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.

Notice of Data Security Incident

Monongalia Health System, Inc., including its affiliated hospitals Monongalia County General Hospital Company and Stonewall Jackson Memorial Hospital Company (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 October 29, 2021, Mon Health concluded its investigation of an email phishing incident which may have resulted in unauthorized access to emails and attachments in several Mon Health email accounts. Mon Health first became aware of the incident after a vendor reported not receiving a payment from Mon Health on July 28, 2021. In response, Mon Health promptly launched an investigation, through which it determined that unauthorized individuals had gained access to a Mon Health contractor's email account and sent emails from the account in an attempt to obtain funds from Mon Health through fraudulent wire transfers.

Upon learning of this, Mon Health secured the contractor's email account and reset the password, notified law enforcement, and a third-party forensic firm was engaged to assist with the investigation. The investigation confirmed that this incident was limited to Mon Health's email system and did **not** involve Mon Health's electronic health records systems. The investigation also found **no** indication that any of Mon Health's other affiliated hospitals or healthcare facilities, including Mon Health Preston Memorial Hospital and Mon Health Marion Neighborhood Hospital, were involved in or impacted by the incident. Importantly, the incident did **not** disrupt the services or operations of Mon Health or any of its affiliated hospitals or healthcare facilities.

Through its investigation, Mon Health determined that unauthorized individuals gained access to certain Mon Health email accounts between the dates of May 10, 2021 and August 15, 2021. In response, Mon Health secured the email accounts and reset their passwords.

Based on its investigation, Mon Health believes the purpose of the unauthorized access to the email accounts was to obtain funds from Mon Health through fraudulent wire transfers and to perpetrate an email phishing scheme, not to access personal information. That said, Mon Health cannot rule out the possibility that emails and attachments in the involved Mon Health email accounts containing patient, provider, employee, and contractor information may have been accessed as a result of this incident.

Thus, out of an abundance of caution, Mon Health conducted a comprehensive search of the contents of those email accounts to identify the information they contained. Through this search, Mon Health identified emails and attachments that contained the following information relating to patients and members of Mon Health's employee health plan: names, Medicare Health Insurance Claim Numbers (which could contain Social Security numbers), addresses, 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.

Beginning on December 21, 2021, Mon Health is mailing notice letters to patients whose information may be involved in this incident and has established a dedicated, toll-free call center to help answer questions from individuals whose information may have been involved in this incident.

Patients who receive notice letters are advised to review the statements they receive from their health care providers and health insurance plan. If individuals see services they did not receive, they should contact the 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 is continuing to review and enhance its existing security protocols and practices, including the implementation of multi-factor authentication for remote access to its email system.

If you have any questions about this incident, please call Mon Health's dedicated, toll-free incident response line at (855) 545-2461, 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 an email phishing incident which may have resulted in unauthorized access to emails and attachments in several Mon Health email accounts that contain patient, provider, employee, and contractor information.

Based on its investigation, Mon Health believes the purpose of the unauthorized access to the email accounts was to obtain funds from Mon Health through fraudulent wire transfers and to perpetrate an email phishing scheme, not to access personal information. That said, Mon Health cannot rule out the possibility that emails and attachments in the involved Mon Health email accounts may have been accessed as a result of this incident.

Thus, out of an abundance of caution, Mon Health conducted a comprehensive search of the contents of those email accounts to identify the information they contained. Mon Health is now mailing notice letters to individuals whose information was contained in emails and attachments that may have been accessed as a result of this incident.

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

The investigation confirmed that this incident was limited to Mon Health's email system and did **not** involve Mon Health's electronic health records systems. Additionally, Mon Health is further securing its email environment by implementing multi-factor authentication for remote access to its email system.

What patient data was involved?

Based on its investigation, Mon Health believes the purpose of the unauthorized access to the email accounts was to obtain funds from Mon Health through fraudulent wire transfers and to perpetrate an email phishing scheme, not to access personal information. That said, Mon Health cannot rule out the possibility that emails and attachments in the involved Mon Health email accounts may have been accessed as a result of this incident.

Thus, out of an abundance of caution, Mon Health conducted a comprehensive search of the contents of those email accounts to identify the information they contained. Through this search, Mon Health identified emails and attachments that contained the following information relating to patients and members of Mon Health's employee health plan: names, Medicare Health Insurance Claim Numbers (which could contain Social Security numbers), addresses, 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.

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

How is Mon Health responding?

Mon Health is continuing to review and enhance its existing security protocols and practices, including the implementation of multi-factor authentication for remote access to its email system.