Boise, Idaho – November 4, 2022 – Givens Purlsey, LLP Notice of Data Security Incident

The privacy and security of the personal information we maintain is of the utmost importance to Givens Pursley LLP ("Givens Pursley").

We determined that unauthorized access to our network occurred on November 19, 2021. Upon learning of this issue, we immediately contained the threat and launched an investigation in consultation with outside cybersecurity professionals, which determined that an unauthorized party potentially removed a limited number of files and folders from our system.

After an extensive forensic investigation and manual document review, we discovered on September 8, 2022 that the files and folders that were potentially removed contained identifiable protected health information pertaining to a limited number of patients of Saint Alphonsus Health System,* such as full names, addresses, dates of birth, clinical and/or treatment information, medications information, medical provider information, patient identification numbers, and health insurance information. Not all information was included for all individuals.

Additionally, we further discovered on September 8, 2022 that the files and folders that were potentially removed contained personally identifiable information pertaining to a limited number of individuals, such as full names, dates of birth, Social Security numbers, driver's license numbers, financial account numbers, and payment card information. Not all information was included for all individuals.

On November 4, 2022 we notified individuals whose information may have been included in the files potentially acquired by the unauthorized party. Notified individuals have been provided with best practices to protect their information, and individuals whose Social Security numbers were contained in the impacted files have been offered complimentary credit monitoring.

Givens Pursley is committed to maintaining the privacy of personal information in our possession and has taken many precautions to safeguard it. Since the incident, we have worked with our Information Technology ("IT") managed services provider to implement additional security measures in an effort to prevent a similar event from occurring in the future.

For individuals who have questions or need additional information regarding this incident, or to determine if they are impacted and are eligible for credit monitoring, Givens Pursley has established a dedicated toll-free response line at **855-532-2135**. The response line is available Monday through Friday, 6:00 a.m. to 3:30 p.m. Pacific Time.

*This notification is being provided on behalf of the following entities to whom Givens Pursley is a Business Associate as defined under the Health Insurance Portability and Accountability Act ("HIPAA"):

- *Saint Alphonsus Health System*

– OTHER IMPORTANT INFORMATION –

1. Consider Placing a Security Freeze on Your Credit File.

We recommend that you place an initial one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax P.O. Box 105788 Atlanta, GA 30348 https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/ (800) 525-6285	***Experian*** P.O. Box 9554 Allen, TX 75013 https://www.experian.com/fraud/center.html (888) 397-3742	***TransUnion LLC*** P.O. Box 6790 Fullerton, PA 92834-6790 https://www.transunion.com/fraud-alerts (800) 680-7289

2. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 https://www.equifax.com/personal/credit-report-services/credit-freeze/ 1-800-349-9960	**Experian Security Freeze** P.O. Box 9554 Allen, TX 75013 http://experian.com/freeze 1-888-397-3742	**TransUnion Security Freeze** P.O. Box 2000 Chester, PA 19016 http://www.transunion.com/creditfreeze 1-888-909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

3. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by

phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If this notice letter states that your financial account information and/or credit or debit card information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

5. Protecting Your Medical Information.

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 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.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 515-281-5164.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 888-743-0023.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392