octillo

LEGAL + TECH

Liberty Building 420 Main Street Suite 1110 Buffalo New York 14202
Rio Clinton Ave 518 Clinton Square Suite 555 Rochester New York 14604
3 Columbus Circle 15000 New York New York 10019
600 Broadway Suite 700 San Diego California 92101
2 Bala Plaza Suite 300 #701 Bala Cynwyd Pennsylvania 19004

July 12, 2022

VIA CERTIFIED MAIL
Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Dear Sir or Madam:

On behalf of Allied Urological Services, ("Allied"), this letter provides notice of a recent data security incident pursuant to N.H. Rev. Stat. Ann. §359-C:20. By providing this notice, Allied does not waive any rights or defenses regarding the applicability of New Hampshire law, and the applicability of the New Hampshire data notification laws or personal jurisdiction.

On January 3, 2022, Allied became aware of unauthorized access to an employee's email account ("Account") which was utilized for scheduling patient appointments (the "Incident"). Upon learning of the Incident, Allied immediately changed the account's passwords, began an investigation to determine what happened, and took further containment measures to mitigate the Incident, reduce the risk to Protected Health Information ("PHI"), and prevent similar incidents from reoccurring in the future.

On May 13, 2022, the investigation identified that between September 26, 2021, and January 3, 2022, the unauthorized actor(s) accessed the compromised email account via Outlook Web Access and an unknown mail client. Based on the available evidence, the unauthorized actor's activity was limited to and aimed at conducting fraudulent wire transfers. There is no evidence that the actor sought to view, access, or otherwise acquire patient information. However, because of the potential that the mailbox was synced to a system of the unauthorized actor, Allied is notifying individuals and applicable regulators.

Following the Incident, Allied has since taken further steps to increase security and protect information, including: increasing password complexity requirements and implementing password expiration and reuse policy; implementing email gateway and content filtering for all inboxes; enhancing reporting, tracking, and notification concerning suspicious log-ons; increasing systems monitoring and adopted new access controls; implementing increased security awareness training, including enhanced phishing training; and completing enhanced vulnerability scanning of servers and employee endpoints.

While there is no evidence the unauthorized actor specifically viewed, accessed, or misused personal information, the investigation revealed the following categories of information were present in the Account at the time of the Incident: contact information (including: name,

address, and date of birth), social security number, driver's license number or state identification number, financial account and/or payment card information, and information related to appointment scheduling (including: medical diagnosis and treatment information, treatment dates, treatment locations, health insurance information, medical provider or doctor's name, medical record number, patient account number, and prescription information). Note that this is an exhaustive list of the data elements, and the majority of the potentially affected individuals were not associated with each data element.

Three (3) New Hampshire residents may have been affected by this Incident. Beginning on July 12, 2022, letters were mailed to potentially affected individuals for whom Allied had complete addresses. A copy of the letters mailed to potentially affected individuals is attached. Allied also notified the U.S. Department of Health and Human Services, Office for Civil Rights, posted a notice on its website, and notified media in relevant jurisdictions on July 12, 2022. As a courtesy, Allied is providing one (1) year of triple bureau credit monitoring and cyber monitoring services to potentially affected individuals.

Please feel free to contact me with any questions at 716-898-2102 or dgreene@octillolaw.com.

Sincerely,

Daniel P. Greene, Esq.
Certified Information Privacy Professional, United States (CIPP/US)
Certified Information Privacy Professional, Europe (CIPP/E)

Encl.

<<Date>> (Format: Month Day, Year)

[redacted]

Dear [redacted]

Allied Urological Services, LLC ("Allied Urological") provides services related to lithotripsy and urological care on behalf of numerous health care providers, including hospitals and doctors' offices. We write to advise you that we experienced a data security incident (the "Incident"). We are writing to let you know how this Incident may have affected your personal information ("Information") and, as a precaution, to provide steps you can take to help protect your Information. We are unaware of any misuse of the Information, but we are contacting you to share what we know about the Incident.

What Happened?

On January 3, 2022, we identified suspicious activity in an employee's email account ("Employee Account") used for scheduling patient appointments. Upon learning of this, we immediately changed the Employee Account's password, began an investigation, and took further steps to contain and remediate the situation, including a detailed examination of the contents of the email account.

Our investigation identified unauthorized access to the Employee Account between September 26, 2021, and January 3, 2022, and that the possibility exists that the contents of the Employee Account were synced to the system of an unauthorized actor. However, the investigation could not confirm or rule out this possibility.

On May 13, 2022, our investigation revealed that some of your Information was present in the email account at the time of the Incident. There is no evidence that the unauthorized actor sought to view, access, or otherwise acquire your Information. We are not aware of any fraud or misuse related to your Information. However, because your Information could have been accessed by an unauthorized actor, Allied Urological is providing this notice [redacted]

Why Does Allied Urological Have My Personal Information?

Allied Urological provides services related to lithotripsy and urological care on behalf of numerous health care providers, including hospitals and doctors' offices. We may have your Information because of the services we provide to [redacted]

What Information Was Involved?

We have no evidence the unauthorized actor specifically viewed, accessed, or misused your Information. Our investigation revealed that your name and/or address, in addition to the following Information may have been involved in the account: [redacted]

What We Are Doing.

We continue to implement appropriate measures to further improve the security of our systems and practices, including implementing additional software protections and retraining personnel. We are working with a leading cybersecurity firm to aid in our investigation and response and will report this Incident to relevant state and federal authorities. Additionally, to help prevent a similar type of incident from occurring in the future, we implemented additional security protocols designed to protect our network, email environment, systems, and personal information.

What You Can Do.

It is always recommended that you regularly and vigilantly review account statements and report any suspicious activity to financial institutions. Please also review the enclosed "Additional Resources" section included with this letter, which describes additional steps you can take to help protect your Information.

To help protect your identity, we are offering a complimentary twelve (12) 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:

- Make certain that you enroll by: [redacted] (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- Provide your activation code [redacted]

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 [redacted]. Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

For More Information.

If you have any questions please call (855) 516-3853, Monday through Friday, 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays.

Sincerely,

Patricia Sablesak, RN, BSN Allied Urological Services, LLC

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 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every twelve (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.

Complimentary Experian IdentityWorks Credit Monitoring. Once you enroll in Experian IdentityWorks, you can contact Experian immediately regarding any fraud issues, and have access to the following features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.[1]
- **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 ExtendCARETM:** 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. [2]

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 Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Security Freeze. You may obtain a security freeze on your credit report, free of charge, to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may also submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report, free of charge, or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place.

To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or 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 five 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

[1] Offline members will be eligible to call for additional reports quarterly after enrolling

[2] The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

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.

For New Mexico residents: You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

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 avoid 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 Alabama Residents: You may contact the Attorney General's Office for the State of Alabama, Consumer Protection Division, 501 Washington Avenue, Montgomery, AL 36104, www.oag.state.md.us, 1-800-392-5658.

For District of Columbia Residents: You may contact the District of Columbia Office of the Attorney General, 400 6th Street NW, Washington, D.C. 20001, consumer.protection@dc.gov, (202) 442-9828.

For Illinois Residents: You may contact the Illinois Office of the Attorney General, 100 West Randolph Street, Chicago, IL 60601, https://illinoisattorneygeneral.gov/about/email_ag.jsp, 1-800- 964-3013.

For Iowa Residents: You may contact the Iowa Office of the Attorney General, 1305 E. Walnut Street, Des Moines IA 50319, consumer@ag.iowa.gov, 1-888-777-4590.

For Kansas Residents: You may contact the Kansas Office of the Attorney General, Consumer Protection Division, 120 SW 10th Ave, 2nd Floor, Topeka, KS 66612-1597, https://ag.ks.gov/, 1-800- 432-2310.

For Kentucky residents: You may contact the Kentucky Office of the Attorney General, Consumer Protection Division, 1024 Capital Center Drive, Suite 200, Frankfort, Kentucky 40601, www.ag.ky.gov, 1-800-804-7556.

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 Minnesota Residents: You may contact the Minnesota 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 Missouri Residents: You may contact the Missouri Office of the Attorney General, Consumer Protection, 207 W. High St., P.O. Box 899, Jefferson City, MO 65102, www.ago.mo.gov, 1-800-392- 8222.

For New Mexico Residents: You may contact the New Mexico Office of the Attorney General, Consumer Protection Division, 408 Galisteo Street, Villagra Building, Santa Fe, NM 87501, www.nmag.gov, 1-844-255-9210.

For New York Residents: You may contact the New York Office of the Attorney General, Office of the Attorney General, The Capitol, Albany, NY 12224-0341, https://ag.ny.gov, 1-800-771-7755.

For North Carolina Residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Main Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7266.

For Rhode Island Residents: You may contact the Rhode Island Office of the Attorney General, Consumer Protection Division, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 1- 401-274-4400.

For Texas Residents: You may contact the Texas Office of the Attorney General, Office of the Attorney General, PO Box 12548, Austin, TX 78711-2548, www.texasattorneygeneral.gov, 1-800- 621-0508.

Reporting of identity theft and obtaining a police report. You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file 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 North Carolina Residents: You are advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General.

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

For Rhode Island residents: Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.