

**IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY**

Dear [REDACTED]:

The privacy and security of the personal information we maintain is of the utmost importance to ProPath Services, LLC ("ProPath"). We are writing with important information regarding a recent data security incident that may have involved some of your information. ProPath is an anatomic and clinical pathology medical practice located in Dallas, Texas that performs laboratory and pathology testing services for patients it receives directly from ordering physicians as well as from other laboratories that do not perform the specific test requested. You previously had testing performed at the direction of your physician and one or more of those tests were referred by your physician to ProPath. We want to provide you with information about the incident and let you know that we continue to take significant measures to help protect your information.

What Happened?

We recently learned that as a result of a phishing attack, an unauthorized individual may have obtained access to a ProPath employee email account. Upon learning of the incident, ProPath disabled the impacted email account and required a mandatory password reset to prevent further misuse. There is no evidence that the purpose of the phishing campaign was to obtain patient information and we have no evidence that any of your information was actually acquired or used by the unauthorized individual. However, out of an abundance of caution, we are providing notice to you.

What We Are Doing.

Upon learning of this issue, we immediately secured the account and commenced a prompt and thorough investigation. As part of our investigation, we have worked very closely with external cybersecurity professionals. After an extensive forensic investigation and manual document review, we discovered on January 28, 2021 that the email account that was accessed between May 4, 2020 and September 14, 2020 contained some of your personal and/or protected health information.

Since the date of this incident, we have taken several steps to implement additional technical safeguards on our email system to prevent the recurrence of similar incidents. We have also implemented additional training and education for our employees to increase awareness of the risks of malicious emails, including how employees can identify and dispose of malicious emails.

What Information Was Involved.

The impacted email account contained some of your protected health information, including your [REDACTED].

What You Can Do.

We have no evidence that any of your information has been misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident. We have no evidence that your medical information involved in this incident was or will be used for any unintended purposes. However, the following practices can provide additional safeguards to help protect against medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your “explanation of benefits statement” which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

For More Information.

Please accept our apologies that this incident occurred. We have taken necessary steps to prevent this from happening again. We remain fully committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it and to prevent subsequent occurrences. We continually evaluate and modify our practices to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated toll-free response line at [REDACTED]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do if you are concerned about potential misuse of your information. The response line is available Monday through Friday, 8:00 am to 5:30 pm Central time.

Sincerely,



David Rose
Compliance Officer
ProPath Services, LLC