OceanViews Optical
and Jennifer L Loar OD PA

November 9, 2022

Dear Patient,

I am writing to let you know about a recent computer breach that encrypted part of our database.

Sometime on Saturday October 8, there was a shut down of our office software. The following Monday morning, the disruption revealed its source. Ransomware, the Venus Virus had encrypted our database. Servers were shut down immediately and assessment began. It was obvious within the first several hours that this ransomware virus had encrypted the database and caused corruption bridging into the two external hard drives and back up server. So there was not immediate back up database. We utilized paper charts for the next 9 days.

Investigation revealed a gap in our database from July 2021 to October 8, 2022. That gap in database is encrypted and has been stored securely for future recovery. When decryption is discovered for this particular ransomware, the data will be restored to the current database.

The following personal information is stored in our database:

Name
Nickname
Address
Phone numbers
Date of birth
Email
Ethnicity
Preferred language
Insurance
Medical diagnosis
Medications
Allergies to medications
Reports
Eyeglass orders
Contact orders

It's important to tell you that we:

DO NOT STORE SOCIAL SECURITY NUMBERS
DO NOT STORE PAYMENT INFORMATION; NO CREDIT CARDS NOR BANK INFO

I have reported the incident to the necessary authorities that track ransomware; CISA, FBI, HHS.gov and IC3. I have met in person with an FBI agent cyber security division and he took an encrypted hard drive for investigation and hopefully decryption. I have a meeting later today with a representative of hhs.gov.

I have had our servers replaced and reconfigured. New virus, malware, ransomware programs have been implemented. Server, backup server, virtual server and external hard drives are set up. The FBI cyber division agrees that this is very good security.

It is unlikely that the database was exported since ransomware is used to encrypt a database and demand payment or corrupt the database. I did not pay the ransom, instead I chose to scrap the servers and resume with backup database.

It is always wise to monitor our credit. There are numerous ways. Experian has free credit monitoring, for example. https://www.experian.com/consumer-products/credit-monitoring.html

I am disappointed that this faceless Venus Virus has entered into my office. You know I value my beloved patients. I am giving my email below for you, if you have questions or comments. I will answer as promptly as I can. Please contact me via email rather than calling the front desk.

DrLoar@OceanViewsOptical.com

Sincerely,

Dr. Jennifer Loar