LEWIS BRISBOIS

LEWIS BRISBOIS BISGAARD & SMITH LLP

Todd M. Rowe
550 West Adams Street
Suite 300
Chicago, IL 60661
Todd.Rowe@lewisbrisbois.com
Direct: 312.345.1718

May 23, 2022

File No. 49905.119

VIA EMAIL

Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
DOJ-CPB@doj.nh.gov

Re: Notification of Data Security Incident

Dear New Hampshire Office of the Attorney General:

Lewis Brisbois Bisgaard & Smith LLP represents Allwell Behavioral Health Services ("ABHS") in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with New Hampshire's data breach notification statute, N.H. Rev. Stat. §§ 359-C:19 et seq.

1. **Nature of the Security Incident**

On March 5, 2022, ABHS discovered unauthorized party was able to gain access to and encrypt some of its servers. ABHS immediately notified the Federal Bureau of Investigation ("FBI") and U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency ("CISA"), and immediately began containment, mitigation, and remediation measures to reduce the impact on its operations. Additionally, ABHS engaged cybersecurity experts to supplement its response efforts, including conducting a forensic investigation to identify the source of the compromise.

The forensic investigation determined that an unknown third-party gained access to ABHS's network and may have acquired certain data without authorization from its quality assurance system related to the treatment of patients at ABHS, as well as ABHS's employee human resources system. Following this finding, ABHS reviewed the affected files to determine whether they contain personal information relating to any individuals and if so, the categories of information involved for each.

On April 19, 2022, ABHS determined that the affected files contained personal information relating to its some of its employees. Upon this determination, ABHS worked diligently to identify current address information for the affected individuals in order to provide notice of the incident. ABHS completed this process for the majority of the affected individuals on May 18, 2022.

To date, there is no evidence to suggest that the information in the affected files was published, shared, or otherwise misused.

2. Type of Information and Number of New Hampshire Residents Involved

The incident involved personal information for approximately 1 New Hampshire resident. For ABHS patients, the information involved in the incident may differ depending on the individual but may include the following for affected New Hampshire residents who were patients of ABHS: name, date of birth, Social Security number, phone number, treatment activity, treatment provider, treatment date, treatment location, and payer information.

Again, ABHS has no reason to believe that the information involved has been or will be published, shared, or otherwise misused.

3. Notification to Affected Individuals

On May 23, 2022, notification letters were sent to affected New Hampshire residents via USPS First Class Mail. The notification letter provides resources and steps individuals can take to help protect their information. The notification letter also offers complimentary identity protection services, including credit monitoring, dark web monitoring, $1 million identity fraud loss reimbursement policy, and fully-managed identity theft recovery services. A sample notification letter is enclosed.

4. Measures Taken to Address the Incident

In response to the incident, ABHS retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the compromise. ABHS is in the process of implementing additional security measures to further harden its digital environment in an effort to prevent a similar event from occurring in the future.

As noted above, ABHS has reported the incident to the FBI and CISA and will cooperate fully to assist with any investigation.

As discussed above, ABHS is notifying the affected individuals and providing them with steps they can take to protect their personal information, including enrolling in the complimentary identity protection services offered in the notification letter. It is also notifying nationwide consumer reporting agencies of the incident.

5. Contact Information

ABHS is dedicated to protecting the sensitive information within its control. If you have any questions or need additional information regarding this incident, please do not hesitate to contact me at Todd.Rowe@lewisbrisbois.com or 312.345.1718.

Sincerely,

Todd M. Rowe

Todd M. Rowe of
LEWIS BRISBOIS BISGAARD & SMITH LLP

TMR:MFF

Encl.: Sample Consumer Notification Letter
cc: Michael Ferragamo, Lewis Brisbois (Michael.Ferragamo@lewisbrisbois.com)

P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:
1-833-909-0995
Or Visit:
https://response.idx.us/allwell
Enrollment Code: [XXXXXXXX]

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

May 23, 2022

Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

I am writing to inform you of a data security incident that may have involved your personal information. At Allwell Behavioral Health Services ("Allwell"), we take the privacy and security of our patient's information very seriously. This is why we are notifying you of the incident and informing you about steps you can take to help protect your personal information.

What Happened? On March 5, 2022, we discovered a data security incident. In response, we took steps to secure our computer systems and immediately began an investigation with the help of cybersecurity experts. The investigation team determined that on or about March 2, 2022, an outside party gained access to the computer system that we use to store quality assurance information related to the treatment of patients at Allwell. In late April 2022, the investigation concluded and it was determined that it appears likely the unauthorized party was able to take an undetermined number of files containing client information from the computer system. While at this time we have no evidence that any client information was misused, out of an abundance of caution we are providing credit protection to our client community.

What Information Was Involved? The information in the quality assurance system varied but potentially may have included things such as your name, date of birth, Social Security number, phone number, treatment activity, treatment provider, treatment date, treatment location, and payer information. We have no information that the information on the quality assurance system has been misused.

What Are We Doing? As soon as we discovered the incident, we took the steps described above. Additionally, we have upgraded our information technology and computer systems to provide additional security to protect against further unauthorized access. We also notified federal law enforcement authorities and the U.S. Department of Health and Human Services Office for Civil Rights.

In addition, we are offering identity theft protection services through IDX, a leading data breach and recovery services firm. IDX identity protection services include: [12 months/24 months] of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-833-909-0995 or going to https://response.idx.us/allwell and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is August 23, 2022.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully informed of the incident and can answer any questions you may have regarding protection of your personal information.

For More Information You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter. Please call 1-833-909-0995 or go to https://response.idx.us/allwell for assistance or for any additional questions you may have.

The security of our clients' personal information is of the utmost importance and we deeply regret that this data security incident occurred.

Sincerely,

James McDonald

James McDonald
President and CEO
Allwell Behavioral Health Services
2845 Bell Street
Zanesville, Ohio 43701
1-833-909-0995

(Enclosure)

Recommended Steps to Help Protect Your Information

1. **Website and Enrollment.** Go to https://response.idx.us/allwell and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-833-909-0995 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

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

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, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. 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. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.