 105788
Allen TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-800-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

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

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior 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, military identification, etc.);
7. 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.

As an alternative to 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 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 agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Additional Information

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.

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); 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. 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; 1-410-528-8662; or www.oag.state.md.us.

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 agencies 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 provides resources regarding identity theft protection and security breach response at www.ag.ny.gov/internet/privacy-and-identity-theft. The New York Attorney General may be contacted: by phone at 1-800-771-7755; toll-free at 1-800-788-9898; or online at www.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; or www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General can be reached contacted at 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov, or 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. The number of Rhode Island residents potentially impacted by this incident is not currently known.

For Washington, D.C. residents, the Office of Attorney General for the District of Columbia may be contacted at: 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001; 1-202-442-9828; or https://oag.dc.gov.