

To Whom it May Concern:

6/29/21

The undersigned is the Privacy & Security Official of the Fairbanks Cancer Care Physicians, P.C. We are writing to inform you of a recent data security incident that involved our business associate, Elekta, Inc. ("Elekta"). Related to this incident, we as the covered entity are subject to the breach notification rules of the Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA"), which requires that a covered entity provide Substitute notice on the homepage of their website for 90 days in the case which there is insufficient or out of date contact information for 10 or more individuals following the discovery of a breach of Protected Health Information ("PHI"). On May 4, 2021 we were informed by Elekta that an incident requiring notice occurred. Please consider this letter notice to you of this situation, as described below.

What Happened?

On or about April 6, 2021, Elekta's first-generation cloud-based storage system experienced a data security incident. Immediately upon learning of this incident, Elekta engaged a forensic investigator to launch an investigation to determine the nature and scope of the suspicious activity. On April 28, 2021, the forensic investigation confirmed that there was access to PHI as a result of the incident. While the forensics investigation is still ongoing, out of an abundance of caution, Elekta must conclude that all data within Elekta's first-generation cloud system was compromised. The compromised system remains shut down to protect patient and customer information and to prevent any further access to Elekta's system.

What Information Was Involved?

The following types of PHI belonging to Fairbanks Cancer Care Physicians, P.C. patients residing in Alaska or neighboring states may have been involved in the incident: full name, social security number, address, date of birth, height, weight, medical diagnosis, medical treatment details, appointment confirmations, and other information. No financial account, credit card, or debit card information was involved in this incident.

What We Are Doing.

We take this incident and the security of patient information seriously. Upon learning of this incident, Elekta launched an in-depth investigation of the incident by engaging a third-party forensic investigator, and took steps to prevent any further access to its systems. Elekta also promptly notified its customers, including us, of the incident. Immediately after we were notified of the incident, we began working with Elekta to better understand the nature and scope of the incident and coordinate our efforts to find alternate ways to continue treating patients. We will continue working with Elekta to ensure our patients continue to receive treatment, further secure the patient information, and notify regulatory authorities as required. As an added precaution, Elekta is also offering complimentary access to identity monitoring, fraud consultation, and identity theft restoration services to affected individuals. Affected individuals will receive direct notice via First Class Mail provided they have a current mailing address on file. This notice found on our website is for Substitute notice.

What You Can Do.

You can find out more about how to protect against potential identity theft and fraud in the attached Reference Guide.

For More Information.

We understand that you may have questions about this incident that are not addressed in this letter.

If you have additional questions, please call our dedicated assistance line at (866) 281-0520, Monday through Friday from 9 a.m. to 11 p.m. Eastern, and Saturday and Sunday from 11 a.m. to 8 p.m. Eastern. Please be prepared to provide engagement number B015171.

Sincerely,

Michelle Coleman

Operations Manager

Privacy & Security Officer

Fairbanks Cancer Care Physicians, P.C.

REFERENCE GUIDE

In the event that you suspect that you are a victim of identity theft, we encourage you to remain vigilant and consider taking the following steps:

Order Your Free Credit Report. To order your free 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 website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Do not contact the three credit bureaus individually; they provide your free report only through the website or toll-free number.

When you receive your credit report, review the entire report carefully. Look for any inaccuracies and/or accounts you don’t recognize, and notify the credit bureaus as soon as possible in the event there are any.

You have rights under the federal Fair Credit Reporting Act (“FCRA”). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf> or www.ftc.gov

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 you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be a victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can report potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus.

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	1-800-525-6285	www.equifax.com
Experian	P.O. Box 9532 Allen, Texas 75013	1-888-397-3742	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 2000 Chester, Pennsylvania 19016	1-800-680-7289	www.transunion.com

Place a Security Freeze on Your Credit File. You have the right to place a “security freeze” on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. You can request a security freeze free of charge by contacting the credit bureaus at:

Equifax	P.O. Box 740241	www.equifax.com
---------	-----------------	--

Atlanta, Georgia 30374-0241

Experian P.O. Box 9554 www.experian.com
Allen, Texas 75013

TransUnion Fraud Victim Assistance Division www.transunion.com
P.O. Box 2000
Chester, Pennsylvania 19016

The credit bureaus may require that you provide proper identification prior to honoring your request. 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 law enforcement agency concerning identity theft

Placing a security freeze on your credit file may delay, interfere with, or prevent timely approval of any requests you make for credit, loans, employment, housing or other services. For more information regarding credit freezes, please contact the credit reporting agencies directly.

Contact the U.S. Federal Trade Commission. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and the Federal Trade Commission ("FTC"). If you believe your identity has been stolen, the FTC recommends that you take these additional steps.

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can learn more about how to protect yourself from becoming an identity theft victim (including how to place a fraud alert or security freeze) by contacting the FTC:

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

For District of Columbia Residents: You can obtain information from the FTC and the Office of the Attorney General for the District of Columbia about steps to take to avoid identity theft. You can contact the D.C. Attorney General at: 441 4th Street, NW, Washington, DC 20001, 202-727-3400, www.oag.dc.gov

For Iowa Residents: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For Maryland Residents: You can obtain information from the Maryland Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, www.oag.state.md.us

For Massachusetts Residents: You have a right to request from us a copy of any police report filed in connection with 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. As noted above, you also have the right to place a security freeze on your credit report at no charge.

For New York Residents: You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information:

New York Attorney General's Office
Bureau of Internet and Technology
(212) 416-8433
<https://ag.ny.gov/internet/resource-center>

NYS Department of State's Division of
Consumer Protection
(800) 697-1220
<https://www.dos.ny.gov/consumerprotection>

For North Carolina Residents: You can obtain information from the Federal Trade Commission and the North Carolina Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, www.ncdoj.gov

For Oregon Residents: State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. You can contact the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392, www.doj.state.or.us

For Rhode Island Residents: You can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. As noted above, you have the right to place a security freeze on your credit report at no charge, but note that consumer reporting agencies may charge fees for other services.