Aultman/AultWorks
CYBER INCIDENT
Answers to Potential Questions

Incident Details-What Happened

On March 28, 2018, during an investigation of a security incident, Aultman's Information Technology Department learned that unknown individuals had accessed several Aultman email accounts without authorization. Aultman immediately began working with outside information security experts to verify the nature and scope of the incident. Based upon the investigation, Aultman determined that access to the compromised email accounts happened between February and March of 2018. The extent of the access and whether emails and attachments were actually viewed remains unclear. In an abundance of caution, however, Aultman is making this information public because some of the email accounts contained information about some patients of Aultman Hospital and the Aultman physician practices listed in Attachment A ("Aultman"). Additionally, certain individuals who had employment-related examinations and tests with AultWorks Occupational Medicine had information in one of the email accounts. All of these individuals are being notified with recommendations on steps they should take to protect their personal information that might have been affected.

To date, we have no evidence of any actual or attempted misuse of information as a result of this incident.

Frequently Asked Questions Relating to Incident

ABOUT THE BREACH

Q – When did Aultman first learn of this incident and how?

A: Microsoft alerted Aultman on March 28, 2018, that certain email accounts might have been compromised. While conducting a follow-up investigation, we discovered that additional email accounts had been accessed without authorization. Our staff then worked with outside security experts to identify and confirm which email accounts had been accessed without authorization and the scope of the access.

Q – How many people were impacted?

A: Approximately 43,000 individuals were potentially affected.

Q – How many computers were involved?

A: None of the software systems that store the electronic health records for Aultman patients were affected by this incident.

Q – Was the data encrypted?

A: The data stored in the email accounts was not encrypted.

PATIENT INFORMATION

Q – Whose information was compromised?

A: Certain current and former patients of Aultman Hospital and some of its physician groups, as well as individuals for whom AultWorks Occupational Medicine conducted employment-related physical examinations and testing.

Q – How do you know what data was contained in the email accounts?

A: We used a nationally recognized forensic computer investigative team who worked closely with our team to conduct a detailed review of the records that were maintained in the affected email accounts. As a result, we were able to determine which email accounts contained protected health information and whose data was contained in the emails.

Q – What protected health information was involved in the incident?

A: Various types of information were included for different individuals based on their relationship with Aultman. Protected health information that was potentially compromised may have included name, address, date of birth, Social Security Number, driver's license number, diagnostic information, and medical histories, as well as physical, drug, hearing, and breathing test results.

Q –Was my Social Security number contained on one of the affected email accounts?

A: If you received a letter indicating that there may have been unauthorized access to your protected health information, including your Social Security number, then your Social Security number or your Driver's License number was included in the email accounts involved in the incident. If your letter does not state that your Social Security number was included in the protected health information that may have been subject to unauthorized access, then your Social Security number was not included in the accounts involved in the incident.

Q – Why were Social Security numbers in the email accounts?

A: Employers that use AultWorks often use SSNs to identify employees and potential employees in connection with testing.

Q – Why was my data in the email accounts?

A: **For recipients of AultWorks letter**: A business that you have been or are currently employed by or that you sought employment with uses AultWorks for testing.
A: **For recipients of Aultman letter**: The account that was accessed contained information related to patients of Aultman's physician practices or Aultman Hospital.

Q – Do you suspect that any information has been used fraudulently?

A: The extent of the access and whether emails and attachments were actually viewed remains unclear. To date, we have no evidence of any actual or attempted misuse or fraudulent use of information as a result of this incident. However, that is why the patient notification letter recommends certain steps that individuals should take to safeguard their data and monitor it for misuse.

Q – Why did it take Aultman so long to notify me?

A: Aultman needed to review a large number of records in order to: (1) verify that your personal information was stored on the impacted email accounts; (2) determine whether Aultman needed to provide notice; and (3) determine the identity and address of those people requiring notice. Because of the diversity and complexity of the potentially affected data and the detailed analysis required, it took time to identify files that might have been exposed and to confirm the nature of the information that the files contained. Obtaining current contact information for potentially affected individuals, preparing and mailing notification letters to alert them of this incident, and setting up a toll-free call center required additional time. Aultman worked diligently to complete these tasks as rapidly and thoroughly as possible while at the same time meeting all of its legal requirements.

Q – Has anyone been adversely affected as a result of their information being accessed?

A: At this time, we have no indication this information has been misused or there has been an adverse effect on any individual. We believe that it is unlikely that this information has been accessed or used, since no person has reported an event that would indicate this information has been accessed or used.

Q – I was never a patient at Aultman. Why does Aultman have my name and other personal information?

There are a number of reasons why Aultman may have this information, including:

- You may have been a patient of one of Aultman Medical Group's physician practices; and/or
- You may have been examined or tested for work-related purposes at Aultman or by an Aultman physician.

AULTMAN'S ACTION STEPS

Q – What's being done to prevent this from occurring again?

A: We are continually working to enhance our systems and practices to reduce the likelihood of such events happening again. Keeping our data secure from unauthorized access is a top priority for us. We are continuing to:

- Enhance our information systems with the latest security protections;
- Conduct an ongoing, comprehensive information security assessment to help prevent future cyber incidents;
- Enhance our email systems with additional reporting and blocking of foreign locations;
- Increase auditing of email accounts and related activity;
- Strengthen email complexity requirements for passwords;
- Conduct mandatory training to enhance privacy awareness and fraudulent email practices being used to obtain information;
- Review and revise our policies and procedures on data security and privacy.

Q – Have the issues that caused the incident been eliminated from Aultman's email accounts?

A: Aultman believes it was successful in enabling enhanced security features and altering account credentials to prevent any further unauthorized access. Aultman is encouraged that this is working because it has not seen any further incidents of unauthorized access. Aultman has committed to preventing these types of situations and continues to invest in the processes and systems to assure that something like this does not happen again.

WHAT CAN SOMEONE DO

Q – How would someone know if their identity was stolen?

A: Aultman has arranged with Experian to provide free credit monitoring to all persons whose Social Security numbers or driver's license numbers were in the email account involved in the incident.

Q –Has my family been impacted by this incident?

A: No. Only your personal information was found in the email accounts.

Q – Does this mean that I'm a victim of identity theft?

A: No. The fact that information was potentially illegally accessed does not mean you are a victim of identity theft or that the information has been accessed to commit fraud. Aultman wanted to let you know about the incident in accordance with law and so that you can take appropriate steps to help protect your identity. A good way for you to help protect yourself is to remain vigilant by periodically reviewing your credit reports, banking accounts and remaining alert to unusual situations.

Q – Should I close my bank account or cancel my credit cards?

A: At this time, Aultman is not aware of any unauthorized access to bank account or credit card information. However, Aultman recommends that you remain vigilant by monitoring your bank and credit card statements and report any irregularities to your financial institution.

Q – Should I contact the Social Security Administration to change my Social Security number if my Social Security number was part of the information that was contained on the compromised servers?

A: The Social Security Administration is unlikely to change your Social Security number in the absence of any evidence that your Social Security number is actually being misused. In addition, according to information on the Social Security Administration's website, changing your Social Security number may create additional problems because you would lose your existing credit history and because other government agencies (including the Internal Revenue Service and the Department of Motor Vehicles) and private businesses (such as banks and credit reporting companies) are likely to have records under your current Social Security number.

Q – Should I notify the IRS?

A: The IRS Taxpayer Guide to Identity Theft advises that if your tax records are not currently affected by identity theft, but you believe you may be at risk due to a lost/stolen purse or wallet, questionable credit card activity or credit report, etc., you can contact the IRS Identity Protection Specialized Unit at 1-800-908-4490. See additional information at http://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft.

Q – How do I put a security freeze in place?

A: You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. Fees vary based on where you live, but commonly range from $3 to $15. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348

1-800-685-1111
https://www.freeze.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/

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

Q – What should someone do if they believe their personal information has been used fraudulently?

A: They should immediately: (1) report the crime to their local law enforcement agency, (2) contact any creditors involved, and (3) notify all three credit bureaus. They may also choose to put a credit freeze on their file, but please note that there may be a cost associated with this. Additional guidance is available on the Federal Trade Commission's website at http://www.ftc.gov/bcp/edu/microsites/idtheft.

CREDIT MONITORING

Q – How can I activate my free credit monitoring?

A: If your Social Security number or driver's license number was in the email accounts involved in the incident, you would have received a letter from Aultman which explained the steps to enroll in free credit monitoring through a complimentary one-year membership to Experian IdentityWorks Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. Information regarding how to activate this free service is included in the attachment to the notice letter you received from Aultman together with an activation code for you.

Q – My information was in the email accounts affected by the incident but my notice letter did not include an offer for free credit monitoring. Why not?

A: If you did not receive an activation code, then your Social Security number or driver's license number was not found in the email accounts that were affected by the incident. Credit monitoring informs you after an unauthorized account has been opened or there are other changes to your credit report. The health information contained in the email accounts would not be used to open a new account and therefore credit monitoring would not be of much help. As a precautionary measure Aultman recommends that you monitor your Explanation of Benefits and other medical insurance statements for any activity that you have not authorized. If you suspect

that someone else has used your insurance information, you should contact local law enforcement and Aultman.

Q – I did not receive a notification letter. Does this mean that my personal information was not compromised?

On May 25, 2018, Aultman sent letters to the last known home address of every individual believed to be affected by this incident and for whom Aultman had address information. If you received a letter, it will specify what elements of your personal information are affected. If you have moved recently and you think Aultman does not have your current address please call the toll-free call center assisting Aultman at 855-804-8585. The call center is available to answer your phone call, between 9:00 a.m. and 9:00 p.m. Eastern Standard Time, Monday through Friday, until August 27, 2018. You also can send any questions not answered in these FAQs directly to Aultman at compliance@aultman.com and an Aultman employee will contact you.

If you did not change your address and did not receive a letter, there is no reason to believe that your information is at risk.

ATTACHMENT A
AULTMAN PHYSICIAN PRACTICES

AMG Canton Urology
AMG Endocrinology
AMG General Surgery
AMG Gynecologic Oncology
AMG Hematology and Oncology
AMG Internal Medicine Center- Richard Jones, M.D.
AMG Podiatry
AMG- Waynesburg Family Medicine
Aultman Behavioral Health & Counseling Center
Aultman Louisville Internal Medicine
Aultman North Canton Medical Group- Bolivar Campus
Aultman North Canton Medical Group -Family Medicine of North Canton
Aultman North Canton Medical Group- Internal Medicine- Main Campus
Aultman Physician Center
Breast Surgery Specialists
Canton Plastic Surgeons
Cardiovascular Consultants
Dunlap Family Physicians
Family Medicine of Carrollton
Heart Core
Dr. Kevin Hill, M.D.
Hills and Dales Family Practice
North Canton Medical Center- Dr. Steven Weaver M.D.
Dr. Jean-Claude Tabet, M.D.
Dr. Mark Weiner, M.D.
Women's Health Services -Dr. Amelia Laing