<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

NOTICE OF DATA BREACH

Attention: Please note, this letter is intended to inform you of two, distinct data breaches.

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

As of May 19, 2022, Spectrum Eye Physicians ("Spectrum") has been made aware of two separate events, each of which may constitute a potential breach of certain patient records and information that may be considered electronic Protected Health Information ("ePHI") pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). Both breaches involve the systems of Spectrum's third-party vendor, Eye Care Leaders ("ECL"). The first potential breach resulted from a vulnerability in the Alta Payment Portal of ECL's billing system. The second potential breach resulted from a ransomware attack on the databases of ECL's electronic medical record ("EMR") system. In accordance with Spectrum's requirements under HIPAA and California law, we have provided the details of each breach below.

(1) DATA BREACH: ALTA PAYMENT PORTAL

What Happened?

On May 19, 2022, Spectrum received notice from ECL concerning a potential breach of certain Spectrum patient information that may be considered ePHI pursuant to HIPAA. The breach resulted from a vulnerability in the ECL Alta Payment Portal, a vulnerability which had actually been discovered by a patient of Spectrum (among others). Spectrum notified Alta Billing, the billing service subsidiary of ECL ("Alta"), that one of its patients contacted Spectrum to inform them that, when the patient made payment on the Alta Payment Portal, he/she was able to see the payment receipt of (what he/she assumed was) another patient. Spectrum immediately informed Alta of the information leakage on October 26, 2021. Alta assured Spectrum that it would investigate the issue and follow-up if it was determined that the vulnerability affected more than this single user.

Spectrum did not hear further from Alta until the May 19, 2022 notice. According to the notice, immediately upon being alerted to this vulnerability in its payment system, Alta retained an incident response team to investigate and remedy the vulnerability. Upon investigation, the response team discovered that it was possible to alter the website URL for the Alta Payment Portal, which allowed for unauthorized access to the payment receipts for patients who paid through the portal. After confirming this vulnerability, Alta acted immediately to remedy the issue by taking the system offline to prevent further potential unauthorized access to these transaction receipts.

As of this writing, Alta's findings indicate that the data visible due to this vulnerability was not subject to manipulation or editing, and that only one payment receipt was visible at a time as each receipt required a different URL modification. However, to date, Alta maintains that it lacks sufficient evidence to rule out the possibility that all Alta transaction receipts prior to its remedial action were accessed or otherwise acquired by unauthorized individuals, who may have exploited the vulnerability. Accordingly, until we are informed otherwise, we are presuming that a breach occurred and are writing to provide you with the information that we currently have available, as well as steps you can take to protect yourself from further harm (at the conclusion of this letter).

What Information Was Involved?

Based on the investigation, Alta has found that the following types of information were potentially compromised as a result of the vulnerability:

(i) For credit card transactions - transaction date and time, transaction identification number, patient name, statement numbers, last four digits of the credit card used to process the transaction, the amount processed, an email address associated with the transaction, and information input by the user in a comments section; and

(ii) For bank account transactions – transaction data, patient name, transaction identification number, last four numbers of the bank account used in the transaction, an email address associated with the transaction, and information input by the user in a comments section.

What We Are Doing.

Alta's investigation is ongoing and we are hopeful that the investigation will soon provide more specific information regarding the exact PHI that was accessed. In the interim, Spectrum is working under the assumption that a breach occurred and is fulfilling its obligations as a covered entity under HIPAA. In addition to providing individual notice to all of its patients whose PHI may have been maintained in the Alta Payment Portal, it is notifying the local media (via press release) of the potential data breach, it is filing a Breach Report with the Office for Civil Rights ("OCR") and it is communicating with its legal counsel to determine what, if any, recourse it has against Alta and ECL concerning this breach. It has also made the decision to terminate its Alta billing services contract and transfer its patient billing records to another billing vendor.

(2) DATA BREACH: MYCARE INTEGRITY EMR

What Happened?

On March 1, 2022, Spectrum received a Notice of Data Breach from ECL informing the practice of a potential breach of certain patient records and information that may be considered ePHI pursuant to HIPAA. The breach resulted from a ransomware attack on the databases of ECL's myCare Integrity EMR system (the "Integrity EMR"). ECL has estimated the date of the information leakage to be December 4, 2021, but was unable to confirm that ePHI was involved until the March 1, 2022 notice. As of this writing, ECL continues investigating the ransomware attack in order to determine the exact scope of the data breach. It is possible that, although certain ePHI records were deleted, they may not have been accessed, used or disclosed through the ransomware attack. According to ECL, the containers in which the PHI databases are stored are protected by encryption. The database tables themselves, however, are not encrypted at rest. Therefore, ECL cannot confirm or deny whether the PHI was accessed. Until we are informed otherwise, we are presuming that a breach occurred and are writing to provide you with the information that we do have, as well as steps you can take to protect yourself from further harm (at the conclusion of this letter).

On or around December 4, 2021, cyber attacker(s) acquired "full access" to the Integrity EMR hosted on Amazon Web Services ("AWS") and deleted certain databases and system configuration files, including those containing PHI. The evidence indicates that the attacker accessed the Integrity AWS environment and executed several "delete" commands on December 4, 2021, between 7:18 PM ET and 7:29 PM ET, followed by a break in activity, then another "delete" event occurred at approximately 10:13 PM ET. The attacker also executed several "discover" commands to locate files within the Integrity EMR. No other command actions were evidenced during the attack timeframe.

ECL detected the activity in less than twenty-four (24) hours and ECL's incident response team contained and began investigating the incident immediately upon discovering it. ECL's response team immediately disabled the attack instance, revoked access to it, and forced system password changes. ECL also updated and changed several additional security features within the environment. Shortly after stopping the attack, ECL also began efforts to restore deleted files and databases from backups to limit customer impact to the availability of its patients' PHI. ECL identified and restored available backups for many of the deleted databases. Work is ongoing to determine whether the remaining, unrestored databases can or need to be restored.

What Information Was Involved?

As of this writing, due to the methods of the attack and the limited log evidence available, ECL's incident response team is unable to limit the scope of data that may have been compromised. Although ECL investigators have not identified any evidence that PHI was acquired or transferred outside of the Integrity EMR, there is insufficient evidence to allow investigators to conclude that such acquisition and transfer could not have occurred during the attack. Further, ECL's investigation to date has not revealed any evidence that allows ECL to determine which specific patient information or data within the Integrity EMR system was accessed. As such, ECL has informed Spectrum to assume that this attack impacted all ePHI that was stored on the Integrity EMR.

What We Are Doing.

ECL's investigation is ongoing and we are hopeful that the investigation will soon provide more specific information regarding the exact PHI that was accessed. In the interim, Spectrum is working under the assumption that a breach occurred and is fulfilling its obligations as a covered entity under HIPAA. In addition to providing notice to all of its patients whose PHI was maintained in the Integrity EMR, it is notifying the local media (via press release) of the data breach, it is filing a Breach Report with OCR and it is communicating with its legal counsel to determine what, if any, recourse it has against ECL concerning this breach. It has also made the decision to terminate its Integrity EMR contract with ECL and transfer its patient PHI to another EMR vendor.

The Following Recommendations Apply for Both the Alta Payment Portal and myCare Integrity EMR Data Breaches Detailed Above:

What You Can Do.

To protect from potential harm resulting from the breaches detailed above, we encourage all of our patients to immediately take the following steps:

- Call one of the toll-free numbers listed below to place a fraud alert on your credit report. This can help prevent an identity thief from opening additional accounts in your name. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will automatically be notified to place alerts on your credit report, and all three credit reports will be sent to you free of charge.
    - Equifax: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241.
    - Experian: 1-888-397-3742; www.experian.com; P.O. Box 9532, Allen, TX 75013
    - TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790
- When you receive your credit report, examine it closely and look for signs of fraud, such as credit accounts that are not yours.
- Continue to monitor your credit reports. Even though you placed a fraud alert on your account, you should continue to monitor your credit reports for fraudulent activity.

Additionally, we encourage all patients to monitor account statements, EOBs and credit bureau reports closely and review guidance from the Federal Trade Commission ("FTC") or Office of Attorney General concerning identity theft preventative and responsive measures.

For More Information.

You may contact our Compliance Officer, Samantha Espinoza, with questions or concerns by phone at (800) 958-5549 between the hours of 8:00 a.m. – 4:30 p.m. Pacific Time, Monday through Friday; by e-mail at sespinoza@spectrumeye.com; or addressing a letter to 10300 S. DeAnza Boulevard, Cupertino, CA 95014. We have also established a section on our website with updated information and links to websites that offer information on what to do if your personal information has been compromised. You can access this information at: https://www.spectrumeye.com/notice-and-updates-regarding-ecl-data-breach/.

* * * *

At Spectrum, we take our role of safeguarding your personal information and using it in an appropriate manner very seriously. We sincerely apologize for the inconvenience, undue stress and concern this incident may have caused. We are doing everything we can to rectify the situation. Your information privacy is very important to us and we will continue to do everything we can to correct this situation and fortify our operational protections for you and others.

Sincerely,

Spectrum Eye Physicians

This document includes an important notice. If you cannot read this attached document, please visit https://www.spectrumeye.com/notice-and-updates-regarding-ecl-data-breach/ for translation help. If you do not have access to the internet, please contact the practice at (800) 958-5549 for translation.

Este documento incluye un aviso importante. Si no puede leer el aviso adjunto, por favor visite https://www.spectrumeye.com/notice-and-updates-regarding-ecl-data-breach/ para obtener ayuda de traducción. Si no tiene acceso a internet, por favor póngase en contacto con el consultario a (800) 958-5549 para la traducción.

本文件包含一項重要通知。 若您無法閱讀此附件，請前往 **https://www.spectrumeye.com/notice-and-updates-regarding-ecl-data-breach/** 以獲得翻譯上的協助。 如果您無法使用網路，請致電 **(800) 958-5549** 聯繫機構以索取翻譯版本。