BakerHostetler

Baker&Hostetler LLP

811 Main Street
Suite 1100
Houston, TX 77002-6111

T 713.751.1600
F 713.751.1717
www.bakerlaw.com

Lynn Sessions
direct dial: 713.646.1352
lsessions@bakerlaw.com

July 23, 2021

VIA EMAIL (DOJ-CPB@DOJ.NH.GOV)

Attorney General John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Incident Notification

Dear Attorney General John Formella:

We are writing on behalf of our client, Yale New Haven Health Services Corporation ("YNHHS"), to provide notice of a security incident involving New Hampshire residents.

On May 26, 2021, Elekta, Inc., a vendor that provides a cloud-based mobile application known as SmartClinic, informed YNHHS that an unauthorized party gained access to Elekta's systems between April 2, 2021 and April 20, 2021. During that time, the unauthorized party acquired a copy of the SmartClinic database file that stored some of YNHHS' patients' information. YNHHS immediately undertook an extensive internal investigation to determine what information was involved and identify affected individuals. On June 4, 2021, YNHHS determined that the names and Social Security numbers of two New Hampshire residents were contained within the database file.

This incident did not involve access to YNHHS's systems, network, or electronic health records. It occurred on Elekta's systems, which held a database for cancer patients seen at YNHHS's facilities. The incident was not targeted at YNHHS or its hospitals.

On July 23, 2021, YNHHS will mail notification letters to the New Hampshire residents in substantially the same form as the enclosed letter via U.S. First-Class mail in accordance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")[1] and N.H. Rev. Stat.

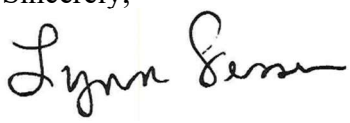
[1] 45 CFR §§ 160.103 and 164.400 *et seq*.

Ann. § 359-C:20.[2] Patient notification will also be effectuated via substitute notice on YNHHS's website in accordance with HIPAA. YNHHS is offering the individuals complimentary, two-year memberships to credit monitoring and identity theft prevention services. YNHHS has also established a dedicated, toll-free call center where all individuals may obtain more information regarding the incident.

To help prevent something like this from happening again, YNHHS is reviewing how information is stored with third-party vendors and is re-evaluating its relationship with Elekta.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,



Lynn Sessions

Enclosure

[2] Please note that 3 additional New Hampshire residents are being notified pursuant to HIPAA, but the information involved for these individuals does not constitute "personal information" as defined by N.H. Rev. Stat. Ann. § 359-C:19.

<<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>>,

On behalf of Yale New Haven Health, we are writing to make you aware of a recent data security incident which impacted one of our vendors, Elekta, Inc. ("Elekta"), a company that provides technology services, including data storage to Yale New Haven Health.

Unfortunately, the occurrence and sophistication of cybercrimes has increased significantly in recent years. This particular security incident was part of a ransomware attack that affected at least forty of Elekta's healthcare clients, including Yale New Haven Health. We were notified by Elekta on May 26, 2021, that an unauthorized party accessed Elekta's systems between April 2 and April 20, 2021, acquiring a copy of a database which contained your protected health information. The following information may have been viewed as a result of this incident: full name, address, phone number, email, Social Security Number, treatment location and preferred language. Please note that at no point in time did the cyber-criminal have access to Yale New Haven Health's electronic medical record or systems as a result of this incident.

Yale New Haven Health understands that your privacy is critically important and we take the security of private information very seriously. We truly value the relationship with our community and the trust you put in us as a community resource. We will continue to work with Elekta to ensure our data is fully protected, however, we are reviewing our relationship with Elekta in light of this incident. In the meantime, we recommend that you remain vigilant of any unusual activity.

What we are doing to protect your information:
To help protect your identity, we are offering a complimentary 24-month membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **<<b2b_text_1(EnrollmentDeadline)>>** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- Provide your **activation code**: **<<Member ID>>**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-288-8057 by **<<b2b_text_1(EnrollmentDeadline)>>**. Be prepared to provide engagement number **<<b2b_text_2(EngagementNumber)>>** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*

- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 877-288-8057. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

On behalf of Yale New Haven Health, we apologize for this incident and truly regret any inconvenience this has caused. It is our goal as a premier healthcare provider to demonstrate respect for patients and our community and to always safeguard their information. If you have any questions regarding this incident, please call (855) 545-1957, Monday through Friday, between 9:00 a.m. and 6:30 p.m. Eastern Standard Time.

Sincerely,

Gayle S. Slossberg
Vice President, Corporate Compliance
Chief Compliance and Integrity Officer

Glynn Stanton
Vice President, Office of Information Security
Chief Information Security Officer

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For New York residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.