



July 26, 2023

Office of the Attorney General
St. Paul Plaza
200 St. Paul Place
Baltimore, MD 21202

RE: Synergy Healthcare Services Security Incident

Dear Sir/Madam:

I am writing to notify you that Synergy Healthcare Services—a HIPAA business associate—suffered a security incident involving the potential unauthorized access to the personally identifiable information of 815 Maryland residents. Synergy Healthcare Services delivers consulting and professional support services to the following covered entities: Consulate Health Care, Raydiant Health Care, Independence Living Centers, and their affiliated care centers. Because we were processing the affected data on their behalf, we are providing this notice for them.

We identified suspicious activity on our network in early December 2022 and engaged third-party experts to investigate. We determined on December 15th that an unauthorized third party accessed a portion of our computer network containing a number of files, including those with personally identifiable information. On December 22nd, our investigation identified which files the unauthorized third party may have accessed, and later that same day we posted notice of the incident on our website. We also promptly shared those results with a data-review company so they could help us determine what information was in those files. The data-review company provided us their results on May 16, 2023, and we have been working diligently since then to (1) assess our notification obligations, (2) coordinate with the data owners, and (3) ensure we have accurate contact information for individuals requiring notice.

Having reviewed the data, we have reason to believe that the threat actor potentially acquired the personally identifiable information of 815 Maryland residents. The affected files included information such as an individual's name, contact information, government identification (driver's license, Social Security number, etc.), medical/treatment history, insurance details, and financial information. But, at this time, we have no reason to suspect the information was or will be misused.

Consistent with our state and federal obligations, we are notifying the affected individuals that a limited portion of their personally identifiable information and/or protected health information may have been acquired by an unauthorized party. Our notices include 1 year of complimentary credit monitoring for individuals who had their Social Security number, driver's license number, or similar government identifier impacted. We are relying on a combination of mailed notice and substitute notice. We are mailing the notices on July 27, 2023 and issuing substitute notice around the same time. I have attached templates of the notices we are sending to Maryland residents.

In addition to providing notice and conducting a thorough investigation, we have taken a variety of steps to further bolster our security. This includes, among other measures, adding multifactor authentication for all remote access.

If you have any questions or need any additional information regarding this incident, please contact me at 813-769-6280 or email me at Rachel.S.Carlock@synergyhcs.com.

Sincerely,

A handwritten signature in blue ink that reads 'Rachel S. Carlock'.

Rachel S. Carlock, Esq., CHC



Return mail will be processed by: IBC
PO Box 847 • Holbrook, NY 11741

1040 Crown Pointe Parkway, Suite 600
Atlanta, GA 30338
P (770) 698-9040 • F (770) 730-1268
SynergyHealthcareServices.com

NOTICE OF DATA BREACH

July 27, 2023

Dear [REDACTED]:

Synergy Healthcare Services is writing to inform you of a security incident that may have affected some of your protected health information. We received the affected information in connection with providing professional services to Consulate Health Care, Raydiant Health Care, Independence Living Centers, and their affiliated care centers. While monitoring our network, we detected suspicious behavior in early December 2022 and soon detected unauthorized access to a limited portion of our files. We have been working since then to identify all of the affected individuals. While that process was ongoing, we posted information about this incident to our website on December 22nd. We are now providing this notice to give you more information on what happened and what we are doing in response.

WHAT HAPPENED

We identified suspicious activity on our network in early December 2022 and engaged third-party experts to investigate. We determined on December 15th that an unauthorized third party accessed a portion of our computer network containing a number of files, including those with personal health information. Shortly thereafter, our investigation identified which files the unauthorized third party may have accessed. We shared those results with a data-review company on December 22nd so they could help us determine what information was in those files. The data-review company provided us their results on May 16, 2023, and we have been working diligently since then to determine who needs notice and ensure we have accurate contact information for those individuals.

WHAT INFORMATION WAS INVOLVED

The affected files may include information such as your name, birthdate, signature, insurance details, contact information, medical history/treatment, and financial information (such as your bank account number). At this time, we have no reason to suspect that any of the affected information has been used fraudulently.

WHAT WE ARE DOING

We worked with third-party experts to investigate and respond to the incident, and we are further securing our systems to protect your information.

WHAT YOU CAN DO

We have provided a list of steps on the next page that you can take to protect yourself.

FOR MORE INFORMATION

Synergy Healthcare Services takes the privacy and security of the information in our care seriously, and we regret any inconvenience this incident may cause you. Should you have any questions, you can contact us at (866) 935-7074, and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

A handwritten signature in cursive script that reads 'Rachel S. Carlock'.

Rachel S. Carlock, Esq., CHC

LAVIE-ADT-NOCM

ADDITIONAL STEPS YOU CAN TAKE

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports. You can also find additional suggestions at www.IdentityTheft.gov.

- You should confirm that your credit card company has the correct address on file for you and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.
- You should obtain and review a free copy of your credit report by visiting www.annualcreditreport.com or calling 1-877-322-8228. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. The alert lasts for one year, but you can renew it.
- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which makes it harder for someone to open an account in your name. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and previous addresses. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe you are the victim of identity theft, consider (1) notifying your Attorney General, local law enforcement, or the Federal Trade Commission; (2) filing a police report and requesting a copy of that report; and (3) visiting IdentityTheft.gov to report the issue and get recovery steps.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft.

Federal Trade Commission

600 Pennsylvania Ave. NW
Washington, DC 20580
(202) 326-2222
www.ftc.gov

Equifax

P.O. Box 740241
Atlanta, GA 30374
(800) 685-1111
www.equifax.com

Experian

P.O. Box 9701
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion

P.O. Box 2000
Chester, PA 19016
(888) 909-8872
www.transunion.com

**Maryland
Attorney General**

200 St. Paul Place, 25th Floor
Baltimore, MD 21202
(888) 743-0023
www.marylandattorneygeneral.gov

**New York
Attorney General**

The Capitol
Albany, NY 1224
(800) 771-7755
www.ag.ny.gov

**North Carolina
Attorney General**

9001 Mail Service Center
Raleigh, NC 27699
(919) 716-6400
www.ncdoj.gov

**Washington, DC
Attorney General**

400 6th St. NW
Washington, DC 20001
(202) 727-3400
www.oag.dc.gov

You can also find your Attorney General's contact information at: <https://www.usa.gov/state-attorney-general>.



Return mail will be processed by: IBC
PO Box 847 • Holbrook, NY 11741

1040 Crown Pointe Parkway, Suite 600
Atlanta, GA 30338
P (770) 698-9040 • F (770) 730-1268
SynergyHealthcareServices.com

NOTICE OF DATA BREACH

July 27, 2023

Dear [REDACTED]:

Synergy Healthcare Services is writing to inform you of a security incident that may have affected some of your protected health information and other personal information. We received the affected information in connection with providing professional services to Consulate Health Care, Raydiant Health Care, Independence Living Centers, and their affiliated care centers. While monitoring our network, we detected suspicious behavior in early December 2022 and soon detected unauthorized access to a limited portion of our files. We have been working since then to identify all of the affected individuals. While that process was ongoing, we posted information about this incident to our website on December 22nd. We are now providing this notice to give you more information on what happened and what we are doing in response.

WHAT HAPPENED

We identified suspicious activity on our network in early December 2022 and engaged third-party experts to investigate. We determined on December 15th that an unauthorized third party accessed a portion of our computer network containing a number of files, including those with personal health information. Shortly thereafter, our investigation identified which files the unauthorized third party may have accessed. We shared those results with a data-review company on December 22nd so they could help us determine what information was in those files. The data-review company provided us their results on May 16, 2023, and we have been working diligently since then to determine who needs notice and ensure we have accurate contact information for those individuals.

WHAT INFORMATION WAS INVOLVED

We determined that some of the affected files contained protected health information and other personally identifiable information. The affected files may include information such as your name, birthdate, signature, insurance details, contact information, government identification (such as a driver's license or Social Security number), medical history/treatment, and financial information (such as your bank account number). At this time, we have no reason to suspect that any of the affected information has been used fraudulently.

WHAT WE ARE DOING

We worked with third-party experts to investigate and respond to the incident, and we are further securing our systems to protect your information. Additionally, we are providing you with complimentary credit monitoring. You can activate that monitoring service by following the instructions on the next page.

WHAT YOU CAN DO

We have provided a list of steps on the next page that you can take to protect yourself.

FOR MORE INFORMATION

Synergy Healthcare Services takes the privacy and security of the information in our care seriously, and we regret any inconvenience this incident may cause you. Should you have any questions, you can contact us at (866) 935-7074, and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

Rachel S. Carlock, Esq., CHC

LAVIE-ADT

ADDITIONAL STEPS YOU CAN TAKE

Activate your complimentary credit monitoring – To help protect you from fraud or identity theft, we are offering a complimentary one-year membership to Experian's IdentityWorks. This product helps detect possible misuse of your personal information. To register, please:

- Ensure that you enroll by: **October 20, 2023** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
- Provide your activation code:

If you have questions or want an alternative to enrolling in Experian IdentityWorks online, please contact Experian at 1-877-288-8057 by October 20, 2023, and provide them with engagement number [REDACTED].

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports. You can also find additional suggestions at www.IdentityTheft.gov.

- You should confirm that your credit card company has the correct address on file for you and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.
- You should obtain and review a free copy of your credit report by visiting www.annualcreditreport.com or calling 1-877-322-8228. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. The alert lasts for one year, but you can renew it.
- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which makes it harder for someone to open an account in your name. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and previous addresses. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe you are the victim of identity theft, consider (1) notifying your Attorney General, local law enforcement, or the Federal Trade Commission; (2) filing a police report and requesting a copy of that report; and (3) visiting IdentityTheft.gov to report the issue and get recovery steps.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft.

Federal Trade Commission

600 Pennsylvania Ave. NW
Washington, DC 20580
(202) 326-2222
www.ftc.gov

Equifax

P.O. Box 740241
Atlanta, GA 30374
(800) 685-1111
www.equifax.com

Experian

P.O. Box 9701
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion

P.O. Box 2000
Chester, PA 19016
(888) 909-8872
www.transunion.com

Maryland Attorney General

200 St. Paul Place, 25th Floor
Baltimore, MD 21202
(888) 743-0023
www.marylandattorneygeneral.gov

New York Attorney General

The Capitol
Albany, NY 1224
(800) 771-7755
www.ag.ny.gov

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
(919) 716-6400
www.ncdoj.gov

Washington, DC Attorney General

400 6th St. NW
Washington, DC 20001
(202) 727-3400
www.oag.dc.gov

You can also find your Attorney General's contact information at: <https://www.usa.gov/state-attorney-general>.