Wellstar
HEALTH SYSTEM

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

[redacted]

[redacted]

[redacted]

Dear [redacted]

The privacy and security of the personal information we maintain is of the utmost importance to WellStar Health System ("WellStar"). We are writing with important information regarding a recent data security incident that may have involved some of your information. We want to provide you with information about the incident and let you know that we continue to take significant measures to protect your information.

What Happened?

WellStar was the target of an email phishing attack that resulted in a limited number of employees receiving a suspicious email containing a malicious link. Two (2) employees unfortunately fell victim to the phishing attack, resulting in an unauthorized individual gaining access to those employees' email accounts. Upon learning of the incident, WellStar disabled the impacted email accounts and required mandatory password resets to prevent further misuse.

There is no evidence that the purpose of the phishing attack 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 of this incident and offering you recommendations for protecting your information.

What We Are Doing.

Upon learning of this issue, we immediately commenced a thorough investigation. As part of our investigation, we have worked very closely with external cybersecurity professionals. After a comprehensive forensic investigation and manual document review, we discovered on February 7, 2022 that one or more of the email accounts that were accessed between December 6, 2021 and January 3, 2022 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 handle malicious emails.

What Information Was Involved.

The impacted email account(s) contained some of your protected health information, including your name, medical record number, WellStar account number unique to WellStar, and a clinical description of a laboratory test and result that was ordered by your provider. Your Social Security number and financial information were not included in the information that may have been accessed.

What You Can Do.

We have no evidence that any of your information has been misused or was impermissibly accessed. Nevertheless, out of an abundance of caution, we have chosen to make you aware of the incident. To protect against medical identity theft, we recommend that you follow these practices:

- 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.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-7755.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226.

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

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, https://oag.dc.gov/consumer-protection, Telephone: 202-442-9828.

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 and confidential toll-free response line that we have set up to respond to questions 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, 9:00 a.m. to 6:30 p.m. EST. (Excluding Major U.S. Holidays)

Sincerely,

[redacted]

WellStar Health System