Benefis Health System is committed to providing the highest quality patient care, as well as protecting the privacy and confidentiality of our patients' information. Regrettably, we are writing to inform you of an incident involving some of your information.

What Happened

Earlier this year, we discovered that on certain dates between May 26, 2021 and July 15, 2021, your information may have been accessed by an unauthorized third party as a result of phishing emails sent to our employees. We discovered the potential for access shortly after the dates it may have occurred and acted immediately to cut off that potential access and further secure Benefis's email systems. We began a thorough internal investigation into what happened and whose information may have been involved. We also engaged a third-party forensics firm to help investigate and respond to this incident. Thorough and accurate investigation takes time, and we only recently confirmed that your information may have been involved.

What Information Was Involved

As part of our investigation, we determined that the information that could have been viewed by an unauthorized third party included demographic information (such as names, addresses, dates of birth, and Social Security numbers), clinical information contained in emails (such as diagnoses, conditions, medications, and admission and discharge dates), and certain financial information (such as banking details and credit card numbers). While we do not know for certain whether your information was viewed in the incident, we also cannot rule that out at this time.

To be clear, the incident did not impact our ongoing operations or diminish the patient care we provide.

What We Are Doing

As a result of our investigation, we have taken steps to prevent a similar event from occurring, including retraining our staff regarding identification and caution around phishing emails and implementing additional controls. In addition, we are conducting a thorough review of our security measures, internal controls, and safeguards.

We deeply regret that this incident has occurred. We have no reason to suspect that there has been any misuse or further release of your information, and we do not believe that your medical records or other information stored elsewhere at Benefis, including in patient portals for office visits and hospital stays, could have been accessed in the incident.

What You Can Do

We encourage you to remain vigilant against incidents of identity theft and misuse. We also encourage you to review your credit reports for suspicious activity and promptly inform your financial institution of any anomalies. Because we cannot rule out that financial information for some patients could have been viewed in the incident, we are offering you credit monitoring services through Experian IdentityWorks for 12 months at no cost to you. To activate your membership and start monitoring your personal information, please call **(855) 797-1895**. You must call and enroll by **February 28, 2022**. Be prepared to provide engagement number **B022146** as proof of eligibility for the identity restoration services by Experian. Please see the attached/enclosed information for more details.

In addition, please refer to the attachment titled Additional Resources for information about more steps that you can take to protect your identity.

If you have any questions regarding this incident, please call **(855) 797-1895** Monday through Friday, 7:00 a.m. to 9:00 p.m., Mountain Time, and Saturday and Sunday, 9:00 a.m. to 6:00 p.m., Mountain Time.

Sincerely,

Deborah McCracken
Chief Risk and Corporate Compliance Officer

Additional details regarding your 12-month Experian IdentityWorks Membership:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** 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.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at **(855) 797-1895**. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for 12 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

* Offline members will be eligible to call for additional reports quarterly after enrolling

** 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.

ADDITIONAL RESOURCES

The following provides additional information and actions you can consider taking to help protect your information. You may also contact the U.S. Federal Trade Commission ("FTC"), the credit reporting agencies, or your state's regulatory authority to obtain additional information about avoiding identity theft, including information about fraud alerts and security freezes, as further detailed below. Contact Information for the Federal Trade Commission and credit reporting agencies is set forth below:

Federal Trade Commission		
Federal Trade Commission Consumer Response Center 600 Pennsylvania Avenue, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft		
Credit Reporting Agencies		
Equifax P.O. Box 740241 Atlanta, GA 30374 1-800-525-6285 www.equifax.com	**Experian** P.O. Box 4500 Allen, TX 75013 1-888-397-3742 www.experian.com	**TransUnion** P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com

Order Your Free Annual Credit Report. You can order your free annual credit report online at www.annualcreditreport.com, by phone (toll free) at 877-322-8228, or by mail by submitting a completed Annual Credit Report Request Form to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can download a copy of the request form on the FTC website: www.ftc.gov. You can also visit the Consumer Financial Protection Bureau's website for more information on how you can obtain your credit report for free: www.consumerfinance.gov. Once you receive your credit reports, review them carefully for any 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 agency.

Review Your Accounts and Report Unauthorized Activity. We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the FTC. Carefully review your credit reports and bank, credit card, and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company. You may also consider filing or obtaining a police report.

We recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive regular explanation of benefits

statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the web site of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from potential identity theft, you may consider placing a fraud alert on your credit file. A fraud alert is intended to make it more difficult for someone to open a new credit account in your name. A fraud alert indicates to an entity requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the alert notifies the entity to take steps to verify your identity. You may contact one of the credit reporting agencies listed above for assistance.

Consider Placing a Security Freeze on Your Credit File. You also may consider implementing a security freeze (also called a "credit freeze"). Placing a freeze on your credit report restricts access to your credit report and will prevent lenders and others from accessing your credit report entirely. This means you (or others) will not be able to open a new credit account while the freeze is in place. You can temporarily lift the credit freeze if you need to apply for new credit. With a security freeze in place, you may be required to take special steps when you wish to apply for any type of credit. You may contact one of the credit reporting agencies listed above for assistance.

Remain Vigilant and Lookout for Phishing Schemes. We also encourage you to remain vigilant in managing and handling your information and be on the lookout for suspicious emails, such as phishing schemes. Phishing schemes are attempts by criminals to steal your information, including credit card numbers and Social Security numbers, over email. These attempts are often made by manipulating an email to make it look as if it came from a legitimate source, but which is actually sent by a fraudulent impersonator. Pay particular attention to anyone asking you to click on a link or attachment, especially if the email requests sensitive information, and pay close attention to the email address (e.g., look for misspellings). It is also important that you check the recipient's email address when replying to emails to ensure it is legitimate. Also consider taking steps such as carrying only essential documents with you, being aware of how and with whom you are sharing your information, and shredding receipts, statements, and other sensitive documents once you no longer need them.