A Notice to our Patients

Ridgeview Institute is notifying individuals of an incident that involved the personal information of some of its patients.

What happened? On or about January 14, 2020, we became aware of an incident where an employee of Ridgeview Institute, who has since been terminated, copied and emailed documents of Ridgeview Institute and its patients to a personal email account. The former employee disclosed these electronic documents and emails to an unauthorized third party and an attorney.

Upon discovery of the incident, Ridgeview Institute performed an internal investigation of what happened and conducted an extensive review of the documents forwarded by the former employee. Ridgeview Institute also hand reviewed individual documents, emails, and attachments in order to identify individuals whose information may have been forwarded by the former employee.

What information was involved? On April 1, 2020, Ridgeview Institute was provided a listing of the potentially affected individuals whose information was contained within the documents and emails forwarded by the former employee. The information contained in these documents may have included full names, dates of birth, social security numbers, patient identification numbers, names of insurers, and diagnosis and treatment information which may include the names of treating physicians, medical procedures, prescriptions, lab and/or other test results.

What are we doing? Ridgeview Institute values the privacy and security of patient information and is continuing to take steps to enhance its security measures to prevent something like this from happening in the future. We are attempting to notify by letter those patients for whom we have mailing addresses. We are also offering complimentary identity theft protection services for those individuals whose financial data may have been included within the documents forwarded by the former employee.

The former employee has admitted to taking these documents. Fortunately, the former employee has acknowledged that the documents were only produced to one unauthorized third party and her attorney and that any additional copies of the documents in the former employee's possession have been destroyed. We have also obtained assurances from the unauthorized third party who received the documents that the documents will not be shared with any additional third parties.

What can you do? We recommend affected persons activate the protection services offered and otherwise remain vigilant and monitor account statements and credit reports carefully and report discrepancies to law enforcement. Fraud alerts and security freezes also can be activated to help protect individuals.

For more information or if you have any questions or concerns, please call toll-free (844) 989-2768 Monday through Friday (excluding holidays), between 9:00 a.m. and 6:30 p.m. Eastern Time. We sincerely apologize for any concern this incident may have caused.