University Gastroenterology Notifies Patients of Data Security Incident

PROVIDENCE, RI – September 9, 2016 – University Gastroenterology ("UGI") has become aware of a data security incident that may have resulted in the inadvertent exposure of the personal and protected health information of some patients. Although at this time there is no evidence of any attempted or actual misuse of anyone's information as a result of this incident, we have taken steps to notify our patients and provide resources to assist them.

On July 11, 2016, we discovered that an unauthorized individual had gained access to an electronic file storage system from a practice we acquired in 2014, Consultants in Gastroenterology, and encrypted several files. We immediately took action to secure our system and conducted an investigation to determine what information was contained in those files. We determined that some files may have contained patient names, addresses, dates of birth, Social Security numbers, and medical billing information. Patients' electronic medical records were not exposed and remain secure.

We take the privacy and security of personal information very seriously, have already taken steps to prevent a similar event from occurring in the future, and are making additional security enhancements to protect the privacy and security of patient information. This includes deploying an enhanced anti-malware solution to every computer and server within our system, disabling inactive user accounts, and removing the affected servers from our network.

We mailed a letter to individuals potentially impacted by this event which includes steps patients can take to monitor and protect their personal information. We also have established a toll-free call center to answer patient questions about the incident and related concerns. The call center is available Monday through Friday from 9:00 a.m. to 9:00 p.m., Eastern Time and can be reached at (844) 575-7459. In an abundance of caution, we are offering at no cost to impacted individuals access to credit monitoring and identity theft resolution services through Equifax. Additional information and recommendations for protecting personal information can be found below.

The privacy and protection of patient information is a top priority for UGI, and we deeply regret any inconvenience or concern this incident may cause.

Questions and Answers about the Incident

What happened?

On July 11, 2016, we discovered that an unauthorized individual had gained access to an electronic file storage system from a practice we acquired in 2014, Consultants in Gastroenterology, and encrypted several files. We immediately took action to secure our system and conducted an investigation to determine what information was contained in those files.

What is University Gastroenterology doing about this incident?

We are conducting a thorough response, including notifying those potentially impacted, providing resources to assist them, and taking action to secure our system. We sent letters notifying patients whose information was contained in the potentially exposed records, and set up a toll-free call center to assist with questions. The call center is available Monday through Friday from 9:00 a.m. to 9:00 p.m., Eastern Time and can be reached at (844) 575-7459.

We have already taken steps to prevent a similar event from occurring in the future, and are making additional security enhancements to protect the privacy and security of patient information. This includes deploying an enhanced anti-malware solution to every computer and server within our system, disabling inactive user accounts, and removing the affected servers from our network. The privacy and protection of patients' personal information will continue to be a top priority for us.

When did this happen?

We learned of the situation on July 11, 2016, and we promptly took action to secure our system. In addition, we began an examination to determine the specific patients and information that was contained in these records.

Why did it take time to notify patients?

Our examination involved a thorough and lengthy process to accurately identify what information was contained in the patient records and the individuals potentially affected, and to confirm current contact information for the letters. Additionally, we partnered with Equifax to arrange free identity protection services for our patients.

What personal or medical information may have been exposed?

Some files may have contained patient names, addresses, dates of birth, Social Security numbers, and medical billing information. Patients' electronic medical records were not exposed and remain secure

Has any of this patient information been misused or stolen? Is anyone a victim of identity theft as a result of this incident?

At this time we are not aware of any attempted or actual misuse of any patient's information as a result of this incident. However, we suggest you enroll in the identity protection services being offered through Equifax, which we are providing – free of charge.

I did not receive a notification letter. How do I find out if my information was potentially exposed?

Only those individuals' whose information was potentially exposed were sent a letter. Please call the toll-free call center, and they can help determine if you are potentially affected. The call center is available Monday through Friday from 9:00 a.m. to 9:00 p.m., Eastern Time and can be reached at (844) 575-7459.

The following information is provided to help patients or others wanting more information on steps they can take to protect themselves:

What steps can I take to protect my personal information?

- If you detect any suspicious activity on any of your accounts, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities.
- Obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies. To order your credit report, free of charge once every 12 months, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting agencies is included in the e-mail and letter, and is also listed at the bottom of this page.
- Please notify your financial institution immediately of any unauthorized transactions made or new accounts opened in your name.
- You can take steps recommended by the Federal Trade Commission to protect yourself from identify theft. The FTC's website offers helpful information at www.ftc.gov/idtheft.
- Additional information on what you can do to better protect yourself is included in your letter.

What should I do to protect myself from payment card/credit card fraud?

The incident did not involve any credit or debit card information. However, we suggest you review your debit and credit card statements carefully for any unusual activity. If you see anything you do not understand or that looks suspicious, you should contact the issuer of the debit or credit card immediately.

How do I obtain a copy of my credit report?

You can obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies. To order your credit report, free of charge once every 12 months, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting agencies is included in the e-mail and letter, and is also listed at the bottom of this page:

How do I put a fraud alert on my account?

You may consider placing a fraud alert on your credit report. This fraud alert statement informs creditors to possible fraudulent activity within your report and requests that your creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact Equifax, Experian or TransUnion and follow the Fraud Victims instructions. To place a fraud alert on your credit accounts, contact your financial institution or credit provider. Contact information for the three nationwide credit reporting agencies is included in the e-mail and letter, and is also listed at the bottom of this page.

Contact information for the three nationwide credit reporting agencies is as follows:

Equifax Security Freeze	Experian Security Freeze	TransUnion (FVAD)
PO Box 105788	PO Box 9554	PO Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
1-800-685-1111	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.com	www.transunion.com