FABEN Obstetrics and Gynecology
836 Prudential Dr Suite 1506
Jacksonville FL 32207

«AddressBlock»

January 14, 2019

Re: Notification of Breach

Dear Patient:

On Wednesday November 21, 2018, FABEN Obstetrics and Gynecology, LLC ("FABEN") experienced and detected a ransomware infiltration.

The ransomware infected a server that maintained files created from January 2007 through April 10, 2017. The ransomware that infected the server is commonly known as "GandCrab." Once GandCrab accesses a particular file, it encrypts that file and demands a payment to decrypt the file. In other words, the ransomware converts the file into a non-readable form that requires a key to return it to its original plain text form. To mitigate the effects of the ransomware attack, FABEN deleted the infected files.

The ransomware did not exfiltrate any files. In other words, third parties were never able to access, nor were they sent, any of the data, patient records, or other files on the server. Once in the server, the ransomware encrypted records.

The ransomware only encrypted certain files created between January 2007 and April 10, 2017. Most patient records were backed up and are being quickly restored. Recovered files include clinical electronic medical records created between 2007 and April 2014. These files contain diagnosis and treatment information concerning the medical services (e.g., patient visits, labor and delivery) provided to patients.

Unfortunately, certain records are not recoverable. Non-recoverable records include any items that were manually scanned by FABEN into patient medical records and certain information for medical charts created between September 11, 2014 and April 10, 2017. These files include, but are not limited to, blood sugar logs, blood pressure logs, Family and Medical Leave Act documentation, and medical records that patients provided to FABEN in paper form during the aforementioned period of time.

Out of an abundance of caution, all patients from September 11, 2014 through April 10, 2017 are receiving this notification. Receipt of this notification does not necessarily mean that any of your records were compromised; however, there is a possibility that certain files concerning your care and information, as described above, were deleted and/or compromised as a result of the ransomware attack.

FABEN is conducting a thorough investigation in collaboration with local and federal law enforcement agencies to determine the source and ultimate extent of the ransomware attack.

Since the infected files were encrypted but not exfiltrated, there is no increased risk of identity theft, nor is there an increased risk that a third party may view your protected health information at this time as a result of the ransomware attack. However, there are certain steps you should take to avoid further issues concerning your protected health information:

1. Maintain copies of all records that you brought to FABEN in paper form concerning your treatment and care.
2. Contact FABEN with any questions or concerns about the medical records that were compromised as a result of the ransomware attack.
3. Many of the records affected during the applicable time period were records brought in by patients, for example, from a previous OB/GYN provider, primary care physician, laboratory service provider, or employer. To the extent any records are missing, as determined in consultation with FABEN, please contact the third-party source of the records to obtain such records.

FABEN intends to continue to work with law enforcement and private security consultants to protect your health information and to maintain the integrity of your records. FABEN has already utilized additional backup servers and implemented additional security procedures.

We will continue to provide quality medical care to our patients. If you have any questions or would like to learn additional information about this matter, please contact FABEN at **1-800-733-0194**.

Sincerely,

FABEN Obstetrics and Gynecology