Notice of Data Breach

December 6, 2021

Oregon Anesthesiology Group, P.C. (OAG) experienced a cyberattack on July 11, after which we were briefly locked out of our servers. We were able to respond quickly to restore our systems from off-site backups, after which we began the process of rebuilding our IT infrastructure from the ground up. We also engaged the services of a cyber forensics firm, which started an investigation shortly after the attack.

On October 21, the FBI notified OAG that it had seized an account belonging to *HelloKitty*, a Ukrainian hacking group, which contained OAG patient and employee files. The FBI believes *HelloKitty* exploited a vulnerability in our third-party firewall, enabling the hackers to gain entry to the network. According to the cyber forensics report obtained by OAG in late November, the cybercriminals, once inside, were able to data-mine the administrator's credentials and access OAG's encrypted data.

Patient information potentially involved in this incident included names, addresses, date(s) of service, diagnosis and procedure codes with descriptions, medical record numbers, insurance provider names, and insurance ID numbers. OAG does not store patients' full medical records or their Social Security or credit card numbers, and these data were not involved. The cybercriminals also potentially accessed current and former OAG employee data,

including names, addresses, Social Security numbers and other details from W-2 forms on file.

Data security is a top priority at OAG, and we continually upgrade our security operations to address rapidly developing threats and minimize risks. We already had a broad range of restrictions and security measures in place to protect the sensitive information of our patients and employees. These measures included file encryption, access restrictions, activity alerts, website traffic reports, mandatory password resets and cyber training for all staff, in compliance with the Health Insurance Portability and Accountability Act.

Following the July attack but before we were notified of the account seizure by the FBI, we reevaluated and updated our network access control policies, replaced our third-party firewall and expanded the use of multifactor authentication. OAG also contracted with a third-party vendor for 24/7 real time security monitoring with live response, security system architecture advising, additional compartmentalization of sensitive data and increased use of cloud-based infrastructure.

The data breach potentially impacted about 750,000 patients and 522 current and former OAG employees. Although OAG has no evidence to suggest actual or attempted misuse of information as a result of this incident, we are notifying individuals who may have been affected.

As an extra precaution, we are providing the impacted individuals with access to identity protection services and credit monitoring. OAG has engaged Experian, a third-party privacy protection and fraud prevention company, to manage the mailing of the required notifications and provide call center services for identity protection and credit monitoring enrollment. OAG is offering all impacted individuals a complimentary 12-month membership to Experian's IdentityWorks (SM), which provides identity detection and resolution of identity theft. IdentityWorks services include credit monitoring, internet surveillance, identity restoration and up to $1 million in identity theft insurance.

All impacted individuals will receive a letter outlining the services that are being made available to them. For questions about the incident, please call Experian directly at (866) 666-2187 and reference engagement number B021858.

What Impacted Individuals Can Do

OAG recommends that potentially impacted individuals contact Experian to answer any questions they may have and be enrolled in the complimentary IdentityWorks (SM) program. Services include credit monitoring, internet surveillance, identity restoration and up to $1 million in identity theft insurance.

Potentially impacted individuals should keep an eye out if any of their personal information is shared. They should be wary of any mail that seems suspicious, such as notices from the IRS regarding taxes, medical insurance claims for unknown services or bills from unknown lenders. Impacted individuals should closely monitor financial accounts and set up alert features to keep them notified of any unusual events.

Also, a credit freeze can be placed with each credit bureau (Equifax, TransUnion and Experian) to help protect unwanted people from opening credit in your name. For anyone whose Social Security number was potentially accessed, creating a mySocial Security account with the Social Security Administration will allow them to claim their SSN.

Of note: individuals who have had a credit freeze put in place will need to lift it before creating a new mySocial Security account. More information can be found at ssa.gov/myaccount.

If individuals have received IRS correspondence indicating they may be a victim of tax-related identity theft or their e-file tax return was rejected as a duplicate, they should take these additional steps with the IRS:

- Submit an IRS Form 14039, Identity Theft Affidavit
- Continue to file your tax return, even if you must do so by paper, and attach the Form 14039
- Watch for any follow-up correspondence from the IRS and respond quickly

Individuals can further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps to protect their personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or their state Attorney General.

To report incidents of fraud and identity theft, you can contact the FTC at 1-877-ID-THEFT, through their website at http://identitytheft.gov, or in writing at Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20850, and your local Attorney General's Office.

Credit Bureau Contact Information

- TransUnion, 1-800-680-7289, transunion.com, PO Box 2000, Chester, PA 19016
- Experian, 1-888-397-3742, experian.com, PO Box 955, Allen, TX 75013
- Equifax, 1-888-298-0045, equifax.com, PO Box 105069, Atlanta, GA 30348

We encourage Oregon residents to report suspected identity theft to the Oregon Attorney General at:

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(877) 877-9392 (toll-free in Oregon)
(503) 378-4400

www.doj.state.or.us

Contact OAG
Return to main website