Notice of Data Security Incident

Monongalia Health System, Inc., including its affiliated hospitals Monongalia County General Hospital Company, Stonewall Jackson Memorial Hospital Company and Preston Memorial Hospital Corporation (collectively, "Mon Health") is committed to enhancing the health of the communities it serves, one person at a time, and protecting the privacy and security of the information it maintains.

On December 30, 2021, Mon Health determined that a data security incident resulted in unauthorized access to information pertaining to Mon Health patients, providers, employees, and contractors. Mon Health first learned of the incident on December 18, 2021, when it was alerted to unusual activity in its IT network which disrupted the operations of some of Mon Health's IT systems. Upon learning of this, to protect its patients and secure its systems, Mon Health immediately took a significant portion of its IT network and systems offline and initiated downtime procedures. Mon Health also conducted an enterprise wide-password reset, implemented network hardening measures, notified law enforcement, and launched a comprehensive investigation, with the assistance of a third-party forensic firm.

Mon Health's investigation confirmed that this incident did **not** involve unauthorized access to Mon Health's electronic health records systems. Through the investigation, Mon Health determined that unauthorized parties accessed its IT network between December 8, 2021 and December 19, 2021. Mon Health's investigation cannot rule out the possibility that, while in its IT network, the unauthorized parties may have accessed files on IT systems that contain patient, provider, employee, and contractor information.

This information may have included the following information relating to patients and members of Mon Health's employee health plan: names, addresses, Social Security numbers, Medicare Health Insurance Claim Numbers (which could contain Social Security numbers), dates of birth, patient account numbers, health insurance plan member ID numbers, medical record numbers, dates of service, provider names, claims information, medical and clinical treatment information and/or status as a current or former Mon Health patient or member of Mon Health's employee health plan.

Beginning on February 28, 2022, Mon Health will mail notice letters to patients whose information may be involved in this incident.

Mon Health recommends that patients remain vigilant by reviewing their financial account statements for any unauthorized activity. If patients identify charges or activity they did not authorize, they should contact their financial institution immediately. Additionally, Mon Health encourages patients to review the statements they receive from their healthcare providers and health insurance plans. If patients see any services that were not received, they should contact the relevant provider or health plan immediately.

Mon Health deeply regrets any inconvenience or concern this incident may cause. To help prevent something like this from happening again, Mon Health has implemented, and will continue to adopt, additional safeguards and technical security measures to further protect and monitor its systems.

Month Health has established a dedicated, toll-free call center to help answer questions from individuals whose information may have been involved in this incident. If you have any questions about this incident, please call Mon Health's incident response line at (855) 568-2163, Monday through Friday, between 9:00am to 6:30pm, Eastern Time (except for on major U.S. holidays).

Frequently Asked Questions (FAQs)

What happened?

Mon Health experienced a data security incident which may have resulted in unauthorized access to information pertaining to Mon Health patients, providers, employees, and contractors.

While the investigation confirmed that this incident did **not** involve unauthorized access to Mon Health's electronic health records systems, Mon Health cannot rule out the possibility that, while in its IT network, the unauthorized parties may have accessed files on other IT systems that contain information relating to Mon Health's patients and health plan members.

Mon Health is now mailing notice letters to individuals whose information was contained within files which may have been accessed as a result of this incident.

How do you know Mon Health's patient records / systems are safe now?

Mon Health's response to this incident included taking a significant portion of its IT network and systems offline, the initiation of downtime procedures, an enterprise wide-password reset, and the implementation of network hardening measures. Mon Health methodically brought its systems back online once it confirmed that they were secure and that it was safe to do so.

Additionally, while Mon Health's investigation confirmed that this incident did **not** involve Mon Health's electronic health records systems, Mon Health has implemented, and will continue to adopt, additional safeguards and technical security measures to further protect and monitor its systems going forward.

What patient data was involved?

While the investigation confirmed that this incident did **not** involve unauthorized access to Mon Health's electronic health records systems, Mon Health cannot rule out the possibility that, while in its IT network, the unauthorized parties may have accessed files on other IT systems that contain information relating to Mon Health's patients.

This information may have included the following information relating to patients: names, addresses, Social Security numbers, Medicare Health Insurance Claim Numbers (which could contain Social Security numbers), dates of birth, patient account numbers, health insurance plan member ID numbers, medical record numbers, dates of service, provider names, medical and clinical treatment information and/or status as a current or former Mon Health patient.

Mon Health has begun mailing notices to individuals whose information may have been involved in the incident.

How is Mon Health responding?

Upon learning of this incident, to protect its patients and secure its systems, Mon Health immediately took a significant portion of its IT network and systems offline and initiated downtime procedures. Mon Health also conducted an enterprise wide-password reset, implemented network hardening measures, notified law enforcement and launched a comprehensive investigation. Finally, to help prevent something like this from happening again, Mon Health has implemented, and will continue to adopt, additional safeguards and technical security measures to further protect and monitor its systems.