

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

450 Sentry Parkway, Suite 200
Blue Bell, PA 19422

Phone: (610) 567-0700
Fax: (610) 567-0712

www.C-WLAW.com

A Mid-Atlantic Litigation Firm

Visit us online at
www.C-WLAW.com

JORDAN MORGAN
jmorgan@c-wlaw.com

LEI WANG
lwang@c-wlaw.com

September 26, 2023

Via E-Mail (IDTheft@oag.state.md.us)

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

RE: Security Breach Notification

To Whom It May Concern:

We serve as counsel for WellBe Senior Medical, LLC (“WellBe”) located at 225 West Washington Street, Suite 1500, Chicago, IL 60606, and provide this notification to you of a recent data security incident related to WellBe.¹ By providing this notice, WellBe does not waive any rights or defenses under Maryland law, including the data breach notification statute.

On or around February 1, 2023, WellBe was contacted by a third-party vendor, Fortra, who informed WellBe of a cyber incident that may have allowed an unknown individual to access certain patient information. Notably, Fortra confirmed that they had experienced a cyber incident that allowed access to their application, GoAnywhere. WellBe utilizes the GoAnywhere application to transfer certain patient data. Following this notification, WellBe took immediate action to review the data housed in the GoAnywhere application to determine whether any patient information may have been impacted by the individual(s) who caused this incident. On February 14, 2023, after a thorough investigation, WellBe confirmed that a limited amount of Protected Health Information (“PHI”) information may have been accessed in connection with this incident.

As a Business Associate to various Covered Entities, WellBe began an immediate review of internal records in order to associate impacted patients with the respective Covered Entity. Following this review, WellBe identified 2,322 patients associated with Aetna ACE (“Aetna”) were potentially impacted during this incident. WellBe provided formal notification on behalf of Aetna to impacted patients and the U.S. Department of Health and Human Services in accordance with HIPAA Breach Notification Rule². Notice to patients was provided via First Class Mail on or around April 4, 2023. At the time of this notification, no residents of Maryland were identified as being impacted as a result of this incident.

Following this initial notification, WellBe subsequently learned of additional patient data that was potentially at risk as a result of this incident. In response, WellBe immediately retained a third-party e-discovery review team to data-mine the additional information to identify any individuals who were not previously notified

¹ WellBe is a Healthcare Covered Entity, and in certain circumstances, a Business Associate under the Health Insurance Portability and Accountability Act (“HIPAA”). See, 45 CFR 160.103.

² See, 45 CFR 164.400-414.

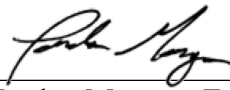
of the incident. On or around June 6, 2023, WellBe received the results of the data mining, which provided a list of all potentially impacted individuals, and their respective information that may have been at risk of access. Upon receipt, WellBe immediately undertook a time-intensive process to locate any available addresses, compile an updated notice list for these individuals, and associate impacted individuals with the respective Covered Entity.

Following this review, WellBe identified additional 39,698 individuals associated with Aetna who were potentially impacted during this incident. Immediately after, on July 13, 2023, Wellbe notified Aetna in accordance with 45 C.F.R. § 164.410, and offered to notify all impacted patients, as well as all applicable regulators on behalf of Aetna. Upon learning of the potential access of information, Aetna immediately performed a thorough review process to analyze what type of information was impacted, and to whom that information belonged. That process was completed on September 14, 2023, and the results identified 6 residents of Maryland. The type of information related to these Maryland residents included one or more of the following: Patient Names, Dates of Birth, Lab Results, Medical History and Treatment Information, Physician IDs, Medical Record Numbers, and/or Patient Identification Numbers.

Immediately after, WellBe will provide formal notification to these impacted individuals on behalf of Aetna via First Class Mail on September 27, 2023. A copy of the notice letter is attached hereto as **Exhibit A**, which provides details of the incident and access to a dedicated call center. WellBe is taking proactive steps to ensure that all state and federal notification obligations are complied with due to this incident. This includes providing notice to the U.S. Department of Health and Human Services in accordance with HIPAA Breach Notification Rule³ and all applicable state regulators.

Please contact me should you have any questions.

Very truly yours,



Jordan Morgan, Esq.

³ See, 45 CFR 164.400-414.

Exhibit A



Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

RE: NOTICE OF HIPAA BREACH
Important Security Notification. Please read this entire letter.

Dear <<Name 1>>:

WellBe Senior Medical, LLC (“WellBe”) writes to notify you of a recent incident that may impact the privacy of certain information provided to us. Aetna ACE has engaged WellBe to provide health management and treatment services for its members. In order to provide these services, WellBe needs access to certain information, and Aetna ACE entrusts WellBe with the required data.

We take the privacy of information in our care seriously, and while we have no evidence to suggest that any information was misused, in an abundance of caution, we are providing you information about the incident, our response, and steps you can take to help protect your information.

What Happened:

On or around February 1, 2023, WellBe was contacted by a third-party vendor, who informed WellBe of a cyber incident that may have allowed an unknown individual to access certain patient information. Notably, the vendor confirmed that they had experienced a cyber incident that allowed access to an application that WellBe utilizes to transfer certain patient data. Following this notification, WellBe took immediate action to determine whether any information may have been accessed by the individual(s) who caused this incident. On September 14, 2023, after a thorough investigation, WellBe confirmed that a limited amount of your protected health information may have been accessed in connection with this incident.

To date, we have no evidence to suggest any actual or attempted misuse of information. However, we are providing this notification to you out of an abundance of caution and so that you may diligently monitor your personal information and resources.

What Information Was Involved:

It is important to note, as mentioned above, that there is no evidence to suggest that any information has been misused. The information that could have been subject to unauthorized access may have included your first and last name, in combination with one or more of the following data elements: Date of Birth, Lab Result, Medical History and Treatment Information, Physician ID, Medical Record Number, and/or Patient Identification Number.

What We Are Doing:

WellBe has taken every step necessary to address the incident and is committed to fully protecting all of the information entrusted to us. Unfortunately, these types of incidents have become increasingly common and this incident is similar to others experienced by other companies across the country. Upon learning of this incident, we took steps to enhance the security of all information to help prevent similar incidents from occurring in the future and are reviewing our current policies and procedures related to data protection.

What You Can Do:

We recommend that you remain vigilant in regularly reviewing and monitoring all of your account statements and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on any of your accounts, please promptly change your password and notify your financial institution or company, if applicable. Additionally, please report any suspicious incidents to local law enforcement and/or your state Attorney General. We have provided additional information below, which contains more information about steps you can take to help protect yourself against fraud and identity theft.

For More Information:

Should you have questions or concerns regarding this matter, please do not hesitate to contact us at 1-888-596-6356, Monday through Friday, 9:00 a.m. to 9:00 p.m. Eastern Time, or write us at 225 West Washington Street, Suite 1500, Chicago, Illinois 60606.

WellBe takes the security of information entrusted to our care very seriously. While it is regrettable this potential exposure occurred, please be assured we are taking appropriate actions to rectify the situation and prevent such incidents in the future.

Sincerely,

Joshua Aubey
Chief Compliance & Privacy Officer
WellBe Senior Medical, LLC

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address history for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver’s license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000 TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Experian 1-888-397-3742 www.experian.com Experian Fraud Alert P.O. Box 9554 Allen, TX 75013 Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	Equifax 1-888-298-0045 www.equifax.com Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069 Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788
---	---	--

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies

may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to employers; (v) you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; (vi) and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There is one (1) resident of Rhode Island impacted by this incident.

For Washington, D.C. residents, the District of Columbia Attorney General may be contacted at 400 6th Street NW, Washington, D.C. 20001; 202-442-9828, and <https://oag.dc.gov/consumer-protection>.