On or about December 21, 2018, a vendor of Beloit Health System (BHS") OS, Inc. ("OS"), learned of suspicious activity occurring within an OS employee's email account, which may impact the privacy of the personal information of some BHS patients. OS immediately launched an investigation and began working with forensic experts to determine the nature and scope of the suspicious activity. On February 20, 2019, the investigation confirmed an unauthorized actor gained access to its employee's email account from October 15, 2018 through December 21, 2018, utilizing account credentials harvested through a phishing email campaign. OS immediately took steps to secure the contents of the impacted account and ensure that the unauthorized actor no longer had access to the account.

The forensic experts were unable to confirm the specific messages or attachments within the email account that may have been subject to unauthorized access or acquisition. However, out an abundance of caution, OS began conducting a thorough and systematic review of the impacted email account, working to confirm the identities of the individuals whose information may have been accessible to the unauthorized actor. On April 5, 2019, OS notified BHS that patient information may be impacted by this event and subsequently confirmed the identities of the individuals whose information may have been accessible within the email account.

No medical records nor financial account information was impacted as a result of this event. The information contained in the email account of OS's employee affected by the event include: patient name, dates of service, patient account numbers and for a very small group of individuals, Medicare patient identification numbers (social security numbers). At this time, we have no evidence of any actual or attempted misuse of the information accessible within the email account.

We take this incident and the security of personal information seriously. Upon learning of this incident, OS immediately took steps to secure the email account and launched an in-depth investigation to determine the nature and scope of the incident. We are offering complimentary access to 12 months of Fraud Consultation and Identity Theft Restoration services through Kroll to all affected individuals. As an added precaution, we are also offering complimentary access to identity monitoring, fraud consultation and identity theft restoration services to the limited number of individuals who may have had social security numbers impacted by this event. Individuals who wish to receive these services must contact the dedicated assistance line listed below. As part of our ongoing commitment to the privacy of personal information in our care, we ensured that OS reviewed its existing policies and procedures and implemented additional safeguards to further secure the information in its systems. We will continue working to ensure that OS further secures the information in its systems going forward. We are also notifying regulatory authorities, as required.

Individuals seeking additional information regarding this event can call our dedicated assistance line at 1-866-775-4209, and the call center hours will be Monday through Friday, 8:00 a.m. to 5:30 p.m. Central Time, or you may call BHS directly at 1-888-655-5397 Monday through Friday from 8:00 a.m. to 4:30 p.m. Central Time. You may also write to OS at: W237 N2920 Woodgate Road, Suite 100, Pewaukee, WI 53072.

Best Practices

While we are unaware of any misuse of the personal information in the impacted email account, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian
PO Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com/credit-freeze

Equifax
PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:
1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center. html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-680-7289
www.transunion.com/fra ud-victim-resource/place-fraud-alert

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

Although we have no reason to believe that your personal information has been used to file fraudulent tax returns, you can contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to address a fraudulent tax return filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek

damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For Rhode Island Residents: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.