



April 20, 2022

Via email: ldtheft@oag.state.md.us

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Dear Sir or Madam:

We are writing on behalf of our customer health plan, Blue Shield of California, to notify you of a data privacy incident involving one (1) Maryland resident. National Imaging Associates, Inc. (NIA), a subsidiary of Magellan Health Inc. (Magellan), administers radiology health benefits on behalf of Blue Shield of California as their contracted vendor. We review certain proposed health care services to decide whether they are medically necessary and covered under the health plan.

Summary of Incident

NIA discovered an employed Physician Clinical Reviewer (“PCR”) was violating numerous NIA policies by providing a non-employee with access to his computer via Zoom for the apparent purpose of having the non-employee perform the PCR’s job-related tasks. The PCR is a board-certified radiologist who was employed by NIA from October 2021 through March of 2022 to conduct medical necessity reviews.

NIA discovered the incident on March 7, 2022 after identifying irregularities in the PCR’s activities. Once flagged, NIA undertook a review of the PCR’s work. At that time, the PCR was observed allowing a non-employee guest to join a company Zoom session while conducting a plan member’s case review. The PCR shared his screen via Zoom with the non-employee and then granted functional remote access to the non-employee through a Zoom feature. This gave the non-employee the ability to see the member’s case and clinical records. Based on our investigation, we believe the PCR was granting access to the non-employee so they could complete the PCR’s reviews.

The PCR, who was working from home, was not authorized to grant access to any third parties. He misused company resources in doing so, and acted in violation of his training and NIA’s policies and procedures. Once NIA discovered the violation, the PCR’s system access was terminated. The PCR is no longer employed by NIA. Our investigation indicated this PCR may have engaged in the same or similar behavior when conducting member case reviews for services requested by providers between November 1, 2021, through March 8, 2022.

Type of Information Involved

The information which the non-employee guest could have seen would include health information from the medical record that a provider sent to us for review, such as diagnosis, treatment, dates of service, medical history, test results, prescription information, provider name, or anything similar in a medical file or record. It would also include demographic data in NIA’s system such as name, address, gender, phone number, date of

birth, health plan, and health plan member ID number. Social Security Number was not identified as being included.

Remedial Efforts

Following this incident, NIA reviewed its IT controls and determined there was no IT or control failure.

Notwithstanding this determination, NIA has taken the following actions to prevent this from happening again:

1. The remote-control feature was disabled for all NIA Zoom users. The feature is locked so users are unable to manually enable it. The Remote Support feature is enabled for a subset of IT personnel and trainers that need the functionality to support the business. The Remote Support feature has improved logging over Remote Control, so we can identify abuses of this feature.
2. We have tightened the permissions on our enterprise Zoom account and now have a process to request elevated permissions for using the Remote Support feature.
3. We have disabled and locked the ability to share files within the in-meeting chat for the "General Users" Zoom group. This was the default setting, but is now locked and cannot be changed by users.
4. In Zoom Chat, chat communications are only permitted between employees. This setting has now been applied to all employees.
5. NIA has implemented a ZOOM meeting monitoring process. This process requires users and managers to verify that meetings over 10 hours with less than 3 people are legitimate.
6. PCR's laptop sent for further forensic analysis.
7. Compliance Alert to be issued to all employees.
8. Reporting the PCR to the State Medical Boards and law enforcement.

Attached is the letter template being used to notify affected Blue Shield of California members, including the one (1) Maryland resident, on or about April 22, 2022.

If you have any questions or need further information regarding this incident, please do not hesitate to contact my office.

Respectfully submitted,



Carla S. Jackson, Esq.
Chief Compliance Officer
Magellan Health
410-953-4709
csjackson@magellanhealth.com



[insert date]

RECIP_ADDR_LN1
RECIP_ADDR_LN2
RECIP_ADDR_LN3
RECIP_ADDR_LN4

RE: Notice of Privacy Breach

Dear [insert Member Name]:

National Imaging Associates (NIA), a subsidiary of Magellan Health Inc. (Magellan), administers your radiology health benefits on behalf of [insert health plan]. We review certain proposed health care services to decide whether they are medically necessary and covered under your plan.

We are writing to let you know that we recently learned some of your protected health information may have been shared with an unauthorized person. This situation occurred as the result of an employee performing work in an unauthorized manner.

What Happened

On March 7, 2022, NIA learned through a targeted performance review of one of NIA's Physician Clinical Reviewers (PCR) that the PCR had a non-employee guest logged into a company Zoom session while conducting a health plan member's case review. A PCR is a physician who reviews medical records from your doctor to decide if health care services are medically necessary and covered under your plan. The PCR shared his screen via Zoom with this unknown person and then granted remote access to the person through a Zoom feature. This gave the non-employee the ability to see and review the member's case and clinical records. The PCR was not authorized to do this.

After learning about this, we suspended the PCR's system access and started an investigation into the PCR's actions. Our review indicates this PCR may have done the same or similar behavior when conducting your case review(s) for services requested by your provider between November 1, 2021, through March 8, 2022.

What Information Was Involved

The information which the unknown person could have seen would include health information from your medical record that your provider sent to us for review, such as diagnosis, treatment, dates of service, medical history, test results, prescription information, provider name, or anything similar in your medical file or record. It would also include your demographic data in NIA's system such as name, address, gender, phone number, date of birth, health plan, and

health plan member ID number. Your Social Security Number was not identified as being included.

What We Are Doing

NIA recognizes the importance of protecting the confidentiality of your health information. Please know that we take such situations very seriously. This incident was the result of the unauthorized actions of a single employee who acted in violation of NIA's training and our policies and procedures. The PCR is no longer employed by NIA. We are also exploring technical enhancements which could prevent something like this from happening again.

What You Can Do

While we have no reason to believe your personal information is at risk of further misuse, to help protect your identity we are offering a complimentary 12-month membership of Experian's® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: 7/31/2022** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll:
<https://www.experianidworks.com/plus>
- Provide your **activation code: [insert code]**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9332 by **7/31/2022**. Be prepared to provide engagement number **B046992** as proof of eligibility for the identity restoration services by Experian.

Other Important Information

Keep a copy of this letter for your records in case of any potential future problems with your health plan benefit records. Review any statements you receive about your health plan benefits regularly and carefully; if you see any suspicious activity, such as service(s) that you believe you did not ask for or receive, call the number on your member ID card.

If you have any questions or would like any additional information, please do not hesitate to contact us at (800) 442-4179.

Sincerely,



Carla S. Jackson, Esq.
Chief Compliance Officer
Magellan Health

Additional Steps You Can Take

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

Equifax	Experian	TransUnion
Phone: 1-800-685-1111 P.O. Box 740256 Atlanta, Georgia 30348 www.equifax.com	Phone: 1-888-397-3742 P.O. Box 9554 Allen, Texas 75013 www.experian.com	Phone: 1-888-909-8872 P.O. Box 105281 Atlanta, GA 30348-5281 www.transunion.com

Free Credit Report. We remind you to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies – Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee.

Don't confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her

as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

For New Mexico residents: You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

For Colorado and Illinois residents: You may obtain information from the credit reporting agencies and the FTC about security freezes.

Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. As of September 18, 2018, when you place a fraud alert, it will last one year, instead of 90 days. Fraud alerts will still be free and identity theft victims can still get an extended fraud alert for seven years.

For Colorado and Illinois residents: You may obtain additional information from the credit reporting agencies and the FTC about fraud alerts.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland Residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For Rhode Island Residents: You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, <http://www.riag.ri.gov>, 401-274-4400.

Reporting of identity theft and obtaining a police report. You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft. You also have a right to file a police report and obtain a copy of it.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

For Rhode Island residents: You have the right to file or obtain a police report regarding this incident.